ÇANKAYA ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
SİYASET BİLİMİ VE ULUSLARARASI İLİŞKİLER ANABİLİM DALI

YÜKSEK LİSANS TEZİ

ULUSLARARASI SİBER GÜVENLİK VE SİBER ORTAMDAKİ TEHDİTLERİN FİZİKSEL BİR SAVAŞA DÖNÜŞME OLASILIĞI

YASEMİN GÜRYUVA

AĞUSTOS 2019

Tez Başlığı: **Uluslararası Siber Güvenlik ve Siber Ortamdaki Tehditlerin Fiziksel Bir Savaşa Dönüşme Olasılığı**

Tezi Hazırlayan: **YASEMİN GÜRYUVA**

Sosyal Bilimler Enstitüsü Onayı

Prof. Dr. Mehmet YAZICI

Sosyal Bilimler Enstitüsü Müdürü

Bu tezin yüksek lisans derecesi elde etmek için gerekli koşulları sağladığını onaylarım.

Prof. Dr. Hasan Bahadır TÜRK

Siyaset Bilimi ve Uluslararası İlişkiler

Anabilim Dalı Başkanı

Bu tez, tarafımdan incelenmiş olup yüksek lisans tezi olarak uygun bulunmuştur.

Doç. Dr. Gökhan AKŞEMSETTİNOĞLU

Tez Danışmanı

Tez Jüri Tarihi: 02 / 08 /2019

Tez Jüri Üyeleri:

Prof. Dr. Cem KARADELİ (Ufuk Üniv.)

Doç. Dr. Gökhan AKŞEMSETTİNOĞLU (Çankaya Üniv.)

Doç. Dr. Ebru ÇOBAN ÖZTÜRK (Çankaya Üniv.)

ÇANKAYA ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ MÜDÜRLÜĞÜ'NE

Bu belge ile bu tezdeki bütün bilgilerin akademik kurallara ve etik davranış ilkelerine uygun olarak toplanıp sunulduğunu beyan ederim. Bu kural ve ilkelerin gereği olarak, tez çalışmamda bana ait olmayan tüm veri, düşünce ve sonuçları bilimsel etik kurallar gözeterek ifade ettiğimi ve kaynağını gösterdiğimi ayrıca beyan ederim. 30.09.2019

Adı, Soyadı: Yasemin GÜRYUVA
İmza:

ÖZET

ULUSLARARASI SİBER GÜVENLİK VE SİBER ORTAMDAKİ TEHDİTLERİN FİZİKSEL BİR SAVAŞA DÖNÜŞME OLASILIĞI

Yasemin GÜRYUVA

Yüksek Lisans Tezi

M.A., Siyaset Bilimi ve Uluslararası İlişkiler

Tez Yöneticisi: Doç. Dr. Gökhan AKŞEMSETTİNOĞLU

Ağustos 2019, 235 Sayfa

Siber alan hayatın her yerinde karşımıza çıkabilecek önemli konulardandır. Özellikle uluslararası ilişkilerde dikkat edilmesi gereken bir güvenlik konusu hâline gelmiştir. Çalışmanın amacı; uluslararası ilişkilerde siber alanında ortaya çıkabilecek tehditlerin fiziksel bir savaşa dönüşme olasılığıdır. Çalışma dört bölümden oluşmaktadır. İlk bölümde; uluslararası siber güvenlik ve siber alan hakkında bilgi verilerek, tarihsel altyapıdan söz edilmektedir. İkinci bölümde; bazı devlet ve örgütler üzerinden, siber alandaki önemli örnekler ve oluşabilecek tehditler için belirlenen önlem ve politikalardan bahsedilmektedir. Üçüncü bölümde; siber tehditlerin bir savaşa dönüşme olasılığında yapılabileceklerden bahsedilip, son bölümde genel bir değerlendirme yapılmaktadır.

Anahtar kelimeler: Uluslararası İlişkiler, Uluslararası Siber Güvenlik, Siber Alan, Siber Tehditler, Siber Savaş

ABSTRACT

INTERNATIONAL CYBER SECURITY AND THE POSSIBILITY OF THREATS IN CYBER SPACE TO A PHYSICAL WAR

Yasemin GÜRYUVA

Master Thesis

M.A., Political Science and International Relations

Supervisor: Doç. Dr. Gökhan AKŞEMSETTİNOĞLU

August 2019, 235 Pages

Cyber space is one of the most important issues that can be encountered in every part of life. It has become a security issue that needs attention especially in international relations. Purpose of the study; the possibility that cyber threats in international relations may turn into a physical war. The study consists of four parts. In the first part; historical infrastructure is mentioned by giving information about international cyber security and cyberspace. In the second part; through some states and organizations are mentioned important examples in cyberspace, measures and policies determined for the possible threats. In the third part; what can be done in the possibility of cyber threats turning into a war. In the last part, a general consideration has been made.

Keywords: International Relations, International Cyber Security, Cyber Space, Cyber Threats, Cyber War

TEŞEKKÜR

Tez çalışmalarım süresince değerli yardım ve bilgileriyle bana yol gösteren saygıdeğer tez danışmanım Doç. Dr. Gökhan AKŞEMSETTİNOĞLU'na ve yüksek lisans boyunca bilgi ve birikimlerini paylaşan çok kıymetli hocalarıma, ayrıca, bu süreçte her türlü desteğiyle yanımda olan sevgili aileme, sabırla bana destek olan kıymetli dostlarıma ve hayat arkadaşıma, verdikleri kıymetli destekleri ve bana karşı sonsuz sabırları için, ayrı ayrı teşekkürü borç bilirim.

İÇİNDEKİLER

DÖRDÜNCÜ BÖLÜM

KISALTMALAR

ABD: Amerika Birleşik Devletleri

APT: Advanced Persistent Threats / Gelişmiş Sürekli Tehditler

ARP: Address Resolution Protocol / Adres Çözümleme Protokolü

ARPA: Advanced Research Projects Agency / İleri Araştırma Projeleri Ajansı

ARPANET: Advance Research Projects Agency Network / İleri Araştırma Projeleri Ajansı Ağı

BİLGEM: Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi

BİS: Bilgi ve İletişim Sistemleri

BND: Bundesnachrichtendienst / Federal İstihbarat Servisi

BSI: Bundesamt für Sicherheit und Informationstechnik / Bilgi Güvenliği Federal Ofisi

BTK: Bilgi Teknolojileri ve İletişim Kurumu

CCD COE: Cooperative Cyber Defence Center of Excellence / Siber Savunma İşbirliği Mükemmeliyet Merkezi

CDC: NATO Cyber Defense Committee / NATO Siber Savunma Komitesi

CDCT: Council of Europe Counter-Terrorism Committee / Avrupa Konseyi Terörle Mücadele Komitesi

CDMB: NATO Cyber Defence Management Board / NATO Siber Savunma Yönetim Kurulu

CERN: Conseil Européen pour la Recherche Nucléaire / European Organization for Nuclear Research / Avrupa Nükleer Araştırma Merkez

CERT CC: Computer Emergency Respons Team Control Center / Bilgisayar Olaylarına Müdahale Ekibi Kontrol Merkezi

CERT-EU: Computer Emergency Response Team-EU / Avrupa Birliği Bilgisayar Acil Müdahale Ekibi

CIA: Central Intelligence Agency / Merkezi İstihbarat Teşkilatı

CODEXTER: Committee of Experts on Terrorism / Terörle Mücadele Uzmanlar Komitesi

CPNI: Centre for the Protection of National Infrastructure / Milli Altyapıları Koruma Merkezi

C-PROC: Cybercrime Programme Office of the Council of Europe / Avrupa Konseyi Siber Suçlar Program Ofisi

CPU: Central Process Unit- Merkezi İşlem Birimi

CSOC: Cyber Security Operations Center / Siber Güvenlik Harekât Merkezi

DARPA: The Defense Advanced Research Projects Agency / Savunma İleri Araştırma Projeleri Ajansı

DDOS: Distributed Denial of Service / Dağınık Servis Dışı Bırakma

DHS: Department of Homeland Security / İç Güvenlik Bakanlığı

DLP: Data Leakage Prevention / Veri Kaçağı Önleme Sistemleri

DNS: Domain Name System / Alan Adı Sistemi

DoD-ARPA: Department of Defence's Advanced Research Project Agency / Savunma Bakanlığı İleri Araştırma Projesi Ajansı

DOS: Denial of Services / Servis Dışı Bırakma

EDA: European Defence Agency / Avrupa Savunma Ajansı

EDT: American Electronic Disturbance Theater / Amerikan Elektronik Karışıklık Tiyatrosu

ENISA: European Union Agency for Network and Information Security / Avrupa Birliği Ağ ve Bilgi Güvenliği Ajansı

ESCD: NATO Emerging Security Challenges Division / NATO Yeni Gelişen Güvenlik Sorunları Bölümü

FBI: Federal Bureau of Investigation / Federal Araştırma Bürosu

FTP: File Transfer Protocol / Dosya Aktarım Protokolü

GCHQ: Government Communications Headquarters / İngiliz Dijital İstihbarat Servisi

GLACY +: Global Action on Cybercrime / Siber Suçlarda Küresel Eylem

HTTP/HTTPS: Hiper Text Transfer Protocol / Hiper Metin Aktarma Protokolü

IBM: International Business Machines / Uluslararası İş Makineleri

ICANN: International Corporation for Assigned Names and Numbers / İnternet Tahsisli Sayılar ve İsimler Kurumu

ICMP: Internet Control Management Protocol / İnternet Kontrol Mesajı Protokolü

IDS: Intrusion Detection System / Saldırı Tespiti Sistemi

IEEE: Institute of Electrical and Electronics Engineers / Elektrik ve Elektronik Mühendisleri Enstitüsü

IMPACT: International Multiliteral Partnership Against Cyber Threats / Siber Tehditlere Karşı Uluslararası Çok Uluslu Ortaklık

IP: Internet Protocol / İnternet Protokolü

IPS: Intrusion Prevention System /Saldırı Önleme Sistemi

ISO/IEC: International Organization for Standardization / International Electrotechnical Commission- Uluslararası Standartlar Teşkilâtı / Uluslararası Elektroteknik Komisyonu

ITU: International Telecommunication Union / Uluslararası Telekomünikasyon Birliği

KSA: Kommando Strategische Aufklarung / Stratejileri Aydınlatma Komandosu

MIT: Massachusetts Institute of Technology / Massachusetts Teknoloji Enstitüsü

NASA: National Aeronautics and Space Administration / Ulusal Havacılık ve Uzay Dairesi

NATO: North Atlantic Treaty Organization / Kuzey Atlantik Antlaşması Örgütü

NCIA: NATO Communications and Information Agency / NATO Muharebe ve Bilgi Teşkilatı

NCIRC: NATO Computer Incident Response Capability / NATO Bilgisayar Olaylarına Müdahale Yeteneği

NCISS: NATO Communications and Information Systems School / NATO İletişim ve Bilgi Sistemleri Okulu

NCSC: National Cyber Security Center / Ulusal Siber Güvenlik Merkezi

NFS: Near Field Communication / Yakın Alan İletişimi

NSA: National Security Agency / Milli Güvenlik Teşkilatı

NSFNET: National Science Foundation Network / Ulusal Bilim Vakfı Ağı

OCSIA: Office of Cyber Security & Information Assurance / Siber Güvenlik ve Bilgi Güvencesi Ofisi

OECD: Organisation for Economic Cooperation and Development / Ekonomik İşbirliği ve Kalkınma Örgütü

OSI: Open Source Interconnection / Açık Kaynak Ara Bağlantısı

OWASP: Open Web Application Security Project / Açık Web Uygulama Güvenliği Projesi

PCeU: Police Central e-Crime Unit / Emniyet Merkezi e-Suç Birimi

PLA: The Chinese People's Liberation Army / Çin Halk Kurtuluş Ordusu

RADAR: Radio Detecting and Ranging / Radyo Algılama ve Değiştirme

SMB: Server Message Block / Sunucu İleti Bloğu

SMTP: Simple Mail Transfer Protocol / Elektronik Posta Gönderme Protokolü

SNMP: Simple Network Management Protocol / Basit Ağ Yönetim Protokolü

SOME: Siber Olaylara Müdahale Ekipleri

SSCB: Sovyet Sosyalist Cumhuriyetler Birliği

SSH: Secure Shell / Güvenli Kabuk

T-CY: The Cybercrime Convention Committee / Siber Suçlar Konvansiyon Komitesi

TCK: Türk Ceza Kanunu

TCP: Tranmission Control Protocol / Geçiş Kontrol Protokolü

TCP/IP: Transmission Control Protocol/Internet Protokol / Geçiş Kontrol Protokolü/ İnternet Protokolü

TELNET: Telecommunication Network / İletişim Ağı

TİB: Telekomünikasyon İletişim Başkanlığı

TÜBİTAK: Türkiye Bilimsel ve Teknolojik Araştırma Kurumu

UDP: User Datagram Protocol / Kullanıcı Datagram Protokolü

UNODA: United Nations Office for Disarmament Affairs / Birleşmiş Milletler Silahsızlanma Dairesi

UNODC: United Nations Office on Drugs and Crime / Birleşmiş Milletler Uyuşturucu ve Suç Dairesi

USOM: Ulusal Siber Olaylara Müdahale Ekibi

VPN: Virtual Private Network / Sanal Özel Ağ

GİRİŞ

Temel ihtiyaçların karşılanması, kişilerin rahat hissetmesi, hedeflerin başarılı olmasında önemlidir. İhtiyaçlar içerisinde en temel olanlardan biri; güvende olmadır. Bir bireyin güvenliği, bir devletin güvenliğiyle aynı oranda önemlidir. Devletin, kendi toplumundaki bir bireyin güvensizliği, toplumun huzurunu bozacak niteliktedir. Bireylerin güvensiz hissetmesiyse; devlete olan güven duygusunun sarsılmasına sebep olur. Bir devletteki güvensizlik; uluslararası alana yansımaktadır. Devletteki güvensizlik; çevresindeki devletler ve bağlı olduğu kuruluşlarda uluslararası alanda bir güvensizliği oluşturur. Uluslararası alanda güvenliğin sağlanması ayrı bir öneme sahiptir. Güvenlikte hepsi birbiriyle bağlantılıdır. Genel olarak tek bir tanımlaması olmayan güvenlik, en çok üzerinde çalışılan konulardan biridir.

Güvenlik; insanlık tarihi boyunca karşımıza çıkmış önemli konulardandır. Yaşamak için hayatta kalmak kadar, gelecek tehditlere karşı korunmak da gerekir. Güvenlik, bireylerin normal yaşamlarını sürdürebilmelerinde ne kadar önemliyse, bir toplumda ya da bir devlette hayatta kalmak ve güvende olmak benzer şekilde önemlidir. Güvenliğin sağlanabilmesi hem bireysel olarak, hem devlet olarak hem de uluslararası alanda belirli amaç ve hedeflere ulaşmakta kolaylık sağlayacaktır. Güvenliğin oluşturulması için tehdit ve risklerin en az seviyeye düşürülmesi gerekmektedir. Güvenlik sürekli büyüyüp yenilenerek, kendine üzerinde çalışılması gereken öğeler ekleme eğilimindedir. Her dönemde yeni tehdit ve güvenlik sorunları ortaya çıkmaktadır. Güvenliğin tarihi çok eski dönemlere dayanmaktadır. Ancak yapılan çalışmalar günümüzde yenilenerek devam etmektedir. Bir düzenin sağlanabilmesi için uluslararası alanda güvenliğin sağlanması gerekir. Güvenlik bir düzen ve amaçların sağlanması için önemlidir. Güvenliğe verilen önemse; tarih içerisinde ortaya çıkan olaylar üzerinden daha çok artmıştır. Güvenlik üzerine çalışmalarsa ihtiyaca göre şekillenmiştir.

Güvenlik, içerik açısından; bireyden uluslararası alana kadar uzanan geniş bir çerçevededir. Bir birey ya da uluslararası bir sistemin düzenini devam

ettirebilmek için güvenliğinin sağlanmasına ihtiyaç vardır. Bu çerçeve içerisindeyse yeni yükselen ve önem kazanan konular vardır. Güvenlikte, çağımızda yeni yükselen, önemli çalışmalara ihtiyaç duyan konularından biri; siber alandır. Siber alan, anarşik bir düzende, belirli kuralları olmadan, yeni ortaya çıkmış bir güvenlik yapısıdır. Güvenlik konuları içerisinde farklı bir yere sahiptir. Siber alanın sınırları yoktur. Siber alanın sınırlarının olmayışı, uluslararası sistemdeki çalışmalarda sorun çıkarabilecek düzeydedir. Küresel bir yapının bulunduğu uluslararası sistemde, her zaman yeni çalışmalar ve düzenlemelere ihtiyaç duyulur. Farklı bir yapısı olması ve yeni ortaya çıkmış bir güvenlik ihtiyacı oluşu, uluslararası güvenlik alanında ayrı bir yerinin olmasına da etki etmektedir.

Uluslararası alan ve siber alanın sınırlarının olmaması, sorunları beraberinde getirir. Alanlardaki sorunların, alan içerisinde bir düzenin hâkim olmamasından kaynaklandığını savunan düşünceler vardır. Uluslararası alanda hâkim ve çalışmalarda en etkili düşünce; realist yaklaşımdır. Çalışmada realist yaklaşımdan söz edilirken, uluslararası alanda etkin diğer yaklaşımlardan da bahsedilecektir. Ancak uluslararası alanda realist yaklaşımın daha hâkim olması, çalışmada da ön planda olmasına sebep olmaktadır. Uluslararası güvenlik sisteminde hâkim olan düşünceler, günümüzdeki bazı düşünce ve çalışmaların temelinde yatmakta olduğu için önemli bir yere sahiptir.

Genel çerçevede; uluslararası ilişkiler alanında yeni ortaya çıkan, kısa sürede, özellikle güvenlik alanında önem kazanan, siber güvenlikten bahsedilecek. Uluslararası alanda, siber yapının özelliklerinden söz edilecektir. Siber alanın önemli yapıları, kullanım alanları, bu alanların getirdiği tehditlere ayrıca bakılacaktır. Siber alandaki gerginlikler sonucunda bazı devletler ve örgütlerin belirlemiş oldukları politikalardan söz edilecektir. Siber alandaki gerginliklerin, fiziksel bir savaşa dönüşme olasılığından bahsedilecektir. Bu olasılığın gerçekleşme halindeyse yapılması uygun olan çalışmalar, çalışmanın amacını oluşturmaktadır.

Çalışmada, başlangıç olarak; "Uluslararası Siber Güvenlik" hakkında bilgi verilecektir. Siber güvenliğin öneminin anlaşılması içinse öncelikle güvenlikten söz edilecektir. Güvenlik ve siber alan hakkında temel bilgilerin açıklanması bölümün amacıdır. Güvenliğin belirli yaklaşımlar üzerinden tanımlanması, siber

güvenliğin tanımında da etkilidir. Siber alanın açıklanmasıysa, siber güvenliğin sağlanmasının öneminin daha iyi görülmesini sağlayacaktır.

Siber alandaki teorik bilgilerden söz edilmesi; siber güvenliğin tanımlaması, üzerinde çalışılabilmesi için belirli düşüncelerin oturmasında yardımcıdır. Çalışmada siber alandan söz ederken; internet yapısı, hackerlar ve alanın getirdiği tehditlere değinmek gerekir. Siber alandaki tehditlerse iki başlık altında incelenecektir. Bilgisayar ortamındaki tehditler ve stratejik tehditler olarak iki başlığa ayrılır, ancak, ikisi de birbiriyle bağlantılıdır. Siber alandaki tehditler temel olarak bilgisayar ortamından çıkmaktadır. Siber alandaki stratejik tehditlerse; bilgisayar ortamındaki tehditler sayesinde sağlanabilmektedir. Tehditlerin açıklanması, savunma için önemlidir. Siber savunma sistemi oluşturulurken nelere dikkat edileceği tehditlerle ortaya çıkar. Tehditlerin ortaya çıkışındaysa bir birikim söz konusudur. Birikimlerin oluşma süreci tarihsel altyapıda görülür. Siber güvenliğin tarihsel altyapısı incelenirken; siber alanın ilk dönem kullanımı, Soğuk Savaş Dönemi ve yakın dönemde kullanımı şeklinde üç bölüme ayıracaktır. Tarihsel altyapıyla beraber siber alanın genel yapısından söz edilmesi, uluslararası alanda siber güvenlik konusunun yerini ve önemini göstermiş olacaktır.

Teorik olan ilk bölümden sonra, siber güvenlik üzerine önemli bilgiler verilmiş olacaktır. Sonraki bölümdeyse; "Siber Ortamda Var Olan Tehditler Fiziksel bir Savaşa Dönüşebilir mi?" düşüncesi incelenecektir. Bu bölümde siber alan için önemli bazı devletler olan; ABD (Amerika Birleşik Devletleri), Çin Halk Cumhuriyeti, Rusya Federasyonu, Federal Almanya Cumhuriyeti, İngiltere, Türkiye Cumhuriyeti ele alınacaktır. Aynı zamanda siber alanda önemli adımlar atmış olan örgütlerden bazıları olan; Avrupa Birliği, NATO, Birleşmiş Milletler, Avrupa Konseyi'nin önemli politikaları üzerinden gidilecektir. Bu devlet ve örgütlerin önemli örneklerinden faydalanılarak bir inceleme yapılacaktır. Yapılan incelemeler sonucunda, bölümün konusu olan tehditten söz edilecektir.

Siber alanda ayrı bir yeri olan bazı devlet ve örgütlerin önemli çalışma ve örneklerinden bahsettikten sonraki bölümde; "Siber Tehditlerin Fiziksel Bir Savaşa Dönüşme Olasılığına Karşı Geliştirilebilecek Çalışmalar"dan söz edilecektir. Önlemler ışığında, çalışmada siber alanda problem olarak görülen kısma dikkat çekilerek, bir çözüm sunulmaya çalışılacaktır.

Söz edilen noktalardan hareketle çalışmada "Siber güvenlik nasıl olmalıdır?", "Ne gibi yöntemlere dayandırılarak bir siber güvenlik ortamı oluşturulmalıdır?" gibi sorular sorularak, bu sorulara belirli bir çerçeve çizilebilecektir. Siber güvenlik kavramının, bir güvenlik kavramını tanımlamaktaki zorlukları kadar, aynı ölçüde bu sorulara cevaplar arama noktasında benzer zorluklar bulunmaktadır. Güvenlik tanımlamasının kesin bir biçimde yapılamayışı belirli bir problem oluşturabilse dahi günümüzde yapılan çalışmalarla ortaya atılan en yakın cevaplar ve çözümler belirli açılardan yol gösterici olmaktadır. Ancak her kavram ve teori gibi, yapılan tanımlar birden ortaya çıkmamıştır. Belirli süreçler içerisinde dönüşüm geçirerek günümüze gelmiştir.

Çalışma; güvenlik içerisinde yeni ve önemli bir yeri bulunan siber alanın, uluslararası alanda oluşturabileceği tehlikeler üzerinden, olası tedbirleri incelemektedir. Çalışmada; doküman analizleriyle veriler toplanarak, nitel araştırma yöntemi kullanılmıştır. Genel tarama yöntemi uygulanarak; kitap, makale, web siteleri ve dergilerden edinilen bilgiler ışığında yorumlamalar yapılıp, çalışma hazırlanmıştır.

BİRİNCİ BÖLÜM

ULUSLARARASI SİBER GÜVENLİK

Güvenlik, uluslararası alanda ciddi bir konuma sahiptir. Her alanda olduğu gibi, güvenlik, hatta güvende olma, uluslararası alanda öncelikli ihtiyaçlardandır. Uluslararası alan içerisinde güvenlik, en çok ihtiyaç duyulan ancak tanımı kolaylıkla yapılamayan bir konudur. Tek bir tanımının olmaması güvenliği önemli bir noktada tutmaktadır. Güvenliğe kim tarafından, hangi açıdan bakıldığı ayrı bir öneme sahiptir. Uluslararası alanda güvenlik, aktör açısından değişim gösterebilecek bir yapıdadır. Güvenliğe farklı açılardan bakılarak, dönemlere göre değişebilen tanımlarının yapılmasıysa, farklı birçok tanımının ortaya çıkmasına neden olmuştur. Önemiyse; içerisinde yeni alanlar barındırması ve her zaman kendini yenileyen bir alan olmasından kaynaklıdır. Kendisini yenileyebilen ve gelişen bir yapısı olmasıysa kendi içerisinde yeni çalışılması gereken alanlar oluşturmasına sebep olmaktadır.

Güvenlik en genel olarak; bir düzenin olduğu, sorun ve problemlerin en az düzeyde seyrettiği süreçtir. Ancak güvenliği açıklarken içinde bulunulan dönem, kim tarafından tanımlandığı ve hangi alanı için tanımlandığına dikkat etmek gerekir. Uluslararası alanda, güvenlikle beraber birçok yeni konu ortaya çıkabilmektedir. Bu konulardan bir tanesiyse; günlük yaşantımız içerisinde önemli bir yere sahip, güvenliğin kendi alt kategorilerinden olan siber güvenlik kavramıdır. Siber güvenlik kavramı ve tanımı, dönem itibariyle yeni bir konu olarak görülmektedir. Ancak bu düşüncenin aksine, siber alan çok uzun zamandır hayatımızın içerisinde yer almaktadır. Siber alandaki güvenlik konusundan bahsedebilmek için öncelikle güvenlik anlaşılmalıdır. Sonrasında; siber kavramından bahsedilmelidir. Siber kavramını açıklayabilmek içinse bu kavrama ait belirli yapıları incelemek gerekir.

Siber güvenliğin anlaşılması için öncelikle; buna ait belirli kavramlar ve tanımlamalar yapılmalıdır. Siber kavramı açıklanmalıdır. Siber kavramıyla birlikte, kavramın bulunduğu alandan söz edilmelidir. Siber alanın yapısı,

teknolojik ilerlemelerle beraber sürekli gelişmekte, gelişmelere bağlı olarak değişikliklere uğramaktadır. Yaşanan değişiklikler siber alanın kullanım alanını da genişletmektedir. Siber alanın kullanımında, beklenen amacın dışına çıkan kullanıcılar da bulunmaktadır. Bu kişilerden ayrıca söz edilmelidir. Hacker adı verilen kişiler, kendi amaçları doğrultusunda kullandıkları siber alanda, daha çok gündelik hayatta kullanılan, belirlenmiş alan dışında faaliyetlerini sürdürmektedirler. Hackerlar genel kullanım alanının dışında çalışmalarda bulunmaları sebebiyle "normal kullanıcılar" dışında söz edilir. Alan için önemli bir parça olmasından dolayı; hackerlerın normal kullanıcılardan kendilerini farklı kılan yönlerinden söz etmek gerekir. Hackerların yaptığı gibi alanın farklı yönlerinin kullanımıyla bağlantılı olarak, siber alan içerisinde meydana gelen tehlikelerin ve tehditlerin varlığından bahsedilmelidir. Ancak uluslararası alanda önemli olan sadece hackerlar değil, büyük aktörlerin de aynı şekilde tehdit ve tehlikeler ortaya çıkarabilme ihtimalidir.

Siber alanda tehditler genel olarak iki şekilde açıklanabilir. Siber alanda bilerek ya da bilmeyerek, sistemsel şekilde oluşturulan ya da kendiliğinden ortaya çıkan tehditler vardır. Birçok şekilde ortaya çıkabilen sistemsel hatalara, her teknoloji kullanıcısı hayatında en az bir kere denk gelmektedir. Hatalar ya da tehditlerin etkileri, yine teknolojik yöntemlerle etkisiz hale getirilebilirken, doğru müdahale edilmesi önemlidir. Ancak siber alanda sistemsel şekilde oluşacak tehditler kadar önemli ikinci bir tehdit söz konusudur. Siber alandaki diğer tehdit çeşidi; var olan belirli tehditleri, bazı amaçlar doğrultusunda, stratejik bir biçimde kullanmaktır. Kullanım şekilleriyle belirli siber savaşlar ve siber terör ortaya çıkmaktadır. Siber savaşlar genel olarak; devletler ya da kabul görmüş aktörler tarafından yapılmaktadır. Siber savaşta, savaş kurallarına uyularak yapılan saldırılar ve saldırılara karşı koyuş biçimleri, siber alan üzerinden yer alır. Ancak, saldırıların bir siber savaş olup olmadığına belirli çerçevelerde karar verilmektedir. Siber savaş dışında, siber alanda yaşanan başka bir tehdit siber terördür. Siber terör; teknolojinin belirli örgütlerin ya da tehdit edici grupların eline geçmesi sonucunda, örgütlerin kendi amaçlarıyla, devletlerin belirli yapılarını tehdit etmesi biçiminde karşımıza çıkmaktadır. Önemli bir noktaysa; siber terörün savaştaki gibi belirli kurallar çerçevesinde değil, kendi kuralları ve amaçları doğrultusunda, var olan kurallar dışında kullanılması şeklinde

gelişmesidir. Tehditler sonucundaysa; belirli savunma yöntemleri, tehdit algılarına yönelik gelişmektedir.

Kavramlar gibi tehditler de belirli bir süreçte ortaya çıkmıştır. Siber tehditlerin ortaya çıkışında da bir tarihsel altyapı bulunmaktadır. Tarihsel altyapıyı çalışmada üç döneme ayırmak mümkündür. Tarihsel altyapının ilk dönemi; başlangıç aşamasında görülen siber tehditlerdir. Teknolojik olarak çok büyük atakların olmadığı, gelişimlerin sürdüğü, aynı zamanda ilk ortaya çıkışların yaşandığı bir dönemdir. 1914-1947 yıllarını kapsayan ilk dönem içerisindeki tanımlamalar siber tehdit biçimde ifade edilmemiş olsa bile, siber anlamda kullanılan tehditlerin ilk ortaya çıkış süreci olarak kabul edilebilmektedir. Sonraki dönem olarak; Soğuk Savaş döneminden söz etmek mümkündür. Teknolojik gelişmelerin artık bir atağa geçtiği, ülkelerin gelişim oranlarının daha çok arttığı, bunlara bağlı olarak daha temkinli bir ortam olduğu bu dönemin 1947-1991 yıllarını kapsamaktadır. Yakın dönemse; 1991 yılından günümüze kadar gelen, gelişmelerin hâlâ devam ettiği bir dönemdir. Siber tehditlerin sıklıkla karşımıza çıktığı, bu tanımlamalardan daha kolay bahsedilebilen ve karşılaşılabilen bir dönemdir. Günümüzde bile tehditler noktasında yenileri karşımıza çıkmaktadır. Tehditler, sürekli gelişip, değişebilen bir dönem içerisinde varlıklarını sürdürmektedir. Günümüzdeki değişimler, tehditler kadar güvenlikte de geçerlidir. Bahsedilen tüm tanımlamaları daha iyi açıklamak için ilk olarak güvenlikten söz edilmelidir. Genel anlamda birçok kavramın çıkış noktası, hatta temel taşı sayılabilecek kavramlardan biri güvenliktir. Güvenliğin tam bir tanımlaması günümüzde hâlâ yapılamıyor olsa bile, söz edilmiş birçok açıdan tanımlama çalışmada temel oluşturmaktadır.

1.1. GÜVENLİK NEDİR?

Uluslararası alanda önemli pek çok alan vardır. En önemli alanlardan bir tanesi güvenliktir. Güvenliği uluslararası alanda politik davranışlardan biri olarak düşünürsek, öncelikle uluslararası politika kavramından bahsetmek gerekmektedir. Dünya politikası genel olarak üç temel şekilde gelişmeler göstermiştir. Dünya politikasının göstermiş olduğu gelişmeler; imparatorluk sistemi, feodal sistem, son olarak günümüzde daha çok hâkim olan anarşik

devletler sistemidir.[1] İmparatorluk sistemi ve feodal sistem günümüzde uluslararası alanda kendini etkin olarak gösteren sistemler değildir. Uluslararası alanda görülen sistem anarşik devlet sistemi olmakla beraber, bu sistem daha çok devletlerin üzerinde etkisi olacak tek bir yapının elinde olmamasından kaynaklıdır. Uluslararası alanda uygulanan politikalar, alanda değişkenlik oluşmasına sebep olmaktadır. Uluslararası politikada devletler yalnız hareket etmeye meyillidir. Bazı devletlerin diğer devletlerden güçlü olması, her an bir güce başvurabilme tehlikesini beraber getirmekte, bu da güvensizlik ortamı ve kuşku oluşturmaktadır.[2] Güvensizlik ve kuşkuyu ortadan kaldırmak için aktörlerin belirli çalışmalarda bulunduğu bilinmektedir. Yapılan çalışmaların genel bir tabiri ise güvenlik olmaktadır. Otuz yıl savaşları sonrasında oluşmaya başlayan, asıl hedefi Avrupa'nın dengesi olan, günümüze benzer şekilde diplomatik, aynı zamanda askeri şekildeki tekniklerin beraberinde olduğu, devletlerarasındaki rekabetlerde etkili, ancak devletleri belirli açılardan sınırlaması gereken bir sistem bulunması gerekmekteydi. Sistem hem rakipleri tahrik etmemeli hem de kendini zayıflatmaması gereken bir yapı olmalıydı.[3] Geçmişten günümüze bahsi geçen bu sistem gelişmiş, uluslararası alanda güvenlik oluşumunu sağlamış, bunun için yapılan çalışmalar gün geçtikçe artmış ve çeşitlenmiştir.

Güvenlik insanlık boyunca var olmuştur. Güvenlik her alanda karşımıza çıkabilecek bir kavramdır. Kesin bir tanımı olmamakla beraber, içerisinde bulunulan durum ve şartlara göre güvenlik bireyden bireye, toplumdan topluma değişebilmektedir. Tanımı değişkenlik gösterebilmesi dışında genel amaç; birey ya da toplum fark etmeksizin, var olan düzenin aynı şekilde sağlanabilmesini içermektedir. Ancak güvenliğin kendi içerisinde çeşitli amaçları barındırdığı bilinmektedir. Güvenliğin kendi içerisinde çeşitli amaçlarının bulunması tam olarak neyi içerisine aldığı üzerine tek bir açıklama yapılması ve evrensel bir anlayış ortaya çıkmasını zorlaştırmaktadır.[4] Bir kişi ya da toplum için güvenli olan bir durum bir başkası için güvensizlik içerebilmektedir. Güvenliğin aktörlere göre değişiklik göstermesi güvenlik ikilemi (security dilemma) ortaya çıkmaktadır.

[1] Joseph S. Nye, Jr. ve David A. Welch, *Küresel Çatışmayı ve İşbirliğini Anlamak*, Çev. Renan Akman (İstanbul: Türkiye İş Bankası Kültür Yayınları, Ekim 2013), 3-4.
[2] Nye ve Welch, *Küresel Çatışmayı ve İşbirliğini Anlamak,* 5.
[3] Michel Foucault, *Güvenlik, Toprak, Nüfus: 1977-1978*, Çev. Ferhat Taylan (İstanbul: İstanbul Bilgi Üniversitesi Yayınları, Aralık 2013), 258.
[4] Emre Çıtak, *Güvenlik ve İstihbarat* (İstanbul: Yeniyüzyıl Yayınları, 2017), 26.

Güvenlik ikilemi; devletlerin kendi güvenliğini sağlamak için alınacak önlemlerin, diğer devletlerin güvenliğini tehdit ettiği durumlardır.[5] Özellikle realist öğreti içerisinde geçen güvenlik ikilemi, devletlerin kendi arasındaki güvensizlikleriyle beraber bir güvenlik ortamının oluşmasına itici güç oluşturabilmektedir. Güvenlik ortamının oluşması için öncelikle bir güvensizlik durumunun bulunması gerekmektedir. Genel olarak güvenlik kavramı; bir açıdan güvensizlik ihtimallerinin ortadan kaldırılmasını ifade etmektedir.[6] Michel Foucault'a göre güvenlik; bir düzenek gibi, izin verilenle yasaklanan arasındaki durumdan çok, belirlenen bir "kabul edilebilir" olanı geçmemek biçimindedir.[7] Genel anlamda; güvenlik oluştuğu zaman, aynı durum başka bir aktör için güvensizlik oluşturmaktadır. Güvenlik oluşan ortamda aktör kendini ifade edip, amaçlarını gerçekleştirebilir. Amaç ve hedeflere ulaşmak için yapılan çalışmalarsa, başka bir aktörün kendi belirlemiş olduğu güvenlik sınırlarını geçtiği anda güvensizlik oluşturur. Güvenliğin sınırı aktöre bağlıdır. Bir durumun güvenli olup olmadığına aktörün kendisi, kendi belirledikleri sınırlar içerisinde karar vermektedir. Bir durumun güvenlik içerisinde olması ya da güvensizlik durumu olmasına karar verebilmek içinde belirli kavramlar olduğu bilinmektedir.

Güvenlikten söz edildiğinde değinilmesi gereken belirli kavramlar vardır. Açıklanması gereken kavramlardan genel kabul görenleri; tehdit, risk ve tehlikedir. Tehdit, risk ve tehlike sözcükleri güvenlik tanımı yapılırken öncelikle belirtilmesi gereken sözcüklerdir. Güvenlik olmadığında güvensizliğin hâkim olduğu bilinmektedir. Güvensizlik ihtimalleriyse riskleri gündeme getirir. Risklerin gerçekleşme ihtimali endişe ve korku yaratır, tehlikelerin yakınlığı ve büyüklüğüyse beraberinde tehditleri oluşturur.[8] Tehditler tanımlanmadığı sürece güvenlik tanımı yapılması zorlaşır. Tehditlerin yoğunluğunu belirleyen risk ve tehlike olmakla beraber korunmak istenen değere gelebilecek her çeşit olumsuzluk bir tehdit şeklinde algılanabilmektedir.[9] Yani; güvenliğin temelinde tehdit, risk ve tehlike kavramları bulunmaktadır. Tehdit, risk ve tehlikenin belirlenmesiyle, aslında iç içe geçmiş kavramlar olması, birlikte güvensizliğin yoğunluğu kendini

[5] Joshua S. Goldstein ve Jon C. Pevehouse, *International Relations* (Amerika Birleşik Devletleri: Pearson Longman, 2012, 10. Basım), 51.
[6] Beril Dedeoğlu, *Uluslararası Güvenlik ve Strateji* (İstanbul: Yeniyüzyıl Yayınları, 2014), 29.
[7] Foucault, *Güvenlik, Toprak, Nüfus*, 8-44.
[8] Dedeoğlu, *Uluslararası Güvenlik ve Strateji*, 28-29.
[9] Fikret Birdişli, *Teori ve Pratikte Uluslararası Güvenlik* (Ankara: Seçkin Yayınları, Ocak 2014), 18.

göstermektedir. Tehdit, risk ya da tehlikenin boyutu güvensizlikle aynı orantıda artmaktadır. Güvensizlik durumunun belirleyici faktörlerinden önemli olan üç kavram güvenliğin tanımlamasında ayrı yer tutmaktadır.

Güvenliğin varlığı, güvensizliğin olmaması olarak düşünülmektedir. Tehditler, riskler ve tehlikelerin ortadan kaldırılması, güvenlik için önemlidir. Üçünden bir tanesinin varlığı güvenlik durumunu tehlikeye düşürür. Bireysel ya da toplumsal olarak herhangi bir tanesinin varlığı bile endişe ve korku oluşturmasından dolayı birey kendini güvensiz hisseder. Bir toplumda, herhangi bir birey ya da grup içerisinde bireyin kendini güvensiz hissetmesi, o toplumda belirli bir rahatsızlık, olası bir kargaşa ortamı ortaya çıkartmaktadır. Söz edilen sebeplerden dolayı, bir toplumda öncelikli dikkat edilmesi gereken konulardan bir tanesi güvenliktir. Laura King'inde bahsetmiş olduğu üzere; Abraham Maslow'un ihtiyaçlar hiyerarşisinde[10] görülebilecek önemli ihtiyaçlardan söz edilmiştir. Öncelikli olan fizyolojik ihtiyaçlardan sonra, ikinci sırada gelen önemli ihtiyaç güvenliktir. Her bireyin fizyolojik ihtiyaçlarını kendi ihtiyaçları doğrultusunda giderdikten sonra, ikinci ihtiyaç duyduğu güvende olmaktır. Güvende olamayan kişiler, hiyerarşide bulunan sonraki aşamalara geçmekte zorluk yaşamaktadır. Aynı ihtiyaçları benzer biçimde bir toplum üzerinden düşünmek de mümkündür. Bir toplumda fizyolojik ihtiyaçlar karşılandıktan sonra, güvenlik hissi yoksa ya da o ülkenin güvenliği sağlanamıyorsa belirli sorunlar oluşabilmektedir. Diğer toplumlar gibi gelişme aşamasına geçebilmesi, aynı zamanda kendi içinde bir bütünlük, var olan sisteme bir güven duygusu oluşumunda problem çıkabilmektedir. Bir toplumu birlikte tutan parçalardan bir tanesinin güvenlik olduğunu söylemek mümkündür.

Güvenlik belirli açılardan bakıldığında; amaçla alakalı bir durumu gösterebilmektedir. Güvenlikle amaç arasında doğrudan bir ilişki vardır; amaçlar değiştikçe güvenlik anlayışı da ona göre değişebilir, hatta yeni güvenlik arayışları ortaya çıkartabilir. Güvenlik tek bir şekilde ya da düzlemde değildir. Birey, toplum, toplumsal alt grup, devlet, coğrafi ve uluslararası sistem güvenliği şeklinde ayrılabilir. Güvenlik uluslararası ilişkilerde; bölgesel kuruluşların, devlet aktörünün davranışları, uluslararası kuruluşlar, evrensel ilkeler açısından bakılan bir kavramdır. Ayrıca güvenlik, kavram olarak insanlıkla beraber başladığı

[10] Laura A. King, *The Science of Psychology: An Appreciative View* (New York: McGraw-Hill, 2008), 379.

hatırlanması gerekir. Uluslararası ilişkilerde güvenlik, farklı bakış açılarından incelenebilmekte, bir süreç içerisinde değerlendirilmesi gerekmektedir.[11]

Zaman ve ortaya çıkan bir olay, bir kavramın tanımını değiştirip geliştirmektedir. Bir güvenlik hali, içinde bulunulan zaman ve yaşanan olaya göre şekillenmektedir. Genel olarak bakıldığında; bir kavramın dahi, incelendiği dönem, algılanış biçimi, ne açıdan bakıldığı o kavramın tanımını etkilemektedir. Bu sebeple güvenlik kavramının tek bir zaman içerisinde genel, her dönemde geçerli kılınabilecek bir tanımının yapılması oldukça güçtür. Süreçler içerisinde yapılacak tek bir tanım başka bir dönem ve olayda aynı şartları sağlamadığı sürece geçersiz kalacaktır. Ancak belirli dönemler ve durumlar içerisinde, dönemin şartları ve içeriğine göre tanımlamalar yapılmaya çalışılmıştır. Günümüzde hâlâ önemli bir yere sahip olan, günümüz çalışmalarına temel olabilecek, hâlâ etkisini gösterebilen tanımlamalar bulunmaktadır. Ayrıca güvenlik tanımı için çalışmalar, yaklaşımlar üzerinden ayrı biçimde yapılmaktadır. Pek çok yaklaşımın güvenliğe bakış açısı kendi içlerinde farklılaşmaktadır. Yaklaşımın kendi bakış açısı, yapmış oldukları tanımlamalarda etkili olmuştur. Aynı zamanda tanımın yapıldığı dönemdeki uluslararası sistem ve yapı ayrı önem taşımıştır.

Güvenlikten söz edildiğinde, uluslararası yapı düşünülmelidir. Uluslararası alanda kesin olarak adlandırılmış bir siyasi gücün olmadığı düşüncesi, uluslararası alanda bir bakıma anarşik bir yapı olduğunu düşündürtmektedir. Genel bir şekilde anarşizmi tanımlarsak; siyasi bir otorite varlığının kötü ve gereksiz olması, işlerin genellikle gönüllü sözleşme ve iş birliği şeklinde idare edilebilmesi şeklindedir.[12] Aynı zamanda anarşizmde; düzensizlikten ziyade baskıyla değil, daha çok üyelerin kendilerince kabul etmiş oldukları sağduyu, beraberinde ahlak kurallarıyla bir düzenleme olmasını kastetmektedir.[13] Tanımlama devlet seviyesinde gibi görünmesine karşın, uluslararası alanda anarşik bir yapı olduğu belirli bir düşünce üzerine yerleşebilmektedir. Yani; uluslararası alanda anarşik bir yapı olduğunu kabul eden düşüncelerin temelinde; devletlerarasındaki ilişkiyi düzenleyen, devletler üstü bir güç olmamasından dolayı kaosun dahi gelişebileceği düşüncesi yerleşmiştir. Başka bir açıdan düşünecek olursak; uluslararası alanda devletler üzerinde bir gücün oluşması, devletlerin varlığına bir

[11] Dedeoğlu, *Uluslararası Güvenlik ve Strateji*, 34-39.
[12] Andrew Heywood, *Siyaset*, Ed.: Buğra Alkan (Ankara: Adres Yayınları, Şubat 2011), 91.
[13] Foti Benlisoy, "Anarşizm: Gönüllü Düzene Övgü" içinde *19. Yüzyıldan 20. Yüzyıla Modern Siyasal İdeolojiler*, der. H. Birsen Örs (İstanbul: İstanbul Bilgi Üniversitesi Yayınları, Ekim 2010), 362.

tehdit oluşturmaktadır. Devletin varlığının tehdit durumunda olması, yine bir güvensizlik oluşturup, daha büyük sorunlara yol açma ihtimaline sebep olacaktır. Aynı zamanda, bir üst gücün varlığının tarafsız şekilde olması gerekir. Ancak henüz bu düşünce içerisinde olabilecek bir devlet ya da büyük bir grup günümüzde ön plana çıkmamıştır. Günümüzde anarşik olarak görünen sistemin kendi sebeplerinden değiştirilemediği düşünülebilir. Ancak anarşik bir yapıda görünen bu sistem üzerinden farklı yaklaşımlarla çalışmalar yürütülmüştür. Güvenlik tanımlamasında yeri bulunan, tanımlama çalışmalarında temel yaklaşımlardan en önemlisiyse realist yaklaşım olduğu bilinmektedir.

Güvenlikten bahsedildiğinde var olan yaklaşımlardan en çok söz edileni realist güvenlik yaklaşımıdır. Realist yaklaşım, siyasetin temelinin insan doğasından farklılaşarak, uluslararası politikada güç ve çıkar kavramlarıyla açıklanıp, evrensel bazı ilkelerin devlet davranışlarında uygulanamayacağını savunan bir düşünce şeklidir. Realist yaklaşım, devleti, uluslararası ilişkilerin en temel aktörlerinden biri olarak kabul etmektedir. Uluslararası politikayla uluslararası ilişkileri devletlerin kendi içerisinde vermiş olduğu mücadelenin bir süreci olarak ele almaktadır.[14]

Realist gelenekte Thukydides'in Peloponnes Savaşı bahsinden, Sun Tzu'nun strateji eserlerine, hatta Niccoló Machiavelli, Thomas Hobbes'a kadar dayanan bir geçmişi bulunmaktadır.[15] Gökhan Bayraktar'ın da söz etmiş olduğu üzere; Thukydides'in düşüncesinde, devletlerin güçlenmesine izin vermektense önlemede başvurulacak yolun savaş olduğunu meşru saymıştır.[16] Joseph S. Nye, Jr. ve David A. Welch ise; Thukydides'in var olan kaçınılmazlık kuramının, daha çok bir taraf güçleniyorsa öbür taraf aynı biçimde güçlenme gereği duyar, bu yüzden savaş çıkabilme durumu kaçınılmazdır şeklinde söz etmiştir.[17] Bilgehan Emeklier ise; Hobbes'un düşüncesinden bahsederken; Hobbes'un "insan insanın kurdudur." (homo homini lupus) sözünden hareketle aslında doğa halini insanın doğası gereği kendi çıkarları doğrultusunda hareket eder şekilde tanımlamıştır. Ayrıca, toplumdan öncesini "herkesin herkesle savaştığı dönem" (bellum omnium contra omnes) şeklinde tanımlayıp, insan doğasının nasıl bir yapı sergilediğinden

[14]Ali Burak Darıcılı, *Siber Uzay ve Siber Güvenlik* (Bursa: Dora Yayınları, Aralık 2017), 9-10.
[15] Heywood, *Siyaset*, 178.
[16] Gökhan Bayraktar, *Siber Savaş ve Ulusal Güvenlik Stratejisi* (İstanbul: Yeniyüzyıl Yayınları, 2015), 45.
[17] Nye ve Welch, *Küresel Çatışmayı ve İşbirliğini Anlamak*, 23-28.

bahsetmiştir. [18] Realistlere göre insan doğası; Hobbes'un belirtmiş olduğu gibi kötü bir yapıya sahiptir. Bu sebeple çatışmayla savaş olağan bir hale gelmiştir. Klasik realizmde; insan doğasının kötü oluşu, devlet davranışları ve diplomaside üst bir otorite bulunmaması sebebiyle olumsuzluklar bulunmakta, bu anarşik bir yapı getirmektedir.[19] Klasik realizmde güvenlik; devletlerin, uluslararası çıkarları ve askeri gücüyle kalıcılığının ve güvenliğinin sağlanıp, çıkarlarının yerine getirilmesidir.[20] Uluslararası alanda güç dengesini değiştirmek isteyecek güçler, her an saldırgan eylemler ortaya koyabilecek şekilde hazır bulunmaktadır. [21] Bu da devletlerin her an saldırı için hazırlıklı olmasını beraberinde getirir. Realist çerçevede güç dengesi önemlidir. Güç dengesinin bozulması savaşı getirmektedir. Realistlere göre; güç ön plandadır. Askeri kaynaklar güvenlik konusunda önemli bir yerdedir. Bu yüzden devletin güvenliği ön planda olup "devlet güvende olursa birey de toplum da güvende olur" anlayışı bulunmaktadır.[22] Fikret Birdişli ise; Machiavelli'nin de söz etmiş olduğu gibi; güvende olabilmenin esası güçlü bir otoriter yönetimle savunmadan geçmekte olduğundan bahsetmiştir.[23] Mehmet Ali Ağaoğulları ise; Machiavelli'nin savunduğu insan doğası her şeyi arzu ederek elde etmek istemekte, başkalarını kıskanabilmekte olduğundan söz etmiştir. "İktidar" elde edilmek istenen olduğunda mücadele ortaya çıkmakta, bu insan doğasının kötülüğünü işaret edebilmektedir. Her insan başka biri karşısında engel görünüp, ona bu kötü sayılmakta, ayrıca insanın özünde bulunan bencilliği ortaya çıkartıp, kötülük denilebilecek her türlü davranışın ortaya çıkmasına sebep olmaktadır. Hobbes'un doğa durumu; insan doğasının kendi içerisinde kötü olmasından kaynaklıdır. Bunun kanıtı; insanların doğa durumunda eşit olması, eşitliğinse güvensizlik getirmesidir. Bu yüzden güvensizliğin sonucunda savaş getireceği, bir egemen bulunmadığındaysa insan doğası gereği çatışmacı bir durum içerisine gireceğinden bahsetmiştir.[24] Başka bir düşüncedeyse Hobbes'a göre; insan, doğası

[18] Bilgehan Emeklier, "Thomas Hobbes ve John Locke'un Güvenlik Anlayışının Karşılaştırmalı Analizi", içinde *Güvenlik Stratejileri Dergisi*, sayı: 13 (2011): 105, E.T.: 1 Haziran 2018, url: http://dergipark.ulakbim.gov.tr/guvenlikstrtj/article/view/5000098892,.

[19] Osman Şen, "Klasik Realizmin Güvenliğe Bakışı ve Kökenleri," içinde *Uluslararası İlişkilerde Güvenlik: Teorik Değerlendirmeler*, der.: Emre Çıtak ve Osman Şen (İstanbul: Uluslararası İlişkiler Kütüphanesi, Eylül 2014), 24.

[20] Darıcılı, *Siber Uzay ve Siber Güvenlik*, 15.

[21] Çıtak, *Güvenlik ve İstihbarat*, 125.

[22] Darıcılı, *Siber Uzay ve Siber Güvenlik*, 17.

[23] Birdişli, *Teori ve Pratikte Uluslararası Güvenlik*, 29.

[24] Mehmet Ali Ağaoğulları, *Sokrates'ten Jakobenlere Batı'da Siyasal Düşünceler* (İstanbul: İletişim Yayınlar, 2011), 327-435.

gereği üç temel sebepten kavga etmektedir. Bir şeyi elde etmek için yapılan rekabet, elde edilene tehlike geleceği güvensizliği yaşayarak şiddet eğilimi, şan ve şerefine gelebilecek herhangi olumsuzluğa karşı şiddet kullanma eğilimidir.[25] Bayraktara göre Hans Morgenthau; uluslararası sistemde güçler dengesinin barışı korumasında etkili unsurlardan biri olduğundan bahsetmektedir.[26] Ancak Ali Burak Darıcılı; Kenneth Waltz gibi neo-realist düşünürlerin klasik realizmden farklı olarak, uluslararası alanda güç edinme isteğinin insan doğası kaynaklı değil, uluslararası sistemin kendi yapısından kaynaklandığından bahsetmektedir.[27] Yani uluslararası alanda pek çok düşünür çatışma durumunun, sistemin kendi içerisinde bulunduğundan bahseder. Sistemin kendi içerisinde var olan, kendi çatışma durumlarına farklı çalışmalarla bir düzen getirmeye de çalışmışlardır. Bu sebeple realist yaklaşımlarla beraber belirli çalışmalar yürütüldüğü bilinmektedir. Realist yaklaşım kendi içerisinde belirli çalışma alanlarına ayrılabilmektedir. Devlet odaklı olmakla beraber, kendi içerisinde Stratejik Güvenlik Çalışmaları ve Barış Çalışmaları olarak ikiye ayrılmaktadır. Barış Çalışmaları dört alt kategoriye ayrılmakta, bunlar; Silahsızlanma (Disarmament), Silahların Kontrolü (Arms Control), Barış Hareketleri (Peace Movements) ve Dünya Düzeni (World Order) şeklinde çalışma ve yaklaşımlar içermektedir.[28] Günümüzde pek çok güvenlik çalışması devam etmekte, diğer farklı yaklaşımlar içerisinden doğan çalışmalar da geliştirilmektedir. Ancak bu çalışmalar güvenlik alanının daha farklı boyutlarında ilerlemektedir.

Realizm dışında güvenlikte başka bir önemli yaklaşımı liberal güvenlik yaklaşımıdır. Liberalizm devlet seviyesinde, devlet odaklı gibi görünmektedir. Ancak uluslararası açıdan daha farklı bir bakış açısına sahiptir. Liberal düşünürler küresel bir toplum yapısının olduğunu savunmakla beraber küresel olarak; ticaret gibi durumlarla devletlerin belirli bağlılıkları olduğunu, ticaretle kurulmuş olan temaslarla mutlak anarşik görüşün yetersiz kaldığını savunurlar.[29] Neo-liberallerse; mutlak kazanç adı altında iş birliği yapan tüm aktörlerin kazanç

[25] Der. Michael Rosen, Jonathan Wolff *Siyasal Düşünce*, Çev.: Sevda Çalışkan, Hamit Çalışkan (Ankara: Dost Kitabevi Yayınları, Temmuz 2006), 32.
[26] Bayraktar, *Siber Savaş ve Ulusal Güvenlik Stratejisi*, 45.
[27] Darıcılı, *Siber Uzay ve Siber Güvenlik*, 20.
[28] Birdişli, *Teori ve Pratikte Uluslararası Güvenlik*, 21.
[29] Nye ve Welch, *Küresel Çatışmayı ve İşbirliğini Anlamak*, 7.

sağlayacağını savunmaktadır.[30] Yani liberal yaklaşımda, uluslararası alanda, daha çok ticaret açısından bakarak bir bağlılık olduğundan söz edilmektedir. Belirli bağlılıkları olan ülkelerin kendi aralarında bir anarşi olduğu düşüncesinin daha zayıf kaldığını ve kendi içlerinde belirli düzenleri olabileceği görüşünü yansıtmaktadır.

Liberal ve Realist yaklaşımlar dışında başka önemli bir yaklaşım; Eleştirel güvenlik yaklaşımıdır. Yaklaşımda güvenliğin nasıl sağlanacağından çok güvensizliğin kaynağının nereden geldiği, barış halinden çok kültürel, ekonomik, sosyal yapıyı kapsayacak bir bütünlükle ele alınarak tehdit algısı eleştirilmiştir.[31] Eleştirel kuramda, güvenlik çalışmalarına dair; genişletilmesi, derinleştirilmesi ve yaygınlaştırılması gerekmektedir. Ayrıca genel kabullerin derinine inilip, egemen devletin güvenliği yerine onu oluşturan bireyin güvenliği ön plana çıkarken, kimin güvende tutulması gerektiği tanımlaması ve faydasında söz edilmektedir. İnsanın özgürlüğüne, varlığının kendisine karşı çıkabilecek tehditlere karşı alınabilecek güvenlik önlemleri eleştirel kuramın temelini oluşturmaktadır.[32] İnsan odaklı yaklaşımlardır. Özgürleştirici (emancipatory) ve özgün (individual) güvenlik yaklaşımları şeklinde ikiye ayrılır. Bunlar kendi içlerinde ayrıca ayrılmaktadır. Özgün güvenlik Çalışmaları; Yapısal Şiddet Teorisi ve Feminist Güvenlik yaklaşımı şeklinde ayrılırken, Özgünleştirici Güvenlik Çalışmaları iki ekol şeklinde ayrılmakta, bunlar; Galler ve Paris ekolüdür.[33] Özgün güvenlik çalışmaları belirli konular üzerine odaklanılmış çalışmalardır. Yani uluslararası alanda önemi olsa dahi, belirli gruplar ya da konular üzerine yoğunlaşmış çalışmalar olarak görülmektedir.

İnşacı (konstrüktivist) güvenlik yaklaşımı, diğer yaklaşımlar kadar önemli bir yaklaşımdır. Özellikle, kendi içerisinde bulunan İngiliz Okulunda; sosyal inşacılıkta belirli norm, değer ve kurumları paylaşmakta olan devletleri, uluslararası ilişkilerde hâkim olduğu söylenilen anarşik doğasına karşın bir 'uluslararası toplum' olduklarından söz etmektedir.[34] Aynı zamanda inşacılıkta;

[30] Fulya Akgül Durakçay, "Uluslararası İlişkilerde Liberal Yaklaşımlar ve Güvenlik Anlayışı," içinde *Uluslararası İlişkilerde Güvenlik: Teorik Değerlendirmeler*, der. Emre Çıtak ve Osman Şen (İstanbul: Uluslararası İlişkiler Kütüphanesi, Eylül 2014), 16.
[31] Birdişli, *Teori ve Pratikte Uluslararası Güvenlik*, 52.
[32] Çıtak, *Güvenlik ve İstihbarat*, 134-135.
[33] Birdişli, *Teori ve Pratikte Uluslararası Güvenlik*, 21.
[34] Mustafa Küçük, "Uluslararası İlişkilerde Sosyal İnşacılık," içinde *Uluslararası İlişkiler Teorileri*, der. Ramazan Gözen (İstanbul: İletişim Yayınları, 2014), 332.

insan doğasının toplumsal bir yapı içerisinde olması devlet yapısına yansımıştır. Bu da uluslararası alanda sosyal bir yapıyla bağdaşmış, kimlik gibi kavramlarla belirli güvenlik yaklaşımlarının oluşmasını sağlamıştır.[35]

Önemli bir diğer nokta; Kopenhag Okuludur. En temel kavramlarından bir tanesi olan güvenlikleştirme (securitisation) teorisiyle güvenlik çalışmalarına katkıda bulunmuştur. Kopenhag Okulunda söz edilen; her problemin anında bir güvenlik sorunu şeklinde algılanmaması gerektiğidir. Ancak bir sorunun zamanla bir güvenlik sorunu haline gelebilme ihtimali unutulmayıp, güvenlikleştirme sürecini getirerek bir bakıma sıra dışı biçimde siyasallaşma süreci olarak adlandırılmaktadır.[36] Kopenhag Okulu güvenliği beş bölüm üzerinden yürütmektedir; çevre, ekonomi, askeri, siyasi ve ideolojik.[37] Kopenhag Okulu güvenlik kavramına olumsuz anlam yüklerken, devletin güvenlikleştirme yaklaşımlarına eleştirel bakmaktadır.[38]

Birdişli'ye göre eleştirel inşacılık olarak adlandırabileceğimiz Kopenhag Okulunun önemli savunucularından ikisi; Barry Buzan ve Olea Waever'dır.[39] Ekolün savunucuları; güvenlik kavramının etkileşim ve iletişim sonucu ortaya çıktığı, güvenliğin sosyal bir şekilde, karşılıklı, öznel olarak yapılanmış olduğunu savunmaktadırlar. Burada; konuşma eylemiyle var olmayan bir tehdit olgusunun, söylemler sayesinde oluşturulması vardır. Ancak her söylem tehdit olarak algılanmamaktadır. Belirli bir güvenlik aktörünün tehdit varlığından söz etmesi bununla birlikte bunu tehdit olarak algılayacak bir alıcı kitlenin olması önemlidir.[40]

İnşacılıkta önemli başka bir nokta; güvenlik topluluğudur. Birdişli'ye göre; inşacı bir yaklaşım olan Karl Deutsch'un yaklaşımı; güvenlik topluluğunun, karşılıklı gelişmekte olan ekonomik ilişkilerinin ortak şekilde, çıkarlara yönelik bir alan oluşturulabileceği fikri ortaya atılmıştır. Ekonomik faktörleri dikkate

[35] Sezgin Kaya "Uluslararası İlişkilerde Konstrüktivist Yaklaşımlar," *Ankara Üniversitesi Siyasal Bilgiler Fakültesi Dergisi* Cilt. 63 Sayı: 3 (2008): 95, E.T.: 23 Haziran 2018, url: http://www.politics.ankara.edu.tr/dergi/pdf/63/3/6-Kaya-Sezgin.pdf.
[36] Fikret Birdişli, *Teori ve Pratikte Uluslararası Güvenlik* (Ankara: Seçkin Yayınları, Ocak 2014), 96.
[37] Çıtak, *Güvenlik ve İstihbarat*, 127.
[38] Çıtak, *Güvenlik ve İstihbarat,* 130.
[39] Birdişli, *Teori ve Pratikte Uluslararası Güvenlik*, 92.
[40] Mehmet Eren, *Avrupa Birliği'nin Siber Güvenlik Politikası* (İstanbul: Beta Yayınları, Mart 2017), 13-15.

alarak, siyasal temellerde bir birlik oluşturmayla yeni çıkabilecek savaşlara engel olma amaçlı bir topluluk düşüncesi vardır.[41]

Uluslararası alanda güvenlik iki şekilde kullanılmaktadır. Devletin güvenlik anlayışı üzerinden yapılanan kullanımlar, sistemin tamamı ya da bireyler için onlara yönelik güvenlik anlayışlarına dayanan kullanımlardır. İkinci söz edilen neredeyse tüm devletlerin ortak tehdit olarak gördüklerini düzenlenmesi anlamında gelirken, ilki; bir devletin iktidarı, vatandaşların refah düzeyi, ülkesel varlığı koruma, geliştirme anlamındadır.[42]

Güvenliğin genel bir tanımı yapılacak olursa; Tek bir düzleme sıkıştırılmadan, bir bireyden bir sisteme kadar, değişen amaç ve süreçlere göre şekillenebilen, sınırları aktörlere bağlı, tehdit, risk ve tehlikelerin kabul edilebilir bir düzeyi geçmeden, var olan bir düzen ya da yapıyı bulunduğu şekline yakın bir biçimde devam ettirmeyi kapsamaktadır. Güvenlik; dönemlere ve yaklaşımlara göre, bakış açısına bağlı olarak gelişip değişebilen bir kavramdır. Her dönem güvenlik, içinde bulunulan şartlara, kişilerin bakış açılarına göre değişim göstermektedir. Hepsinin ortak görüşüyse; güvenliğin sağlanmasıdır. Günümüzde etkisini gösteren bazı düşünceler, önemli düşünürlerin kavramlarının geçmişte kaldığı düşünülse bile, yeni kavramların oluşmasında yer tutmaktadır. Günümüzde ortaya çıkan yeni güvenlik ortamları, şartlara bağlı olarak, dönem açısından teknolojiye bağlı görünse bile, yine güvenlik önlemleri alınırken altında bu düşünceler bulunmaktadır. Ancak güvenlik yapılarındaki gelişmeler sürekliliğini korumaktadır. Güvenlik, zaman içerisinde pek çok değişim yaşamıştır. Beraberinde değişimler yenilikleri getirmiştir. Biraz daha karmaşık bir yapıya evirilmiştir. Günümüzde teknolojinin birçok alan içerisine yayılması, bazı alanlarda sınırlarının tamamen bilinen bir biçimde olmaması beraberinde yeni problemler getirmiştir. Yeni problemlerin oluşmasıysa güvenlik alanında etikler ve çalışmalara sebep olmuştur. Teknoloji güvenlik alanında ciddi bir biçimde kendini göstermiştir. Sadece ülkelerin kullandığı teknoloji ya da savunma alanında değil, farklı alanlar oluşmasına da sebep olmuştur. Özellikle son dönemlerde daha çok kullanılmaya başlayan, hem uluslararası alanda hem siyasi hem teknolojinin yardımıyla etki sağlayabilen bir siber alan ortaya çıkmıştır. Siber alanın dikkat çekici biçimde ortaya çıkmasıysa bir güvenlik alanı olarak da yer

[41] Fikret Birdişli, *Teori ve Pratikte Uluslararası Güvenlik* (Ankara: Seçkin Yayınları, Ocak 2014), 105.
[42] Beril Dedeoğlu, *Uluslararası Güvenlik ve Strateji* (İstanbul: Yeniyüzyıl yayınları, 2014), 82-83.

bulmasını sağlamıştır. Alan içerisinde uluslararası boyutta bir siber güvenlikten söz edilmektedir. Siber güvenlik genel olarak; birçok alan üzerinden incelenebilmektedir. Ancak uluslararası politika üzerinden yapılan çalışmalar, bu çalışma için daha önemlidir. Günümüzde yapılan siber güvenlik çalışmalarının temelinde siber kavramı, kendi içerisinde var olan yapıları, güvenliği ayrı bir önem taşımaktadır. Siber güvenliği anlamlandırmak için hem siber güvenliği hem yapılarını ayrı ayrı incelemek önemlidir.

1.2. SİBER GÜVENLİK NEDİR?

Güvenlik kendini yenilemekte, teknoloji ve pek çok gelişmeyle her kavram gibi kendi içerisinde yeni kavramlarla alanlar üretmektedir. Yeni ortaya çıkan kavramlardan bir tanesi; günümüzde gittikçe gelişip kendini yenileyen siber güvenliktir. Hem güvenlik alanında, hem diğer alanlarda kendini gösteren siber kavramı, beraberinde gelişen siber güvenlik oluşumu kendini gün geçtikçe daha fazla yenileyip gelişmektedir. Siber alanda yaşanan gelişmelerde en önemli parçalardan bir tanesi teknolojidir. Alan teknolojiyle beraber daha çok gelişip yenilenebilmektedir.

Gelişen teknolojiyle günümüzde hemen hemen her evde bir bilgisayar, en azından bir elektronik cihaz bulunmaktadır. Özellikle bilgisayar, cep telefonu gibi cihazların kullanımı günlük hayatta yaygınlaşmaya başladıkça, hem toplumsal değişimlere hem kolaylıklara yol açmıştır. Ancak internetin yaygınlaşması coğrafi sınırların yavaş yavaş ortadan kalkmasına sebep olmuştur.[43] İnternet kullanımı bilgisayar gibi cihazlar üzerinden, coğrafi sınırları aşan bir sistemi olmasından dolayı ayrı bir önem taşımaktadır. Siber güvenlik, kendi içerisinde bulunan internetten kaynaklı olarak belirli coğrafyaya bağlı değildir. Devlet sınırlarını aşan bir sistemi olması, siber güvenlik açısından uluslararası iş birliğini zorunlu hale getirmektedir.[44] Ancak sınırları aşan, güvenlik alanı olarak önemli bir yere sahip olmaya başlayan siber güvenliğin anlaşılması için siber kavramının açıklanması gerekmektedir.

İnternet ve bilgisayarın bağlı olduğu, teknolojinin etkisiyle kendini geliştiren siber kavramından kısaca bahsedecek olursak; daha çok bilgisayar ve

[43] Eren, *Avrupa Birliği'nin Siber Güvenlik Politikası*, 20.
[44] Salih Bıçakçı, *21. Yüzyılda Siber Güvenlik* (İstanbul: İstanbul Bilgi Üniversitesi Yayınları, Ağustos 2013), 4.

ağlarını içeren ya da ilgilendiren her yapıyı tanımlamak amacıyla kullanılmaktadır.[45] Siber sözcüğü sibernetik kelimesinin ön eki gibi durmasına karşın aralarında fark vardır. Sibernetik; kendi kendini yenileyebilen, verilen görev üzerinden hareket edebilen, başkasına ihtiyaç duymadan, yapay ve biyolojik olmak üzere iki ayrı dalda sistem kontrolü, haberleşme ve iletişim üzerinde varlığını sürdüren bir bilim dalıdır.[46]

Sibernetik günümüz anlamına yakın şekilde Norbert Weiner tarafından 1948'de "makinalarda ve hayvanlarda kontrol ve iletişim bilimi" şeklinde kullanılmıştır.[47] Sonrasında "internet ve bilgisayarla ilgili, aynı zamanda iletişim ve süreçleri kontrol etme ve yönetme" gibi bir anlam ifade ettiği görülünce tanımlamalarda farklılıklar oluşmaya başlamıştır. Başka bir kelime tanımlaması sorunu Türkçe'de siber kavramının bilişim kelimesi karşılığında kullanılabilmesi sonucu ortaya çıkmıştır. Siberle bilişim arasında farklılıklar bulunmaktadır. Bilişim, siberden öte bir anlamı işaret etmektedir. Siber kavramı daha çok bilgisayar ve bilgisayara bağlı elektronik düzeneklerin bulunduğu ortamı işaret ederken, bilişim bu ortamdan etkin şekilde faydalanmak ve ortam sayesinde bilgi üretilmesi şeklinde tanımlanmaktadır.[48]

Siberin ortaya çıkışıyla siber güvenlikten de zamanla söz edilmeye başlanmıştır. Siber güvenlik, tüm bilişim sistemlerini kapsayan genel bir güvenliktir. Siber güvenlik çoğu zaman bilgi güvenliğiyle karıştırılmaktadır. Ancak siber güvenlik, bilgi güvenliğine göre daha geniş kapsamlıdır.[49] Siber kavramının içerisinde barındırdığı tanımlamalarla siber güvenlik, hem bilgi hem o alanda kendini gösterecek birçok güvenliği kapsayan, sadece bilişim gibi yapılarla sınırlandırılamayacak bir güvenlik çeşididir. Siber alana dâhil ve bağlı olan diğer pek çok sistemi içeren bir güvenliktir. Alan kullanarak yapılan politikalar, görüşmeler de siber güvenliğin kapsamına girmektedir.

Siber anlamda güvenlik yakın tarihte hayatımıza girmiştir. Siber güvenlik çalışmaları, alanın ortaya çıkışından daha geç bir süreçte başlamıştır. Siber anlamda internette güvenlik düşüncesinin en başında ortaya atılmamasının başlıca

[45] Eren, *Avrupa Birliği'nin Siber Güvenlik Politikası*, 19.
[46] *Siber Mücadeleye Giriş* (İstanbul: Kutlu Yayınevi, Aralık 2017), 43-44.
[47] Norbert Weiner, *Cibernética E Sociedade* (Brasil: Culturix, 1968), 176.
[48] Haydar Çakmak ve Taner Altunok, *Suç, Terör ve Savaş Üçgeninde Siber Dünya* (Ankara: Barış Platin Yayınevi, Mayıs 2009), 26.
[49] Mustafa Altınkaynak, *Uygulamalı Siber Güvenlik ve Hacking* (İstanbul: Abaküs Yayınları, Mayıs 2017), 1.

sebepleri vardır. Bir tanesi; ARPANET (Advance Research Projects Agency Network) zamanında, altyapıyı kullanan sadece belirli, güvenilir birkaç araştırmacı olmasından dolayı günümüzde alınan önlemler, sonradan eklenmiş önlemlerdir.[50] ARPANET, yani internetin ilk hali ve siber alan, ilk dönemlerde güvenliğe ihtiyaç duyacak derecede dışarıya açılmamıştır. Kullanıcı sayısının belirli olması ihtiyaç oluşmamasında etkili olmuştur.

Günümüzde siber güvenliğin ortaya çıkışında pek çok etkili faktör bulunmaktadır. Siber güvenliğin bir güvenlik alanı olarak tanımlanmasında; maliyet düşüklüğü, süre kısalığı gibi faktörler bulunmaktadır. Farklı sektörleri hedefleyen siber saldırılar sonucunda devletlerin kendi siyasi ve askeri yapılanmalarının içinde bulunduğu gizli bilgilerin ortaya çıkması. Kimlik ve toplumsal yapılarla alakalı algılar oluşturulması, ülke ekonomisinin zarara uğraması, altyapının bağlı olduğu sistemlere yapılan saldırılarla beraber çevresel problemlerin kendini göstermesiyle güvenlik alanında önemli bir yeri olduğu görülmüştür.[51] Tehdidin büyüklüğü görülmeye başlandıktan sonra önlem alınma ihtiyacı duyulmuştur. Siber alan, ortaya çıktığı dönemlerde çok zarar verici bir yapıya dönüşebileceği tahmin edilmemiştir. Olası zararlı sonuçlar görüldükten ve yaşandıktan sonra bir güvenlik alanı olması gerektiği düşüncesi ortaya çıkmıştır.

Siber güvenlik; aynı zamanda bulunduğu alana göre farklı anlamlar taşıyabilmektedir. Siber güvenlik, vatandaşlar için; kendi kişisel verilerinin korunması şeklinde algılanırken, iş dünyasında işlerin devamlılığını sağlamak amaçlı kullanılan sistemlerin korunması olarak düşünülmektedir. Kamu politikasındaysa; hem vatandaşların, hem iş dünyasının, hem devletlerin kendi bilişim sistemleri ve alanla ilgili yapacakları çalışmalar için ihtiyaçları sağlamak, bunu güvenli bir şekilde yapmasını desteklemek şeklindedir.[52]

Siber güvenlik, kullanıcıların, kurum ve kuruluşların siber alandaki varlıklarının güvenliği, siber alandaki güvenlik riskleri karşısında korunaklı olmayı, bunun sürdürmesini sağlamayı amaçlamaktadır.[53] Amaçlarla birlikte

[50] Çakmak ve Altunok, *Suç, Terör ve Savaş Üçgeninde Siber Dünya*, 66.
[51] Mehmet Eren, *Avrupa Birliği'nin Siber Güvenlik Politikası* (İstanbul: Beta Yayınları, Mart 2017), 25.
[52] Hamdi Yeşilyurt, "Uluslararası Siber Güvenlik Perspektifinde Siber Güvenlik," *Siber Suçlar: Tehditler, Farkındalık ve Mücadele*, ed. Fatih Tombul vd. (Ankara: Global Politika ve Strateji Yayınları, Ocak 2015), 169.
[53] Hasan Çiftçi, *Her Yönüyle Siber Savaş* (Ankara: TÜBİTAK Popüler Bilim Kitapları, Temmuz 2017), 8.

politikalar, araçlar, güvenlik teminatları, kılavuzlar, risk yönetim yaklaşımları, teknoloji ve eğitimler beraberinde araç olarak kullanılarak faaliyetlerin tümünü kapsayan bir şekilde tanımlanmaktadır.[54] Siber güvenlik, siber tehdit ve saldırılar dışında Bilgi ve İletişim Sistemleri (BİS) bünyesinde yer alan güvenlik açıklarını en aza indirmeyi amaçlamaktadır.[55] Sadece bilgiyle sınırlı kalmayıp, kişilerin alandaki varlıklarına kadar geniş bir yelpazede bulunan siber güvenlik, pek çok alan içerisine yayılmıştır. Bilgiyi kapsamasına rağmen, hem siber güvenlik hem bilgi güvenliğini denk tutmak iki alan için de kendine ait önemli noktaların göz ardı edilmesine sebep olmaktadır.

Siber güvenlik bilgi güvenliğiyle karıştırılmamalıdır. Bilgi çok önemli bir yere sahiptir. Bilginin belirli bir karakteristiği vardır. Bilginin değeri o bilgi hakkında var olan algıyı değiştirmektedir. Böyle bir sistemde bilginin güvenliği üç temel şekilde inşa edilmiştir. Veri Bütünlüğü (Data Integrity), Süreklilik (Availability) ve Gizlilik (Confidentiality), bu üç temel parça siber güvenlikte temel prensipler şeklinde kabul edilmiştir. Ayrıca; hesap verebilirlik (accountability), kimlik doğrulama (authenticity), inkâr edememe (non-repudiation) ve anonim olma (anonymity) gibi güvenlik ilkeleri bulunmaktadır.[56]

Veri bütünlüğü; sistemde, yetkisiz biçimde fark edilemeyen değiştirmeleri önlemek anlamına gelmektedir. Süreklilik; meşru bir varlığın talebi üzerine erişilebilir, kullanılabilir olma yeteneği olup, bunu kesintisiz, erişim kaybı olmadan yapmayı niteler. Gizlilikse; bir sistemde, birey, varlık ya da süreçte, bilginin yetkisiz şekilde ortaya çıkarılmadan kullanılabilmesidir.[57] Hesap verebilirlik, kimlik doğrulama, inkâr edememe ve anonim olmaysa güvenliğin temel ilkeleri biçiminde bulunmaktadır. Bu özelliklerin herhangi birini taşımayan bilgi güvenliği, güvensizlik oluşturmaktadır.

Genel olarak siber güvenlik; siber alandaki veriler, ona bağlı olan yapılar, kurum, kuruluş ve bireyleri olası tehdit, tehlike ve riskten korumak için alınabilecek önlemler şeklindedir. Önlemleri alabilmek için; siber alanda ortaya çıkabilecek olaylar ve tehditlere ayrıca bakılması, incelenmesi siber güvenlik amaçlı uygulanacak yöntemlerde önemli rol oynamaktadır. Genel anlamda

[54] Eren, *Avrupa Birliği'nin Siber Güvenlik Politikası*, 24-25.
[55] Ahmet Naci Ünal, *Siber Güvenlik ve Elektronik Bileşenleri* (Ankara: Nobel Yayınları, 2015), 111.
[56] Yeşilyurt, "Uluslararası Siber Güvenlik Perspektifinde Siber Güvenlik," 170-171.
[57] Sebastian Klipper, *Cyber Security* (Kiel: Springer Vieweg, 2015), 12-13, E.T.: 30 Haziran 2018, DOI: 10.1007/978-3-658-11577-7.

bahsedilebilecek bir siber güvenlik sisteminde; daha önemli olan ve her şeyin ortaya çıkmış olduğu siber alan denilen yapıyı açıklamak gerekir.

1.2.1. Siber Ortam Nedir?

Siber; genel anlamda bilgisayar ve ona bağlı ağları içerir. Siber alanın bulunduğu ortama, bazı kaynaklarda siber ortam, bazı kaynaklarda siber uzay nitelemesi yapılmaktadır. Her ikisi aynı anlam gelse bile, siber ortam farklı şekillerde tanımlanmıştır. Genel olarak aynı ortamdan söz ederken, siber uzay ya da siber ortam sözcükleri kullanılmaktadır. Ancak hepsinin genel adı siber alandır. Farklı sözcük kullanımları Türkçe çevirimlerinde anlam değişimine sebep olabilmektedir. Ancak üç kullanımın da nitelediği sözcük aynı anlama gelmektedir.

Siber alan ifadesi, ilk olarak bilim kurgu yazarı William Gibson'un kitabı olan "Neuromancer"da kullanılmıştır.[58] Siber alan; "Bilginin elektromanyetik şekilde oluşturulmasıyla dünyanın her yanını çevreleyen pek çok sistem aracılığıyla bilgi erişiminin sağlandığı sanal ortamın tümü" şeklinde tanımlanmıştır.[59] Siber alandan söz edildiğinde, pek çok araştırmacı sadece internet ortamı için bu ismi uygun görse dahi, siber alan tüm bilişim kullanıcı ve sistemlerini kapsamaktadır. Genel olarak; insanların, birbirine bağlı olan bilişim sistemleri üzerinden etkileşimde bulunup, fiziksel olmadan iletişim kurdukları alan şeklinde tanımlamak mümkündür.[60] Siber alan, iletişim için paylaşılan donanım, yazılım ve protokoller aracılığıyla etkileşimi kolaylaştıran bilgisayarların ve kullanıcılarının elektronik bir bağlantısı olarak da görülebilmektedir.[61] Diğer bir tanımdaysa siber alan; bilginin kaydedilmesi, tanımlanması, iletilmesi için elektromanyetik dalgalar ve ağ merkezli sistemler kullanılmak şartıyla oluşturulan, internet gibi haberleşme ağlarını kapsayan ortam şeklindedir. Genel bir biçimde; iletişim ve bilişim ağlarını oluşturan uzay şeklinde tanımlanmaktadır.[62] Amerikan Hava Kuvvetlerindeyse; siber alan tanımlaması "fiziksel yapılar ve ağ sistemleri üzerinde verileri depolayıp, değiştirip,

[58] William Gibson, *Neuromancer* (New York: ACE Book, 2004), 4.
[59] Çakmak ve Altunok, *Suç, Terör ve Savaş Üçgeninde Siber Dünya*, 27.
[60] Bıçakçı, *21. Yüzyılda Siber Güvenlik*, 10.
[61] Donald G. Janelle ve David C. Hodge, "Information, Place, Cyberspace, and Accessibility," içinde *Information, Place, and Cyberspace: Issues in Accessibility*, ed. Donald G. Janelle ve David C. Hodge (ABD: Springer, 2000), 4.
[62] Bayraktar, *Siber Savaş ve Ulusal Güvenlik Stratejisi*, 13.

geliştirmek amacıyla elektronik ve elektromanyetik dalgaların kullanılması" şeklinde yapılmıştır.[63]

Siber alan; bilgisayarlar, bilgisayarların onunla alakalı araçları, verilerin depo edildiği cihazlar, elektromanyetik ve iletişim sistemlerinden oluşmaktadır. Siber alanda fiziksel araçlar kullanılmış olsa da vurgu daha çok sanal ortama yapılmakta, ancak tüm söz edilenler siber alanın sadece bir parçasıdır. Siber alan kısaca; verilerin depo edildiği, bu verilere uzaktan erişim sağlanabildiği, iletişimi kolay hale getiren ağ ve bilgisayar sistemlerinin hepsinin bir arada olduğu sanal ortamdır.[64] Teknik anlamdaysa; siber alan, yazılım (işletim sistemleri, uygulama yazılımları gibi), donanım (sunucular, dizüstü bilgisayarlar gibi), iletişim altyapısını (uydu sistemleri, kablolu/kablosuz iletişim ağları gibi) kapsayan bir ortam şeklindedir.[65] Siber alan, oluşumuyla beraber zaman, mekân kavramlarında değişiklik olmuş, fiziksel uzaklık, bilgi aktarımı için gereken zaman internet ortamında kısalmıştır.[66]

Genel anlamda siber alan; siber anlamda kapsanabilecek her şeydir. Yani; siber alan hem alanın kendisini içine alabilirken, alanda bulunan kişileri, onların verilerini, yapılan iletişimlerini, hatta aracı olan interneti kapsamaktadır. Ancak alan kendi içerisinde belirli yapılara ayrılmaktadır. Tek bir bütün olarak bir alandır. Ancak kendi içyapıları ayrı önemli özelliklere sahiptir.

Siber alanın en önemli yapısı; ağ yani network'tür. Genel olarak ağ; birden çok bilgisayarın kendi aralarında veri paylaşımı yapabilmesi amacıyla kurulmuş, iletişimsel yapıdır.[67] Farklı herhangi iki cihaz IP (Internet Protocol- İnternet Protokolü) adresine sahipse, aralarında mesafe olsa dahi yönlendiricilerle haberleşme sağlayabilirler.[68] Pek çok üretici bilgisayar ve cihazların kendi aralarında haberleşme sağlayabilmesi için OSI (Open Source Interconnection- Açık Kaynak Ara Bağlantısı) katmanlarını hazırlamıştır. Katmanlar; fiziksel, veri bağlantı, ağ, nakil, oturum, sunum, uygulama katmanı şeklinde ayrılmıştır.[69]

---

[63] Çakmak ve Altunok, *Suç, Terör ve Savaş Üçgeninde Siber Dünya*, 27.
[64] Çakmak ve Altunok, *Suç, Terör ve Savaş Üçgeninde Siber Dünya*, 27-28.
[65] Çiftçi, *Her Yönüyle Siber Savaş*, 5.
[66] Bıçakçı, *21. Yüzyılda Siber Güvenlik*, 3.
[67] M. Alparslan Akyıldız, *Uygulamalarla Siber Güvenliğe Giriş* (Ankara: Gazi Kitabevi, Ağustos 2015), 31.
[68] Altınkaynak, *Uygulamalı Siber Güvenlik ve Hacking*, 187.
[69] Akyıldız, *Uygulamalarla Siber Güvenliğe Giriş*, 31.

Katmanlardan fiziksel olanı; fiziksel dünyada kullanılan donanım sayesinde, teknoloji kullanılarak, bilgisayarda işlemci (central processing unit), ana kart (main board) gibi ünitelerden oluşmaktadır. Ayrıca kablolar, Ethernet kartı, ağların iletişimi amacıyla yönlendirici (router) gibi ekipmanlarla siber uzay oluşturulabilmektedir.[70] Fiziksel katman 1 ve 0 sinyallerinin taşındığı katmandır. Katmanın görevi; dijital sinyali taşımak, sinyaller zayıfladığı anda durumu güçlendirerek yeniden üretmekle tekrarlayıcı biçimde çalışmaktır. Veri bağlantı katmanı; ağ içerisinde iletişimi sağlarken, katmanda ağ anahtarı cihazı görev yapmakta, ağ anahtarı, ağ içerisinde iletişimi frame'leri (çerçeve) kullanarak sağlamaktadır. Ağ katmanında; ağlar arasındaki iletişimin sağlanması görevini yaparken, burada yönlendirme cihazı (router) görev yaparak farklı ağları birbirine bağlamaktadır. Burada ARP (Address Resolution Protocol- Adres Çözümleme Protokolü), ICMP (Internet Control Management Protocol- İnternet Kontrol Mesajı Protokolü), IP (Internet Protocol- İnternet Protokolü) protokolleri görev yapmaktadır.[71]

Nakil katmanı; uçtan uca iletişimi sağlayabilen katman olarak geçmektedir.[72] Port[73], ağ servislerinin bağlantı kurabilmesi için sistem üzerinde açılması gereken sanal iletişim noktalarını sağlayarak, TCP (Tranmission Control Protocol- Geçiş Kontrol Protokolü) ve UDP (User Datagram Protocol- Kullanıcı Datagram Protokolü)'nin kullanıldığı katmandır. Oturum katmanı; iki bilgisayar arasında oturum açılıp, devam ettirilip, kapatılmasından sorumlu olan katmandır. SMB-Server Message Block/Sunucu İleti Bloğu (Dosya paylaşımları için kullanılır.), NFS-Near Field Communication/Yakın Alan İletişimi (Ağ Dosya Sistemi, ağda birden fazla bilgisayar üzerinde bulunan çeşitli dosyaların tek bilgisayardaymış gibi kullanılmasına olanak sağlayan protokoldür.) burada çalışmaktadır. Sunum katmanıysa; verinin esasen formatının belirlenmiş olduğu katman olup, veriyi şifreleme, sıkıştırma işlemi burada yapılmaktadır. Uygulama katmanında uygulamalar beraberinde FTP, HTTP, HTTPS, DNS, TELNET, SSH gibi pek çok protokol burada çalışmaktadır.[74]

[70] Bıçakçı, *21. Yüzyılda Siber Güvenlik*, 11.
[71] Akyıldız, *Uygulamalarla Siber Güvenliğe Giriş*, 31-32.
[72] Akyıldız, *Uygulamalarla Siber Güvenliğe Giriş*, 33.
[73] Fiziksel olarak cihazda kablonun takılması gereken yer, sanalda ise bilgisayarın veri alışverişinde kullandığı sanal kapı olarak düşünülebilmektedir. Ayrıntılı Bilgi için bkz.: Onur Aktaş, *Siber Güvenlik: Hacking Atölyesi* (Ankara: Gazi Kitabevi, Ağustos 2017), 41.
[74] Akyıldız, *Uygulamalarla Siber Güvenliğe Giriş*, 33-34.

Ağdan bahsettikten sonra, var olan önemli internet protokollerinden kısaca söz etmek gerekir. Belirli bir verinin ağ üzerinden bırakılarak, paketlenip, iletim şeklinin belirlenmesi, bunun iletilmesi aşamasının tümünü denetleyen kuralların tamamına ağ (network) protokolleri denmektedir.[75]

Protokollerden en çok bilinenleri; IP ve TCP/IP protokolüdür. TCP/IP (Geçiş Kontrol Protokolü/ İnternet Protokolü) protokolü, çoğu yerde beraber kullanılmış olsa da farklı iki ağ protokolü olmaktadır. [76] Orijinal TCP/IP protokol paketi, ilk başta donanıma dayalı dört yazılım katmanı olarak tanımlanmış, ancak günümde beş katmanlı bir model olarak düşünülmeye başlanmıştır.[77] Güvenlik açısından bir çözüm şeklinde 1980'de oluşturulmuştur.[78] TCP/IP'nin temelde tasarım amacı; ağlar arasındaki iletişim ağını kurmak, aynı zamanda internet olarak adlandırılan, heterojen fiziksel ağlar üzerinden evrensel iletişim hizmetleri sağlayabilen bir bağlantı kurmaktır. Bu şekilde büyük bir coğrafi alanda, farklı ağlardaki ana bilgisayarlar arasında iletişimi sağlamak, bu protokolle gerçekleştirilebilmektedir.[79] Sınırları aşan bir iletişim bağlantı noktası bu protokolle hayatımıza girmiştir. Günümüzde hâlâ etkisini göstermeye devam etmektedir.

Günümüzde ayrıca en çok karşılaştığımız protokollerden bir tanesi; Http/Https (Hiper Text Transfer Protocol- Hiper Metin Aktarma Protokolü) olmaktadır. Özellikle internetin bağlı olduğu bir bilgisayarda, arama motorunda olası bir web sayfasına girdiğimizde, adresin başında görme ihtimalimizin en yüksek olduğu http/https olmaktadır. Http/Https ortak kullanıma açık olup, bir kaynaktan dağıtılmakta olan hiper-ortam enformasyon sistemleri kullanılan iletişim kuralı olmakta, Https aynı protokolün şifreli biçimi olarak kullanılmaktadır.[80] Protokoller genel anlamda tarayıcılar tarafından temsil edilen kullanıcı arabiriminin altında bulunan ağlar, sunucular ya da istekleri işleyen "motorlara" taşıyan, çeşitli ortamları yinelemekte olan yapılardır. Bilinen kullanımı Tim Berners-Lee tarafından 1990-1993 yılları arasında

[75] Altınkaynak, *Uygulamalı Siber Güvenlik ve Hacking*, 197.
[76] Altınkaynak, *Uygulamalı Siber Güvenlik ve Hacking*, 197.
[77] Behrouz A. Forouzan, *TCP/IP Protocol Suite* (New York: The McGraw-Hill Companies, 2010), 28.
[78] Altınkaynak, *Uygulamalı Siber Güvenlik ve Hacking*, 197.
[79] Lydia Parziale vd., *TCP/IP Tutorial and Technical Overview* (Amerika Birleşik Devletleri: IBM/Redbooks, Aralık 2006), 4, E.T.: 3 Temmuz 2018, url: https://www.redbooks.ibm.com/pubs/pdfs/redbooks/gg243376.pdf.
[80] Akyıldız, *Uygulamalarla Siber Güvenliğe Giriş*, 38.

İsviçre/Cenevre'deki Avrupa Nükleer Araştırma Merkezi olan CERN(Conseil Européen pour la Recherche Nucléaire)'de uygulanmıştır.[81]

DNS (Domain Name System- Alan Adı Sistemi) protokolü bilgisayar isimlerini IP adresleri olarak çözümlemek amacıyla kullanılmaktadır. ICMP (Internet Control Management Protocol- İnternet Kontrol Mesajı Protokolü) temel bir ağ protokolü olmakla beraber yönetim durumundan çok, ağa bağlı cihazlarda, kendi durumlarında hata ve kontrol amaçlı mesajlar gönderilmesi için kullanılmaktadır.[82]

SMTP (Simple Mail Transfer Protocol- Elektronik Posta Gönderme Protokolü) Protokolü, e-postaların aktarılma sürecini denetlerken, SNMP(Simple Network Management Protocol- Basit Ağ Yönetim Protokolü) protokolü, var olan ağ cihazlarının arasında bulunan bağlantıların sağlanması kısmında görevlidir, burada ağ cihazları uzaktan incelenebilmektedir. FTP (File Transfer Protocol- Dosya Aktarım Protokolü) Protokolü; bir bilgisayardan herhangi bir bilgisayara gönderilen veri aktarımını gerçekleştiren protokol olup, dosya aktarımının temelini oluşturmaktadır.[83] SSH (Secure Shell- Güvenli Kabuk) uzakta bulunan bir makineye bağlanabilmesi, o cihazda komut çalıştırılmasına yarayan protokoldür.[84]

TELNET (Telecommunication Network- İletişim Ağı) veri iletişimini şifresiz şekilde, çok güvenli olmayan, uzakta olan bir makineyle bağlantı kurularak, cihazda komut çalıştırılmasını sağlanan protokoldür. VPN (Virtual Private Network- Sanal Özel Ağ); uzakta olan bir ağa, sanki orada fiziksel bir bağlantı yapılmış gibi, o ağ içinde var olan bir bilgisayar görünümünde, şifreli veri aktarımı kullanılan bir bağlantı yapılmasını sağlar.[85] Güvenlik Duvarı (Firewall); dış ağlarla yerel ağ arasında temel olarak iletişimin güvenliğini sağlamaktadır.[86] Belirli kurallar üzerinden gelebilecek saldırı trafiğini engellemek amaçlı yazılımsal ve donanımsal şekilde olan bir yapıdır.[87]

---

[81] John Yannakopoulos, *HyperText Transfer Protocol: A Short Course* (Yunanistan, Ağustos 2003), 1-2, E.T.: 3 Temmuz 2018, url: http://condor.depaul.edu/dmumaugh/readings/handouts/SE435/HTTP/http.pdf.
[82] Altınkaynak, *Uygulamalı Siber Güvenlik ve Hacking*, 198.
[83] Altınkaynak, *Uygulamalı Siber Güvenlik ve Hacking*, 199.
[84] Akyıldız, *Uygulamalarla Siber Güvenliğe Giriş*, 38.
[85] Akyıldız, *Uygulamalarla Siber Güvenliğe Giriş*, 38-39.
[86] Altınkaynak, *Uygulamalı Siber Güvenlik ve Hacking*, 191.
[87] Akyıldız, *Uygulamalarla Siber Güvenliğe Giriş*, 39.

Genel olarak siber alan; bilgisayar ve bağlı olduğu ortamların neredeyse tümünü kapsayan bir yapı olarak tanımlanmaktadır. Ağı kullanan ya da alana bağlı olan kişilerle cihazları kapsadığı bilinmektedir. Alanın fiziksel olarak bilgisayar ve sistemlerini kapsaması, sadece teknolojiyle alakalı gibi görünmesini, dijital olarak sanal alanı kapsamasıysa sadece internet ortamını kapsaması gibi yanlış anlaşılmalara yol açabilmektedir. Önemli nokta; iki alanın bir arada olduğu bu ortamı parçalar halinde değil, bir bütün olarak anlamak gerekliliğidir. Siber alanı sadece bir bilgisayar sistemi ya da internet olarak sınırlamak yanlış olacaktır. Çünkü kapsadığı yapılar çeşitlidir. Siber alandan söz ederken önemli yapılarından bir tanesi olan internetten söz etmek gerekir. Pek çok protokolden söz ederken bunların internetle bağlantılı olduğu bilinmektedir. Bir iletişim ve bunun doğru yapılabilmesini sağlamak adına hazırlanan protokoller, internet üzerinde etkisini göstermektedir. İnternetin anlaşılması siber alanın daha iyi kavranmasını sağlayacaktır. İnternetin daha iyi anlaşılabilmesi için kısaca tarihsel altyapısı ve gelişiminden söz edilmelidir.

1.2.2. İnternetin Gelişimi ve Kısaca Tarihsel Altyapısı

Çağımızda en çok kullanılan, hatta yokluğu bazı alanlarda sorun oluşturan en önemli yapılardan biri internettir. Bir yüz yıl öncesinde, insanların örneğin; bir ülkeden başka bir ülkeye iletişimi günler, hatta aylar sürerken, günümüzde internet sayesinde sadece saniyeler sürmektedir. İnternet, özellikle iletişim açısından olumlu, aynı zamanda büyük bir kolaylık sağlamıştır. Her önemli yapının içerisinde onun avantajları dışında dezavantajlarını kullananlar vardır. Her teknolojik yapı gibi açıklıkları bulunan internetin geçmişten günümüze var olan yapısını genel olarak incelemek, sorunların nereden geliştiğini anlamakta yardımcı olacaktır.

Günümüzde kullandığımız internetin temeli çok derinlere dayanmaktadır. İnternetin ilk kullanımı iletişimle başlar. Bir iletişim kurmak için ihtiyaçlar karşısında internet ortaya çıkmıştır. Yapılan ilk çalışmalar interneti bulmak amacıyla olmasa dahi, gelişmesi, evrimleşmesi açısından büyük adımlar atılmasına sebep olmuştur.

İnternetin ortaya çıkışından günümüze kadar hayatın her alanına yayıldığı bilinmektedir. Her alanda, o işin işleyişine yarayan altyapılar vardır. Günümüzde enerji dağıtımı altyapıları, banka altyapıları, telefon hatları, hastane sistemleri,

telefon sistemleri gibi önemli sistem ve hizmetlerin neredeyse tümü internetin altyapısını kullanmaktadır.[88] Yani; kullanmış olduğumuz pek çok önemli altyapı sistemi internet sayesinde rahatlıkla iletişim içerisindedir.

Altyapıların bağlı olduğu internetin ortaya çıkışı, başta yavaş bir biçimde olmuştur. Ancak gelişimi beklenenden hızlı sürmüştür. İlk internet kullanım; dört farklı bilgisayarın birbirine bağlanması şeklinde olmuş, bunlar; UC Santa Barbara, Stanford, UCLA ve Utah Üniversitelerinde gerçekleşmiştir.[89]

İnternetin, günümüzde kullanılan cihazlar içerisinde ilk kullanım alanlarından bir tanesi bilgisayarlar olmuştur. İlk bilgisayarı üreten kesin bir biçimde söylenememektedir. Ancak gerçek makine şeklinde bilgisayar denileceklerden bir tanesi IBM (International Business Machines- Uluslararası İş Makineleri) ve Harvard ortaklığıyla, mermi yolu hesaplamak amaçlı yapılmıştır. Yapılan makine 1944'te ABD'de ilk programlanabilme özelliğine sahip, ancak tamamen elektronik olmayan 'Harvard Mark 1' bilgisayarıdır.[90] Başka bir bilgisayar denilebilecek makineyse; İkinci Dünya Savaşı döneminde 'Colossus' isimli küçük bir oda boyutundaki kriptografik (Şifreli Yazı) kodları çözmek amacıyla yapılmış, İngiltere Bletchley Park'taki genel amaçlı, ancak yeniden programlanabilme özellikli elektronik cihazdır.[91]

Bilgisayar ve teknolojilerin ilerlemesiyle internet duraksamadan gelişmeye devam etmiştir. Cihaz ve sistem olarak ilerleme gösteren internet hâlâ gelişmelerine devam etmektedir. İlerlemeler dışında kendi içerisindeki temel yapılarında gelişmeler ve yeni ortaya çıkan yapılar olmuştur.

İnternetin temel kavramları vardır. En önemlilerinden biri; ağdır. İnternetin teknolojik unsuru ağın ortaya çıkışı; ilk yıllarda, ana bilgisayara tek bilgisayarın erişimi söz konusuyken, iki bilgisayarın aynı anda erişimi ortaya çıkınca, bunun için gerekli işlemci ve iletişim protokollerinin gelişmesiyle olmuştur. İlerleyen süreçlerde ortaya çıkan protokoller (FTP ve TCP) sayesinde pek çok kullanıcı, sunucu bilgisayara bağlanabilmektedir. Günümüzde kullanmakta olduğumuz telsiz iletişim teknolojileri (tabletler ve akıllı telefonlar

[88] Akyıldız, *Uygulamalarla Siber Güvenliğe Giriş*, 1.
[89] Richard A. Clarke ve Robert K. Knake, *Siber* Savaş, Çev.: Murat Erduran (İstanbul: İstanbul Kültür Üniversitesi Yayınları, 2010), 47.
[90] "IBM's ASCC Introduction," *IBM*, E.T.: 3 Ağustos 2019, url: https://www.ibm.com/ibm/history/exhibits/markI/markI_intro.html.
[91] Jack Copeland, "Introduction," içinde *Colossus: The Secrets of Bletchley Park's Codebreaking Computers*, ed. Jack Copeland (New York: Oxford University Press, 2006), 1-2.

gibi) beraberinde geniş bir alana yayılmış, ağ teknolojisinin önemi gün geçtikçe artmıştır.[92]

İnternet, bilgisayar ve iletişime daha çok önem katmıştır. Dünyanın her köşesine hızlıca yayın imkânı sağlamış, yayın imkânıyla bilgi aktarımını kolaylaştırmıştır. Kişiler ve bilgisayarlar aracılığıyla coğrafi konumun önemsizleşmeye başlayarak rahatça iş birliği, daha önemlisi karşılıklı iletişimin kolaylaşmasında önemli bir araç olmuştur.[93] İnternet zamanla bilgisayar ve iletişimle kısıtlanamayacak kadar yayılmaya ve gelişmeler göstermeye başlamıştır. Günümüzde yeniliklere devam etmekte ve birçok alanda kendini göstermektedir.

İnternetin gelişimi hâlâ devam etmektedir. Genel anlamda ortaya çıkışının yakın tarihte olduğu düşüncesi yaygındır. Aslında daha öncelerinden temeli atılmıştır. Yeni ortaya çıktığı düşünülen alanın esasında ilk çıkışının biraz daha uzak tarihlerde olduğu bilinmektedir. Ancak pek çok alanda kendini ciddi bir konumda göstererek, incelenmeye başlanması yakın tarihte olduğu için bu görüş daha yaygındır.

İnternetin ilk ortaya çıkışı, iletişim ihtiyacıyla olmuştur. Ancak bilgisayarların gelişerek buna izin verecek teknoloji ortaya çıkmaya başlayınca, bunun üzerine çalışmalar yapılmıştır. Bilgisayarın gelişimi sayesinde yapılan çalışmalar sonucu, 7 Şubat 1958 yılında 5105.15 Direktifiyle, kitle iletişim teknolojileri ve bilgisayar bağlantıları araştırmalarına odaklanmış ABD Savunma Bakanlığı İleri Araştırma Projesi Ajansı-US Department of Defence's Advanced Research Project Agency (DoD-ARPA) kurulmuştur.[94] ARPA'nın ortaya çıkışında, özellikle gelişiminin devletler seviyesinde hızlanması, Soğuk Savaş Dönemi'nde olmuştur. 4 Ekim 1957 yılında, dünya yörüngesine gönderilen ilk yapay uydunun SSCB (Sovyet Sosyalist Cumhuriyetler Birliği) tarafından yerleştirmesi, 3 Kasım'da Sputnik II'nin uzaya gönderilmesi, ABD'nin atağa geçmesine sebep olmuştur. 1958 yılında ABD rekabet gücüne katkı sağlamak amaçlı İleri Araştırma Projeleri Ajansı (Advanced Research Projects Agency-ARPA)'nı kurmuştur. Projenin kapsamı; ABD'nin milli güvenliğiyle, her daldan bilim insanını uzay araştırmaları ve savunmada pek çok konu üzerinde çalışmaları

[92] Bıçakçı, *21. Yüzyılda Siber Güvenlik*, 2.
[93] Çakmak ve Altunok, *Suç, Terör ve Savaş Üçgeninde Siber Dünya*, 61.
[94] "ARPA Is Born," DARPA, E.T.: 4 Ağustos 2019, url: https://www.darpa.mil/about-us/timeline/dod-establishes-arpa.

için bir araya getirmektir.[95] Teknolojik gelişmelerle ARPA ilk bilgisayara yönelik çalışmalara başlamıştır. İşlemcilerin, çoklu kullanıcıların sisteme girebileceği kapasitede olmaması, işlemlerin yavaş ilerlemesine sebep olmuştur. Bu işlemlerin yavaşlığından sonra çalışmalara katkı sağlayabilmesi için; bilim insanları tek ağdan girebilmek amaçlı teknik altyapıyı kurmuştur. 1958 yılında kurulmuş olan NASA (Ulusal Havacılık ve Uzay Dairesi - National Aeronautics and Space Administration)'nın gerekli araştırma grubunu oluşturmak amaçlı 1962 yılında İleri Araştırma Projeleri Ajansı Ağı (ARPANET) ortamı hazırlamıştır.[96] Organizasyon iletişim teknolojilerini bir iletişim aracı olarak kullanabilme durumuna odaklanmıştır. 1962 yılında, Joseph Carl Robnett Licklider'ın "Galaktik Ağ" adı verilen, günümüz internetine benzer, küresel biçimde birbirine bağlı ilk sürümü şeklinde söz edilebilecek bu sistem tartışılmaya başlamıştır.[97]

1968 yılında DARPA, bazı projelerini özel sektör yerine araştırma üniversitelerine geçirmek için ihale yapmıştır. Önemli projelerinden biri olan veri 'paketleri'nin transferi sistemi isimli ARPANET projesi bunun içerisinde olmuştur. 1972 yılında ARPANET halka tanıtılmıştır. 1981 yılında ilk internet protokolü oluşturulmuş, bilgi etkin olarak iletilmeye başlanmış, ortak bilgisayar dilinin kullanılması sağlanmıştır. Sonraki 18 yıl; hizmet kurumları, e-posta ve haber grupları gibi bağlantıları kendi içine alma, hatta sınırlı uluslararası iletişimi büyümeye başlamıştır. Ancak ARPANET kurumsal iletişim ağı olarak görevine devam etmiştir.[98]

Füze Krizi ve SSCB'nin ilerlemeleri yeni konular ortaya çıkmıştır. Nükleer saldırı sonucu iletişim hatlarının daha az etkilenerek çalıştırılmasını sağlamak konulardan biri olmuştur. Bunun üzerinde Paul Baran 'Herhangi olası fiziksel saldırı sonrası geriye kalan en büyük grupla elektrik bağlantısı kurularak' iletişimi devam ettirebilecek bir ağ yapısından söz etmiştir.[99] Birçok yeni düzenlemeyle 1970'li yıllarda internetin esas temeli olan, askeri niteliğe sahip ARPANET çalışmalarda bulunmuştur. ABD'nin müttefiki olan devletlerin ağ

[95] Bıçakçı, *21. Yüzyılda Siber Güvenlik*, 5-6.
[96] Bıçakçı, *21. Yüzyılda Siber Güvenlik*, 6.
[97] Leonard J. Waks, *Education 2.0: The LearningWeb Revolution and the Transformation of the School* (ABD: Paradigm Publishers, 2013), 73.
[98] Çakmak ve Altunok, *Suç, Terör ve Savaş Üçgeninde Siber Dünya*, 62-63.
[99] Paul Baran, "On Distributed Communication Networks," (Kaliforniya: The RAND Corporation, Eylül 1962), 2, E.T.: 4 Ağustos 2019, url: https://www.rand.org/content/dam/rand/pubs/papers/2005/P2626.pdf.

sistemleri; Fransa'nın 'Cyclades' isimli araştırma ağı, İngiltere'nin ticari ağı olan Ulusal Fizik Laboratuvarı (National Physical Laboratory)'na bağlı ağıyla birleşerek internetin (International Network of Computer Networks- Bilgisayar Ağlarının Uluslararası Ağı) yani uluslararası bilgisayar ağları şeklinde ilk oluşumunun tohumları atılmıştır.[100] Genel anlamda günümüzde birbirine bağlı, devletlerin arasındaki iletişimin sağlanabildiği, temeli ARPANET ile atılmış olan internet yapısı bu dönemde ortaya çıkmaya başlamıştır.

ARPANET'in genel protokolleri; güvensiz, açık ve esnektir. Sistemin amacı bilgiyi kolayca paylaşmak, ağda olan kimsenin de bir gizlilik isteğinde bulunmamış olmasıdır.[101] Sistemdeki teknolojik gelişmeler ve bu durumlar yaşanırken, siber anlamda güvenlik açısından ilk problemler yaşanmıştır. 1971 yılında ARPA'nın ortaklarından BBN Technologies'in çalışanı Bob Thomas, yazdığı program olan, ilk kendini çoğaltma (self-replicating) özelliğine sahip programı -adını Creeper koymuşlardır- bilgisayara yüklenmiştir. ARPANET'te kısa bir sürede yayılan programı Reaper isimli bir programla düzeltilmeye çalışmışlardır.[102] 1988'de "The Morris Worm", isimli programı, adını aldığı Robert T. Morris yazmıştır. Amacı bir bilgisayara bağlanıp, kendini başka bir bilgisayara kopyalayabilecek çeşitli açıklıklar bulup, bunları kullanabilmektir. ARPANET üzerinde bulunan bilgisayarların yüzde onunu bu şekilde çalışamaz duruma getirmiştir.[103] İlk zamanlar güvenliğe ihtiyaç duyulmamasının sonuçları olarak bu problemleri görmek mümkündür. İlk başta bilgi paylaşımı olarak görünen sistem, amacının dışına çıkmak için uzak bir tarihi beklememiştir. Kısa bir süre içerisinde sorunların ortaya çıkması belirli çalışmaları yanında getirmiştir. Ancak yine tam bir çözüm bulunamamış olması günümüzdeki problemlerin meydana gelmesine zemin hazırlamıştır.

Siber alanda güvenliğe ihtiyaç duyulmaya başlanmasıyla bazı adımlar atılmıştır. Günümüzde kullandığımız; internet kullanımı kolaylaştırmak amacıyla TCP protokolü gibi protokoller geliştirilmeye başlanmıştır. 1970'li yıllardaysa önemli iki olay ortaya çıkmıştır. 26 Mart 1976 yılında İngiltere Kraliçesi II. Elizabeth; ilk elektronik postayı Kraliyet Sinyal ve Radar Kurumu'ndan atmıştır.

[100] Bıçakçı, *21. Yüzyılda Siber Güvenlik*, 6.
[101] Sait Yılmaz ve Olay Salcan *Siber Uzay'da Güvenlik ve Türkiye* (İstanbul: Milenyum Yayınları, Şubat 2008), 35.
[102] Bıçakçı, *21. Yüzyılda Siber Güvenlik,* 7.
[103] Yılmaz ve Salcan *Siber Uzay'da Güvenlik ve Türkiye*, 36.

İletişimi farklı bir seviyeye çıkartmıştır. O dönemde internetin dosya paylaşım ve haberleşme özelliğinden belirli sayıda kişi faydalanabildiği için 1970 yılında önemli bir proje olan DIY-Do it Yourself (Kendin Yap) ile ilk kişisel bilgisayarlar ortaya çıkmıştır.[104] 1975 yılında kişisel bilgisayarlar ortaya çıktığından itibaren, Altair 8800 pek çok evde yer almıştır. Aynı yılın Eylül ayında piyasaya sürülen IBM 5100 beraberinde hem bilgisayarlar hem de ağ kültürü, kullanıcılarıyla aynı oranda artmıştır.[105] Teknolojik gelişmelerle alanda ilerlemeler artmaya başlamıştır. Artık bilgisayarlar yavaş yavaş evlere girmiştir. Bilgisayarların evlere girişiyse internetin yayılmasını hızlandırmıştır. Çünkü internetin en yaygın kullanım alanı bilgisayarlardır.

1980ler sonrası bilgisayarlar ve ağ katılımları artmıştır. ARPANET ve ağ kullanıcıları dolaylı şekilde gerçek dünyayı etkileyecek dijital bir alan oluşturmuştur. Alan genişlediği için güvenlik teorisinde geçen risk, internet üzerinden tartışılmaya başlanmıştır. Ağa yönelebilecek tehdit ve tehlikeler ortaya çıkarak, sistem, kullanıcı müdahalelerine açık bir konuma gelmiştir. 1982 yılında, ABD Savunma Bakanlığı, tehditlerin ARPANET üzerinde artmasıyla, askeri veriler için ayrı bir ağ kurma düşüncesine geçmiştir. 1982 yılında MILNET ve ARPANET isimli iki farklı ağ ortaya çıkmıştır. MILNET askeri amaçlı, ARPANET sivil araştırmalar amaçlı kullanıma geçmiştir.[106] ARPANET biraz daha geride kalmaya başlamıştır. İki farklı ağ şeklinde dönüşüm yaşayan ağlar, sonucunda yine ARPANET'teki yavaşlamaya çözüm olamamıştır. Teknoloji ilerledikçe, internet kullanımı artmıştır. Sadece birkaç bilgisayarın iletişimini sağlamak amaçlı kurulmuş olan ARPANET, artık daha fazla ağa bağlanan kullanıcıyı kaldırma konusunda sorunlar yaşamaya başlamıştır.

ARPANET yavaşlamaya başladıktan sonra, 1990'da NSFNET (National Science Foundation Network – Ulusal Bilim Vakfı Ağı) gibi ağların kurulmasıyla tüm yük ARPANET'den alınıp buraya devredilerek, ARPANET'in işlevine son verilmiştir. Aynı yıl belirli protokollerin yardımıyla bilginin erişimini kolaylaştıracak gelişmeler yaşanmıştır.[107] Bu olay World Wide Web (Dünya Çapında Ağ)'in CERN (European Organization for Nuclear Research)'de çalışan Tim Bernes-Lee tarafından 1989 yılında ortaya atılmasını, 1993 yılında kamuda

[104] Bıçakçı, *21. Yüzyılda Siber Güvenlik*, 7.
[105] Bıçakçı, *21. Yüzyılda Siber Güvenlik*, 8.
[106] Bıçakçı, *21. Yüzyılda Siber Güvenlik*, 9-10.
[107] Bıçakçı, *21. Yüzyılda Siber Güvenlik*, 26.

kullanıma açılmasını ve internetin günümüz formuna ulaşmasını kapsamaktadır.[108] Tim Bernes-Lee'nin programı tamamlayıp kullanıma geçirmesi 1992 yılında olmuştur.[109] Aynı yıl, günümüzde kullandığımız internet, hiper metin transfer protokolü (Hyper-Text Transfer Protocol- HTTP) başlatılıştır. Ayrıca HTML-Hyper-Text Markup Language (Hiper Metin İşaretleme Dili) başlatılması, URL -Uniform Resource Locator (Tekdüzen Kaynak Bulucu) kurulması, Netscape ve İnternet Explorer isimli internet tarayıcı sistemlerinin kurulması büyük ölçüde ilerlemeler kaydedildiğini göstermektedir.[110] 1993 yılında kullanımına başlanan tarayıcı sistemlerinin temelinde MOSAIC isimli yazılım bulunmakla beraber bir yıl sonrasında Netscape firmasına ait olan Navigator isimli tarayıcı daha çok kullanılmıştır.[111] 1995 yılındaysa Internet Explorer'ın var olan ilk sürümü kullanıma sunulmuştur.[112] ARPANET'in üzerindeki yük alındıktan sonra internetin geliştirilmesi üzerine çalışmalar daha rahatlamıştır. Gelişmeler sayesinde günümüzde kullanıma sunulan yapı artık genel olarak ortaya çıkmıştır. Yenilenerek kullanıma devam edilen siber alandaki yapılara yeni sürümler eklenmiş ya da yerine daha gelişmiş biçimleri geçmiştir. Teknoloji açısından eski olarak bahsedilen sürüm ve yapılardan bazıları internetin tarihi içerisinde geçerek, kullanılmayan eski sürümler olarak bahsedilmeye başlanmıştır. Aynı tarihlerde, kullanmış olduğumuz, internet için önemli, ancak, bizlerin dikkatini çekmeyen önemli gelişmelerin yaşandığı da bilinmektedir.

Veri miktarı arttıkça bunları bir araya getirme amaçlı çalışmalar başlamıştır. Alan Adı Sistemi-Domain Name System (DNS) ve diğer teknik çözümlerle internet protokolleri numaralı şekilden isimlere dönüşmüştür. Halk Savunma Veri Ağı (Defense Data Network) İletişim Bilgi Merkezi (Network Information Center) sayesinde ".org, .gov" gibi, savunma dışında tüm kayıt hizmetleri sağlanmıştır. 1992 yılında savunma haricinde ABD Savunma Bakanlığı internet desteğini sivillere teslim etmiştir. 1998 yılında IP adres yönetimi ve alan adları için Kaliforniya Marina Del Rey'de merkezi bulunan İnternet Tahsisli

[108] "The Birth of the Web," CERN, E.T.: 4 Ağustos 2019, url: https://home.cern/science/computing/birth-web.
[109] Brian Winston, *Media, Technology and Society: A History From the Telegraph to the Internet* (New York: Routledge, 1998), 333.
[110] Çakmak ve Altunok, *Suç, Terör ve Savaş Üçgeninde Siber Dünya*, 63.
[111] Özgür Aslan ve Selcen Öner, "İnternet Ekonomisi," *İletişim Dergisi* 26 (Ocak 2006): 10, E.T.: 6 Temmuz 2018, url: http://dergipark.gov.tr/download/article-file/212226.
[112] Hüseyin Cem Köylü, "Dünden Bugüne Internet Explorer," *Chip,* 5 Nisan 2012, E.T.: 6 Temmuz 2018, url: https://www.chip.com.tr/haber/dunden-bugune-internet-explorer_32928.html.

Sayılar ve İsimler Kurumu- International Corporation for Assigned Names and Numbers (ICANN) kurulmuştur.[113] ICANN'in amacı; internetin sorunsuz çalışmasını sağlamaktır. Ayrıca teknik görevleri yerine getirmek, politik anlamda uzlaşmacı olmaktır.[114] 2000'li yıllardan sonra da günümüzde kullanılan sistemler daha hızlı ortaya çıkmıştır.

Günümüze yakın dönemde, internetin gelişimiyle bahsedilecek başka bir yapılanma daha ortaya çıkmıştır. Deep Web (Derin Ağ), aynı zamanda Dark Web (Karanlık Ağ) diye adlandırılan yapılanma, internetin arama motorlarında kolayca bulunamayan bölümüdür. Bazı araştırmacılara göre; internetin yüzde doksanını Deep Web oluşturmaktadır.[115] Deep Web genellikle, herkesin kullandığı internette ulaşılamayacak, zararlı pek çok içeriğe sahiptir. Silah satışı, uyuşturucu madde satışı, para aklama örgütleri, hassas bilgilerin sızdırılması gibi örnekler mevcuttur. İçerikleri saklamak için özel yöntemlerle sadece bu siteleri kullanmalarına izin verilenlerin giriş yapabileceği bir sistem halinde kullanılmaktadır.[116] Karanlık bir ortam olmasından alan bu şekilde adlandırılmıştır.[117] Teknolojik gelişmelerle paralel olarak ortaya çıkmış deep web, internetin tamamını kullanamadığımız, görünenden farklı bir sistem olduğunun kanıtıdır. İnterneti gördüğümüz kadar düşünürsek yanılmış oluruz. İnternet tamamen teknolojik olup, sınırları olmamasından her şeye açıktır.

Genel olarak; internetin oluşumu sistemler aracılığıyla, iletişimin ihtiyacı sonucu ortaya çıkmıştır. Tarihi açıdan çok kısa sürede ortaya çıkmış gibi görünse dahi, çok büyük gelişmelerle, düşünülenden daha uzak bir tarihte çalışmalarına başlanmıştır. İnternet, ilk başlarda farklı amaçlarla oluşmaya başlamıştır. Günümüze avantaj ve dezavantajları beraber gelmiş bir yapıdır. Her yaştan ve çevreden kullanıcısı vardır. Bir kısmı kişisel amaçlarla, bir kısmı kurumsal amaçlarla kullanmaktadır. İnternetin ilk yıllarında, güvenlikle beraber oluşmamış olması zarara karşı açıklıkları yanında getirmiştir. Boşluklardan yararlanıp, interneti farklı amaçlarla kullanan belirli bir grup günümüzde mevcuttur. Bu grup

[113] Çakmak ve Altunok, *Suç, Terör ve Savaş Üçgeninde Siber Dünya*, 64.
[114] Sash Jayawardane vd., "Cyber Governance: Challenges, Solutions, and Lesson for Effective Global Governance," *Policy Brief* 17 (Kasım 2015): 6, E.T. : 6 Temmuz 2018, url: http://www.thehagueinstituteforglobaljustice.org/wp-content/uploads/2015/12/PB17-Cyber-Governance.pdf.
[115] Alper Başaran, *Siber Savaş Cephesinden Notlar* (İstanbul: Arion Yayınevi, Mayıs 2016), 115.
[116] Başaran, *Siber Savaş Cephesinden Notlar*, 115-116.
[117] Altınkaynak, *Uygulamalı Siber Güvenlik ve Hacking*, 3.

hackerlardır. Hackerları anlamaksa bazı konulara açıklık getirmede yardımcı olacaktır.

1.2.3. Hackerlar Kimlerdir?

İnternet, kullanıcıların kendi aralarında iletişim sağlayabildikleri bir ortamdır. Kullanıcı olarak çeşitli kişilerin bağlandığı bilinmektedir. Günümüzde kullanıcı olarak bağlantı kuranlar; her kesimden ve her yaş grubundandır. Amaçları kişilerin kullanım biçimine göre değişmektedir. Dikkat çekici kullanıcılardan bir tanesiyse; hackerlardır. Hackerlar internet ortamında en çok duyulan kullanıcılardandır. Hack, hacker, hacktivist (Eylemci hacker) ayrı ayrı tanımlanması gereken kavramlardır. Her birinin anlamı, yeri ayrıyken, birbiriyle de bağlantılıdır. İnternet ortamında önemli bir yer taşıyan hacker ve ona bağlı kavramlardan bahsetmek bazı konuları anlamlandırmak açısından önemlidir.

Hack, siber güvenlikte bir açıklığı kullanmak biçiminde tanımlanır.[118] Hackin ilk ortaya çıkışı; ABD'de MIT (Massachusetts Institute of Technology-Massachusetts Teknoloji Enstitüsü)'de üniversite öğrencileri tarafından yapılan bir şaka olarak, tanımlama açısından teknik bir tesisi kandırmak şeklinde olmuştur.[119] Kelimenin MIT'de ikinci bir anlamı daha vardır. Başarılı şekilde yapılan yapılandırmalar, çözümlemeler anlamına gelmektedir.[120] Ancak bilgisayarlarla ilişkilendirilince ilk anlamını kaybetmeye başlamıştır. Bir şakayla ortaya çıkan hack kavramı, zamanla değişerek günümüzde kullanılan, kırmak anlamına yaklaşmıştır. İnternet ortamında, bir veriye erişmek amaçlı güvenliğin kırılması anlamına gelmiştir.

Hacker kelimesi Türkçe'de bilişim korsanı, siber korsan şeklinde geçerken birebir aynı anlama gelmemektedir. Genel anlamada bilişim alanında oldukça yetenekli, bilgili kişiler şeklinde söz edilmektedir.[121] Hackerlar kendi içlerinde üç gruba ayrılırlar. Siyah şapkalılar; politik, finansal ya da kişisel nedenlerle,

[118] Altınkaynak, *Uygulamalı Siber Güvenlik ve Hacking*, 1.

[119] Waldemar Vogelgesang, Rainer Winter and Thomas A. Wetzstein, *Auf digitalen Pfaden Die Kulturen von Hackern, Programmierern, Crackern und Spielern* (Leverkusen: Westdeutscher Verlag, 1991), 153, E.T.: 7 Temmuz 2018, ISBN 978-3-322-92485-8.

[120] Gökşin Akdeniz, "Hacker Etiği," *Hack Kültürü ve Hacktivism: Yeni bir Siyaset Biçimi, Mustafa Akgül'e Armağan,* der. Ali Rıza Keleş ve Yetkin Sal (İstanbul: Alternatif Bilişim Yayınları, Temmuz 2013), 10, E.T.: 27 Mart 2017, url.: https://ekitap.alternatifbilisim.org/files/hack-kulturu-ve-hacktivizm.pdf.

[121] Atalay Keleştemur, *Siber İstihbarat* (İstanbul: Level Kitap, Ağustos 2015), 209.

bilgisini sistemlere zarar vermek amaçlı kullanabilen kişilerdir. Beyaz şapkalılar zıt şekilde; bilgi ve yeteneğini sistem güvenliği amaçlı kullanan, güvenlik uzmanı şeklinde adlandırılabilen, kanunlara uyan kişilerdir. Gri şapkalılar, hem siyah hem beyaz şapkalılar gibi yeri geldiğinde davranışlarını gösterebilen hackerlardır.[122] Hackerlar kötü ya da iyi amaçlar uğruna davranışlar gösteren kişiler diye kesin sınırlamalar içerisine koyulmadan önce, var olan ayrımlara, tepki ve durum değerlendirmesine göre karar vermek gerekir. Ancak tanımlara baktıktan sonra yargıda bulunmak daha doğru olacaktır.

Hacker kavramı üzerine birçok tanımlama ve varsayım vardır. 1960'larda unvan olarak hacker; en hızlı, iyi, akıllı bilgisayar programı yazmak şeklindeydi.[123] Yakın dönemlerde bir tanımda hackerlar için; kendini sınamak amaçlı bilgisayarla uğraşmakta olan kişi denilmektedir. Başka bir tanımda; sistemlerin detaylarını bilmek isteyen, öğrenmeyi seven, herhangi bir sistemde herkesin yapılabileceği şeylerden çok sistemin en üst düzeyde kapasitesini öğrenip, onu zorlamayı seven kişiler olarak bahsedilmektedir.[124] Günümüzdeyse hacker felsefesinin motivasyonlarında farklılaşmalar olmuştur. Ağ ya da bilgisayar sistemlerine zarar veren kişiler için daha farklı isimlendirmeler yapılmaya başlanmıştır. Hackerler yeni yöntem ve yollar ortaya koyma amacında olmuş, ancak kendilerinden ayrılan gruplara farklı isimler verilmiştir. Bunlardan biri Cracker'lardır. Bilgisayarlardaki güvenlik kontrollerini kendi amaçları uğruna, suç sayesinde aşan kişiler olarak tanımlanır.[125] Crackerlar güvenliği kesip, devre dışı bırakabilen, niyetleri kötü, amaçları suç olan kişisel ya da bir kurumun rakipleri için çalışan kişiler olmaktadır.[126] Hackerlar kendi aralarında gruplar ve isimler olarak farklılaşmaktadır. Farklılıklardan dolayı; hackerlar tamamen pozitif ya da negatif olarak tanımlanamamaktadır. İçinde bulunulan durum, olay, olayın bir suç teşkil edip etmemesi hackerların tanımlanmasında etkilidir.

1980'li yıllarda ABD'de hacker felsefesi yayılmaya başlamıştır. Bunun yayılmasında pek çok sebep vardı. Bu dönemde hacker felsefesinin üst seviyeye çıkmasında 'War Games' isimli filmin önemli rolü bulunmaktadır. Dönem

[122] Akyıldız, *Uygulamalarla Siber Güvenliğe Giriş*,1-2.
[123] KURGAN, *Siber Mücadeleye Giriş* (İstanbul: Kutlu Yayınevi, Ocak 2018), 38.
[124] Bıçakçı, *21. Yüzyılda Siber Güvenlik*, 20.
[125] Bıçakçı, *21. Yüzyılda Siber Güvenlik,* 24-25.
[126] Solange Ghernaouti, *Cyber Power: Crime, Conflict and Security in Cyberspace* (Switzerland: EPFL Press, 2013), 190.

içerisinde önemli olan; ortaya çıkan hacker felsefesidir. Hacker felsefesinin altı temel şartı vardır.[127] Dünyanın işleyişi hakkında bir şeyler öğretecek her şeye bilgisayardan erişim sınırsız olmalıdır. Tüm bilgiler bedava olmalıdır. Otoriteye güvenmeyerek, âdemi merkeziyetçiliği teşvikle, bilgi erişiminde engel olmadan, açık sistem biçiminde bir sistem olmalıdır. Hackerların kendi yaptıkları eylemler üzerinden değerlendirilmesi gerekmekte, cinsiyet, ırk gibi kriterlerle değerlendirilmemesi gerekmektedir. Bilgisayarda sanat ve güzellik yapılabileceği düşüncesi vardır. Hackerlar ellerindeki araçları kendileri için iyi ve kullanışlı hale getirerek yazdıkları yazılım ya da programı bir sanat eseri gibi görmektedir. Bilgisayarların hayatı daha iyi bir halde değiştireceği düşüncesi vardır.[128] Genel olarak düşüncelerin altında; sınırlı bir kullanım yerine bir şeyleri öğrenmek için sınırsız bir erişim, ücretsiz, açık olunması, hatta kimseye bağlı olmayacak bir ortam olması yatmaktadır. Hackerlar değerlendirilirken, yaptıkları işlerin bir sanat olarak değerlendirilmesi, kendileri değil, yaptıkları iş üzerinden söz edilmesi gerektiğinden bahseder. Bilgisayarı kullanırken, hayatı iyi yönde değiştirme düşüncesiyle hareket ederler. Ancak, bu felsefe zamanla değişime uğramıştır. Hackerlar için bu felsefe, sonradan çıkanların temelini oluşturduğu için önemli bir yerdedir. Ancak bazı amaçlar farklı yönde dönüşmüştür. Felsefelerde dahi değişiklikler olduğu söylenmekte, kişiye göre düşünceler, bakış açıları değişebilecek bir gerçeklik olmaktadır. Birine göre iyi olan başkası için olumsuzdur.

Hackerların kendi düşünce ve eylemleri vardır. Hackerların bir kısmının bir araya gelerek oluşturdukları, kendi düşünceleriyle belirli eylemler yapan grupları bulunmaktadır. Belirli eylemlerde bulunan hackerlara hactivist (eylemci hacker) denir. Hacktivistler; politik, toplumsal ya da kendilerine yanlış görünen sorunları, sistemlere saldırmak aracılığıyla dikkat çekmeye çalışan kişilerdir.[129] Bir amaç için, hizmet olarak ya da mesaj vermek yoluyla siber suç işleyen kişilerdir. Kendilerini tanımlayan belirli ana özellikleri bulunmaktadır. Asgari düzeyde suç eğilimli, küçük gruplar ya da yalnız eyleme geçen, belirli bir mizah yoluyla gösteren ve siyasi amaçları olan kişi ya da kişilerdir.[130] Hacktivism;

[127] Salih Bıçakçı, *21. Yüzyılda Siber Güvenlik* (İstanbul: İstanbul Bilgi Üniversitesi Yayınları, Ağustos 2013), 19-21.
[128] Steven Levy, *Hackers: Heroes of the Computer Revolution* (America: O'Rielly, 2010), 28-34.
[129] Altınkaynak, *Uygulamalı Siber Güvenlik ve Hacking*, 2.
[130] Başaran, *Siber Savaş Cephesinden Notlar*, 42.

toplumsal ya da siyasi değişim için, bir çeşit şiddet olmaksızın, hukuksal anlamda tartışmalı, siber protesto vesilesiyle direnme ya da öncü olma fikridir.[131] Hactivistler genel olarak; kendileri için ya da o anda bir sıkıntı, problem olarak gördükleri durumları, bildikleri ortam olan internet ve bilgisayarlar aracılığıyla, belirli kişi ya da kişilerin dikkatlerini çekebilmek amacıyla çalışmalar yapan kişilerdir.

Hack ve felsefesinin ortaya çıkışıyla altyapının kuruluşu ABD'de olmaktadır. Bu ortaya çıkış sebebiyle başlarda en çok etkilenen devletlerden biri yine kendisi olmuştur. ABD için dönüm noktası olan pek çok hacker olmasına karşın bunlardan ikisi zamanında daha önemli yer tutmuştur.

Kevin Mitnick, tüm dünyada bilinen en büyük bilgisayar hackerıdır. ABD'deki şirket bilgilerini gizlice kopyalamış, daha ciddi olarak Amerika Ulusal Güvenlik sistemini çökertmiştir.[132] 1970-80 ve 90'lı yıllarda hackerlık yapan Mitnick, ABD için büyük bir sorun olmuştur. Yıllar sonra kendi güvenlik danışmanlık firmasını (Mitnick Security Consulting) açmıştır.[133] Kevin Mitnick dünyanın en ünlü hackeri, aynı zamanda en iyi siber güvenlik konuşmacısıdır. FBI tarafından en çok arananlarından biri olmuştur. Meydan okumak için 40 büyük şirkete saldırmış, ancak günümüzde hükümetler için güvenilir bir güvenlik danışmanı olmuştur.[134] Diğer önemli hacker; Jonathan James'tir. 16 yaşındayken, 1.7 milyon Amerikan doları maliyetinde yazılımı, NASA'nın kendi bilgisayar sisteminden indirmiştir. Savunma Bakanlığı'na yerleştirmiş olduğu küçük bir programla ordunun bütün mesajlarını okuyabilmiştir.[135] Yaptığı bu hackerlıkla beraber, hackerlıktan dolayı ceza alan ilk çocuk hacker olmuştur. Hackerlıkla dünya çapında bir tehdit oluşturmasa da ABD'yi maddi açıdan bir zarara uğratmış olması yaptığının suç sayılmasına neden olmuştur.[136] Bir çok hacker, pek çok önemli olay yaşatmıştır. Ancak, iki hackerın özellikleri dikkat çekicidir.

---

[131] P. W. Singer ve Allan Friedman *Siber Güvenlik ve Siber Savaş*, Çev. Ali Atav (Ankara: Buzdağı Yayınevi, Mart 2015), 112.
[132] Çakmak ve Altunok, *Suç, Terör ve Savaş Üçgeninde Siber Dünya*, 89.
[133] Roger A. Grimes, *Hacking the Hacker: Learn From the Experts Who Take Down Hackers* (Kanada: Wiley Yayınları, 2017), 33.
[134] "About Kevin Mitnick: CEO, Team Leader, and Chief White Hat Hacker," Mitnick Security Consulting, E.T.: 9 Temmuz 2018, url: https://www.mitnicksecurity.com/about/kevin-mitnick-worlds-most-famous-hacker-biography.
[135] Çakmak ve Altunok, *Suç, Terör ve Savaş Üçgeninde Siber Dünya*, 89.
[136] David Stout, "Youth Sentenced in Government Hacking Case," *The New York Times*, 23 Eylül 2000, E.T.: 9 Temmuz 2018, url.: https://www.nytimes.com/2000/09/23/us/youth-sentenced-in-government-hacking-case.html.

Hackerlar ve eylemleri açısından yapılmış olan ilk politik eylemden ayrıca bahsetmek gerekir. Meksika'da, 12 Ekim 1998'de, hükümetin web sitesi hacklenmiş, American Electronic Disturbance Theater- Amerikan Elektronik Karışıklık Tiyatrosu (EDT) bunu gerçekleştirmiştir.[137] Hackerların amacı, dönemin Meksika başkanı Erenesto Zedolli'nin web sitesine saldırarak, tüm dünya ve batı yarımkürede yüzyıllardır süren soykırım, sömürgecilik ve ırkçılığa karşı yapılan direnişin devam ettiğini göstermektir.[138]

Hackerlar genel anlamda; belirli amaçlar doğrultusunda, kendileri için yanlış olan ya da tüm toplum için problemli görünene dikkat çekmekten, kişisel çıkarlara kadar geniş bir yelpazede eylemlerde bulunmaktadır. Yapılan eylemlerle yapılma biçimi, siber alandaki yeniliklerle gelen açıklıkların, sadece biraz uğraşla ortaya çıkarabileceği eylemlerin birer örneğidir. Hackerlar alanda sadece kendi istekleriyle kendilerini geliştirmiştir. Alana hâkim kişilerdir. Her kişi kendini siber alanda geliştirerek, hemen hemen yakın bir kapasiteye ulaşabilecektir. Belirli kapasitelere ulaşan, olumsuz davranış sergileyen kişilerse siber anlamda önemli tehditlere yol açabilecek konuma gelmektedir. Kişilerin yol açacakları dışında, genel anlamda tehditleri incelemekse pek çok açıdan siber alandaki tehditlere açıklık getirecektir.

1.2.4. Siber Alandaki Önemli Tehditler Nelerdir?

Siber alandaki yeni gelişmelerle, teknoloji sayesinde birçok tehdit zamanla kendini göstermeye başlamıştır. Tehditleri iki bölümde incelemek mümkündür. Bilgisayar ortamındaki tehditler ve siber alandaki stratejik tehditler olmak üzere ikiye ayrılabilir. Genel anlamda; tehditleri, bilgisayar ortamındaki virüsler gibi insan yapımı program, yazılımlar olarak ayırmak mümkündür. Ayrıca stratejik olarak; yapılabilecek belirli planlar, hatta davranış, planlı eylemler şeklinde düşünülebilmektedir. Siber savaşlar gibi tehditleri stratejik olarak düşünmek mümkündür. Ancak siber anlamda savaş, terör gibi konuları ayrı incelemekte fayda vardır.

Bir devletin kendi güvenliğine yönelik tehditler, geleneksel anlamda iç ve dış olarak ayırılır. İç tehditler olarak suç ve terör sayılabilirken, dış tehditte

[137] Çakmak, Altunok, *Suç, Terör ve Savaş Üçgeninde Siber Dünya,* 89.
[138] Kenneth Einar Himma, *Internet Security: Hacking, Counterhacking, and Society* (America: Jones and Bartlett Yayınevi, 2007), 64.

savaştan bahsetmek mümkündür. Konu siber alan olduğundaysa daha farklı değerlendirmek gerekir. Siber tehditleri, siber alanda, iç ve dış olarak sınıflandırma imkânı çok düşüktür. Çünkü siber saldırıların belirli bir sınırı yoktur. Uluslararası boyutu olmayan, ancak yine siber saldırı olarak adlandırılabilen saldırılar olduğu için bir sınırı olmadığı söylenebilir.[139] Aynı zamanda tehditlerin sınırlı bir alanı kapsamıyor oluşu –sadece ağ uzmanları ya da bilgisayar mühendislerinin çözeceği teknik problemler olmayışı- hem çözümler açısından hem verilebilecek tepkiler açısından farklılıklar oluşturabilmekte, gelişmelerle zaman, mekân bağıntısı değişime uğramaktadır. [140]

Siber alanın, uluslararası ilişkilerde tüm aktörlere sunduğu en büyük kolaylık ve potansiyel tehditlerin sebebi; coğrafi olarak sınırların büyük ölçüde anlamını yitirmesine sebep olmasıdır.[141] Zaman ve bilgi aktarımında sürenin kısalması, ekonomik, askeri, politik alanlarda kullanılmaya başlanmasına sebep olmuştur.[142] Tehlikesiyse; yeterli bilgisi olan herkesin, nereden olursa olsun, bilgisayar ya da sisteme ulaşarak, saldırısını gerçekleştirebilme şansı olmasıdır. Yapılan çalışmalarla, kritik tesislerin ağ bağlantılarına dışarıdan ulaşma şansını düşürmeye çalışılsa dahi, tamamen başarmak çok zordur.[143] Siber tehditler, kolaylıkla ortaya çıkıp, alanlara göre, uygulanan saldırı biçimine göre farklı adlandırılabilecek biçimdedir. Bunun için belirli tanımlamalar yapıldığı bilinmektedir.

Siber tehditlerin genel bir tanımlamasını yapmak, anlaşılması açısından gereklidir. Siber tehditler; siber ortamda, bilginin ifşa edilmesi, bozulması ya da erişilebilirliğinin kesilmesi gibi istek dışı durumların ortaya çıkma potansiyeli şeklinde bahsedilebilir. Ayrıca iletişim ve bilgi teknolojilerinden faydalanarak, imkânları suç için araç yapıp, klasik suçların siber ortama uyarlanmış şekilde tehdit olarak sayılmasını kapsamaktadır.[144] Siber problemlerin en başında; saldırganların saldırabilmek için ihtiyacı olan teknolojinin, gelişmişlik açısından mevcut, yeterli, temini kolay olması gelmektedir.[145] Siber tehditlerin ortaya

[139] Çakmak ve Altunok, *Suç, Terör ve Savaş Üçgeninde Siber Dünya*, 24.
[140] Bıçakçı, *21. Yüzyılda Siber Güvenlik*, 3.
[141] Çakmak ve Altunok, *Suç, Terör ve Savaş Üçgeninde Siber Dünya*, 29.
[142] Bıçakçı, *21. Yüzyılda Siber Güvenlik*, 3.
[143] Çakmak ve Altunok, *Suç, Terör ve Savaş Üçgeninde Siber Dünya,* 29.
[144] Bayraktar, *Siber Savaş ve Ulusal Güvenlik Stratejisi*, 14.
[145] Yılmaz ve Salcan, *Siber Uzay'da Güvenlik ve Türkiye*, 43.

çıkmasına sebep üç boyut vardır. İnternet tasarımındaki zafiyetler, yazılım ve donanım hataları, kritik sistemlere çevrimiçi erişim imkânıdır.[146]

İnternetin kendi içerisinde beş önemli zafiyeti bulunduğu düşünülmektedir. Adresleme sistemiyle tarayıcılarda açılan adreslerin, kendi taşındıkları bağlantılarda, herhangi bir açık bulunarak rahatça sızılabilmesiyle kolaylıkla bir hacker tarafından farklı bir adrese yönlendirilebilmeyi sağlayabilmektedir. Belirli bir yönetişim olmayışı, yani; yapıyı kimsenin kontrol etmediği, pek çok devlet arasında, sivil toplum kuruluşlarının internetin yönetişim kısmında rol oynadığı için belirli zafiyetler açığa çıktığı bir başka zafiyet çeşididir. Tüm iletişim sisteminin herkese açık, yayımlanan her içeriğin neredeyse şifresiz şekilde dışarıya açık olması farklı bir zafiyettir. Zararlı yazılımların kontrolü olmadan kolayca internet ortamında dolaşabilmesidir. Güvenlik yerine daha çok kimsenin hâkimiyetinde olmayacak, merkezi kontrolü yok etmek amaçlı büyük bir internet altyapısı olmasıdır.[147] Zafiyetler sayesinde alan saldırıya açıktır. Savunmasız biçimde kalan zafiyetler, ciddi boyutta tehditlerin ortaya çıkmasına sebep olmaktadır.

Siber tehditler genel olarak; siber ortamdaki boşlukların belirli kişiler ya da gruplar tarafından olumsuz amaçlar için kullanılma, kullanılabilme ihtimalini kapsamaktadır. Tehditler zamanla tehlikeye dönüşebilmektedir. Tehditlerin icraata geçmiş halleri genellikle büyük tehdit ya da direkt tehlikeler ortaya çıkartabilmektedir.

Siber anlamda, bilgisayarlar üzerinden gelebilecek tehditler, genellikle var olan ya da hazırlanan biçimdedir. Tehditler donanım ya da yazılımları kapsamaktadır. Ancak stratejik anlamda planlanmış, eyleme geçirilmiş, belirli amaçları olan suç, terör ya da savaş tipi eylemleri de içermektedir. Siber istihbaratsa stratejik anlamda siber alanda uygulanan hem güvenlik hem toplanılan taraf açısından tehdit amaçlı olmaktadır.

Siber suç; sistemin sahibinin rızası olmadan, kişinin sitemine yetkisiz giriş, bilgisayar verisine izinsiz erişim, hatta yok edilmesi, değiştirilmesidir. Başka noktaysa; bilgisayar ve ağ sistemleri, yine bilgisayar ve ağ sistemleri tarafından saldırıya uğrayarak suç işlenmektedir.[148] Farklı bir tanımdaysa; siber ortamda

[146] Çiftçi, *Her Yönüyle Siber Savaş*, 300.
[147] Clarke ve Knake, *Siber* Savaş, 45-46.
[148] Çakmak ve Altunok, *Suç, Terör ve Savaş Üçgeninde Siber Dünya*, 34.

işlenen suçlar, yeni teknolojiler ve internetle, klasik suçların bu ortamda gelişerek ortaya çıkan yeni suçlarla bu kapsama girmesi şeklindedir.[149] Genel olarak siber suç; siber alan üzerinden işlenebilen, alanı kapsayarak ortaya çıkabilen, kanunlar üzerinden suç olarak sayılan pek çok durumu içermektedir. Savaş ve terör gibi büyük tehditleri kapsamasıysa tartışmalıdır.

Siber suçlardan söz ederken savaş ve terörden daha farklı söz edilmelidir. Siber suçlar dışında, siber alandaki tehditlerden önemlilerinden bir tanesi siber terördür. Siber suçlardan siber terörizmi ayıran önemli özelliklerden biri; eylemin siyasal bir neden taşımasıdır.[150] Siber suçlar genellikle ufak, bireysel suçları kapsayabilecek, daha az insan grubuna zarar verebilecek biçimdedir. Siber terörü suçtan ayırmak için en önemli nokta, içerisinde siyasallık barındırıp barındırmadığıdır.

Siber savaş kısaca; uluslararası alandaki savaş tanımından farklı olarak, siber barbarlıktan, gerçek anlamda siber araçlardan faydalanılarak oluşan savaşa kadar geniş bir yelpazededir.[151] Siber savaş, geleneksel savaş ve çatışmada olduğu gibi, siber güvenlik ve tehdit ortamının en uç noktasındadır.[152] Ciddi boyutlarda görülebilecek siber savaşa uluslararası alanda dikkat edilmelidir. Siber savaştan bahsederken aynı zamanda istihbarattan da bahsedilmelidir.

Siber alanda önemli konulardan birisi de siber istihbarattır. Siber istihbarat, yani, siber casusluk; ekonomik, askeri, kişisel, politik anlamda, avantaj için, bilgisayar ve iletişim ağlarına yasadışı girilip, rakiplerden (devlet, kişi ya da grup) sırlarını izinsiz elde etmektir.[153]

Genel olarak; siber alanda tehditler iki genel başlıktadır. Bilgisayar ortamı ve stratejik biçimde karşımıza çıkabilecek tehditler siber alanda söz edilen esas iki tehdit biçimidir. Siber alanda açıklıklar[154] pek çok tehdit ya da tehlike ortaya çıkarabilmektedir. Her tehlike gibi bunu savunabilmek ya da önüne geçebilmek için önlemler alınmalıdır. Teknik bir biçimde ortaya çıkabilecek tehditler tek başına bir tehdit olarak görülebilirken, stratejik tehditler için de temel oluşturur.

[149] Bayraktar, *Siber Savaş ve Ulusal Güvenlik Stratejisi*, 14.
[150] Çakmak ve Altunok, *Suç, Terör ve Savaş Üçgeninde Siber Dünya*, 41.
[151] Singer ve Friedman *Siber Güvenlik ve Siber Savaş*, 164.
[152] Julian Richards, *Cyber War* (ABD: Palgrave MacMillan, 2014), 5.
[153] Çiftçi, *Her Yönüyle Siber Savaş*, 9.
[154] Açıklık; sistem, uygulamalar ve ağları tehlikeye sokabilen, genelde beklenmeyen ya da istenilmeyen zayıflık veya uygulama hatası olarak geçmektedir. Devamı için Bkz.: Yılmaz ve Salcan, *Siber Uzay'da Güvenlik ve Türkiye*, 63.

Stratejik anlamda siber tehditler; ortaya çıkmış tehditlerin amaçlar üzerinden doğru bir biçimde kullanılmasıdır. Teknik anlamda ortaya çıkan tehditleri bilgisayar ortamındaki tehditler biçiminde adlandırmak tanımlamaya yardımcı olacaktır. Çünkü temelde neyin yattığını bilerek hareket etmek önemlidir. Tek başına bir tehdit oluşturabilecek bilgisayar ortamını kapsan suçlar ve tehditler de bulunmaktadır. Bunu sadece stratejik alan için bir temel olarak görmek de hata olacaktır. İyi anlaşılabilmesi içinse bilgisayar ortamındaki tehditlerden öncelikli olarak söz edilmelidir.

1.2.4.1. Bilgisayar Ortamındaki Tehditler

Siber alandan bahsedildiğinde, fiziksel olarak ilk akla gelen bilgisayar ve bağlı olduğu ortamlardır. Fiziksel ortamda belirli yazılımsal ve donanımsal tehditler vardır. Tehditler, daha çok sistemin yapısına zarar verebilecek tehditler olduğundan bilgisayar ortamındaki tehditler şeklinde söz edilir. Her tehdidin getirdiği olumsuz sonuçlar vardır. Olumsuz sonuçlar alana zarar verebilecek her boyuttadır. Zararlı yazılımların verebileceği hasar içerisinde ilk akla gelen ekonomik boyutlardır. Ancak sistem içerisinde bulunan verilerin, o veri sahipleri için güvenlik sorunu oluşturması, ortamdaki problem ve tehditlerin başlarında gelmektedir.[155]

Genel anlamda; donanım ve yazılım tehditleri birbirini etkileyebilecek tehditlerdir. Bilgisayar ortamında genellikle yazılımsal tehditler daha ön plana çıkar. İkisi de bilgisayar ve ağlara bağlı olduğu için, genel zarar; bilgisayara, kendi iç sistemine, kullanıcılara olur. Donanım üzerine genelde teknik tehditler vardır. Ancak hem donanım hem yazılım birbirini etkileyebilecek yapılardır. Donanımsal yapılar; bilgisayara yerleştirilen parçalar, yazılımsal yapılarsa; kodlar sayesinde oluşturulabilen programları kapsamaktadır.[156] Genel anlamda esas tehdit oluşturan yazılım üzerindendir.

Donanımsal olarak; bilgisayarlarda ilk akla gelen tehditlerden biri mikro chip (Mikro yonga)'dir. Aygıtların esas çalışmasına yarayan bütünleşmiş devreler olup, savunmasız olmaları, sistemlere kolayca girerek tehlikeye sebep olabileceğini gösterir. Bir kahve makinesinden, bir savaş jetine uzanan yelpazede

[155] KURGAN, *Siber Mücadeleye Giriş*, 113.
[156] Keleştemur, *Siber İstihbarat*, 204-205.

sonuçlar çok tehlikeli boyutlara çıkmaktadır.[157] Elektronik bir cihazın sistemine girilmesi, cihazın tehdit gibi görünmemesine karşın, girildiği anda sonucu tehlikelidir. Sistemsel problemlerse yazılımlarla bağlantılı sorunları oluşturmaktadır.

Yazılım açısından birçok tehdit vardır. En bilinenlerinden bir tanesi; DOS (Denial of Services- Servis Dışı Bırakma)'dur. Bir grup saldırgan tarafından, başka yerlerden yapılan saldırı şeklineyse DDOS (Distributed Denial of Service- Dağınık Servis Dışı Bırakma) denir. Saldırının amacı; hizmet veren sunucu bilgisayarın hizmet veremez hale gelmesi ya da fazlasıyla yavaşlayıp verdiği hizmetin anlamlı olmayacak hale gelmesidir. Önemli bir amacıysa; sunucu bilgisayarın kendi ağ kaynaklarını tüketmektir.[158] Sistemin kesilmesi, bir bilgisayarın sabit diskini imha etmek kadar ciddi veya sistemin tüm mevcut belleğini kullanmak kadar basit biçimde olabilir.[159] DOS/DDOS atakları hedef sistemin erişilebilirliğini engellemektedir. Hedef cihaza sürekli paketler göndererek CPU(Central Process Unit- Merkezi İşlem Birimi) değerlerini arttırıp, doluluğu sağlayarak devre dışı kalması ya da yavaşlamasına sebep olur.[160] Saldırılarda başarılı olabilmelerindeki sebeplerden bazıları; CPU yani; işlemci gücünün fazla olmaması, altyapının tasarımının düzgün olmayışı ya da hafızanın dolu olmasıdır.[161] DDOS saldırılarında; merkez bir sistemden, zombi bilgisayarlar adı verilen bilgisayarlarla, en son kullanan kişilerin bilgisayarlarına bulaştırılan zararlı yazılımlarla kontrolü ele alınır. Uzaktan zararlı amaçlar için kullanılan, kontrol edilebilen bilgisayarlar, verilen bir komutla, zombi bilgisayarların üretmiş olduğu paketlerle hedef bilgisayara saldırıp erişimi engeller.[162] DOS denilen saldırılar; hedef alınan sistemin cevap veremeyeceği sayıda istek üretmesi denilebilir. Bu sayede cevap üretemez, yeni istek alamayacağı için hizmet veremeyecek hale gelir.[163] Sistem içerisinde en büyük problemse; sistemin hizmet

[157] P. W. Singer, "Saklanacak Yer Yok," *Popular Science* 35 (2015): 72.
[158] Bıçakçı, *21. Yüzyılda Siber Güvenlik*, 39.
[159] Joseph Migga Kizza, *Computer Network Security and Cyber Ethics* (ABD: McFarland & Company, Inc., Publishers, 2014), 71.
[160] Akyıldız, *Uygulamalarla Siber Güvenliğe Giriş*, 251.
[161] Ahmet Ünal, "Dağıtık Servis Dışı Bırakma (DDOS) Saldırıları: Güncel Yöntemler ve Mücadele," *Siber Suçlar: Tehditler, Farkındalık ve Mücadele*, ed. Fatih Tombul vd. (Ankara: Global Politika ve Strateji Yayınları, Ocak 2015), 15.
[162] Akyıldız, *Uygulamalarla Siber Güvenliğe Giriş*, 251.
[163] Altınkaynak, *Uygulamalı Siber Güvenlik ve Hacking*, 199.

verememesidir. DOS ve DDOS saldırılarıysa bunu en rahat başarabilen saldırılardır.

DOS saldırı tipi bir hacking yöntemi olarak birebir geçmez, çünkü saldırı kaynağı engellenerek problem giderilebilir. Ancak DDOS pek çok sistem kullanıldığı için, engellenmesi daha zor, saldıranın kim olduğunu bilmek imkânsız denecek kadar problemlidir.[164] Bu saldırıların yapıldığı yerler daha çok e-ticaret siteleridir. Çünkü ticaret yapan sitelerin, internet alışveriş sisteminin aksaması, zarara uğramalarına sebep olur.[165] Bu saldırıların bir siber savaş aracı olarak kullanıldığı ilk yerse; 25 Nisan 2007 yılında Estonya Hükümeti'nde olmuştur. Hükümet, İkinci Dünya Savaşı'nda hayatını kaybetmiş Rus askerlerini anma amaçlı yapılan anıtı farklı bir yere taşıma kararı sonrasında, devletin internet altyapısı DDoS saldırılarıyla felç olmuştur.[166] Günümüzde de sık kullanılan saldırının tercih edilme sebebi; gerçekleştirmesi kolay, kimin yaptığının öğrenilmesiyse zor olmasıdır.[167] Genel anlamda; DOS ve DDOS saldırıları, bilgisayar sistemlerinin hizmet veremez hale gelecek kadar dolu görünmesini sağlayacak şeklide bilgisayara yükleme yapmaktadır. Bu saldırının iki çeşit görünmesinin sebebi; DOS'un tek bir yerden olup, DDOS'un çoklu bir saldırı olmasıdır. Kullanımının kolay oluşuysa en çok tercih edilen saldırılardan bir tanesi olmasının sebeplerindendir. Günümüzde e-ticaret sitelerinin yaygın kullanılması, bu saldırılara uğrayabilecek pek çok site olduğunu göstermektedir. Kullanım alanı olarak pek çok sistemde aksama görülmesine sebep olabilecek saldırılar, kullanıcı için ayrı tehdit oluşturmaktadır. Saldırı çeşidine göre, önüne geçmek, engellemek, gelişen teknolojiyle kolaylaşmaya başladığı bilinmektedir.

Yapılan saldırı gibi saldırı yapanlar da bir kişi ya da grup halindedir. Saldırılar bireysel olarak işlenebilirken, çeşitli yöntemlerde gruplar halinde saldırılar da vardır. Grup halinde yapılabilen saldırılara örneklerden bir tanesi; gönüllü grupları organize eden, Anonymus saldırıları olup, saldırılarında çoğunlukla botnetler kullanılmaktadır.[168]

---

[164] Altınkaynak, *Uygulamalı Siber Güvenlik ve Hacking*, 199.
[165] Ünal, "Dağıtık Servis Dışı Bırakma (DDOS) Saldırıları: Güncel Yöntemler ve Mücadele," 16.
[166] Alper Başaran, "Siber Savaş Tarihinden Bazı Olaylar," *Alper Başaran,* 25 Temmuz 2014, E.T.: 10 Temmuz 2018, url.: http://alperbasaran.com/siber-savas-tarihinden-bazi-olaylar/.
[167] Ünal, "Dağıtık Servis Dışı Bırakma (DDOS) Saldırıları: Güncel Yöntemler ve Mücadele," 17.
[168] Bıçakçı, *21. Yüzyılda Siber Güvenlik*, 40.

Botnetler siber alanda en çok sözü edilen yapılardandır. Botnetler, başka bir söylenişle köle bilgisayarlardır. Tehlikeli olmasında en önemli özelliklerden biri; koordineli biçimde hem büyük hem küçük çaplı saldırılarda ana bilgisayar gruplarını kullanmasıdır.[169] Günümüzün dikkat çeken güvenlik tehlikelerinden biri olan botnetler, 1999'da 'win32/prettypark' zararlı yazılımı sayesinde oluşturulmuş, DDoS saldırılarında kullanılmıştır. Botnetlerde üç ana unsur vardır. Saldırgan, yani botnetin kontrolünü üstlenen, yönlendiren kişi, diğer adıyla botmasterdır. Botnet zararlı yazılımdır; bu sayede kendi ağına zombi bilgisayar kazandırır. Komuta kontrol sunucuları vardır; yani saldırgan ve köle bilgisayar arasındaki bağı kuracak yapıdır.[170] Botnetler; yapılacak herhangi bir saldırı için emir bekleyen, bunun için planlanmış sistemler olup, botmasterların yazdıkları zararlı yazılımlar sayesinde oluşmaktadır. Yazılım içerisinde çalışmaya başlayan bilgisayarlar bilmeden botnete dâhil olurlar. Botmasterdan emir bekleyen zombi bilgisayarlara dönüşür, daha çok spam, bilgi çalmak, kanun dışı eylemler gibi amaçlarla kullanılmaktadır.[171] Botnetler oluşturulmuş sanal bilgisayarlar şeklindedir. Verilen emre, yapılması gereken eyleme göre programlanabilirler. Botneler daha basit bir açıklamayla; kullanım amacı genellikle zarar vermek olan, sanal anlamda kullanılabilen, botmaster yani; saldırganın verdiği emirlere uyarak hareket eden bilgisayarlardır. Botnetler bir kişi tarafından birden çok şekilde oluşturulabilir. Bir amaç için gönderi yapabilen köle bilgisayarlar birçok saldırıda, özellikle; DDOS gibi çoklu saldırılarda en çok işe yarayanlardan biridir. Botnetler ayrıca spam gibi saldırılarda da işe yaramaktadır.

Tehditler içerisinde karşımıza çıkan önemli diğer bir tanesi Spam (İstem Dışı Alınan Elektronik Postalar)'dir. Spam; genelde e-postalarda görülen, ürün reklamı, fikir propagandası ya da bilgi yayılması amaçlı, tek seferde çok kişiye ulaşılabilme imkânı sağlayan mesajlardır.[172] Ancak spam adını alması için; gönderilen mesajların çok sayıda aynı mesajdan olup, kullanıcının mesajları alma talebinde bulunmadan zorla gönderilmiş olması gerekir.[173] Bu mesajlarla internet gereksiz yere meşgul olup, bankacılık, ticaret, resmi işlemler gibi işlemler

[169] W. Timothy Strayer, David Lapsely, Robert Walsh ve Carl Livadas, "Botnet Detection Based on Network Behavior," içinde *Botnet Detection: Countering the Largest Security Threat,* ed. Wenke Lee, Cliff Wang ve David Dagon (New York: Springer, 2008), 1.
[170] Ünal, "Dağıtık Servis Dışı Bırakma (DDOS) Saldırıları: Güncel Yöntemler ve Mücadele," 23-24.
[171] Bıçakçı, *21. Yüzyılda Siber Güvenlik*, 40.
[172] Bayraktar, *Siber Savaş ve Ulusal Güvenlik Stratejisi*, 87.
[173] Yılmaz ve Salcan, *Siber Uzay'da Güvenlik ve Türkiye*, 60.

yavaşlamaktadır. Depolandıkları e-postalarda yer işgal eden mesajlar, kötücül yazılımların yayılmasına meydan vererek suç işlenmesine ortam yaratmaktadır.[174] Spamler e-posta ya da bu tip ortamları kullanan her kullanıcının en az bir kere karşısına çıkmış bir saldırı türüdür. Spam dışarıdan zararsız, hatta bir spam olduğu anlaşılmayacak şekilde görünse dahi sonuçları rahatsız edicidir. E-postada yer sıkıntısı, bankacılık işlemlerinde problem yaratması gibi olaylar bir süre sonra can sıkıcı ve sistemin yavaşlaması açısından rahatsız edici bir görüntü ortaya çıkartır. Bazı kişiler spami sistemsel bir hata gibi görmektedir. Bazı kişilerse spam saldırısını, belirli kişi ya da sitelere özellikle yapmaktadır. Spam dediğimiz tehdit her zaman her kullanıcının karşısına çıkabilecek tehditlerdendir. Ancak bunun dışında kişilere, sitelere zarar verebilecek başka saldırılarda vardır.

Başka bir tehdit; IP aldatmacası (IP Spoofing), diğer bir adıyla gizlenmesidir. IP aldatmacası; var olan bir IP adresini, sunucu ya da sistemlere farklı göstermektedir. Saldırı siber saldırganların genelde tercih ettiği bir yöntemdir. Yöntem kullanılırken; hedef sisteme saldırı yapılacağında gösterilecek kaynak IP adresini farklı bir yer olarak gösterip, hedefe kendi belirledikleri başka bir IP adresi gönderilir.[175] Saldırgan internet mesajlarının kendisinden değil, daha çok saldırılanın tanıdığı birisinden geliyormuş şeklide gösterir.[176] Tehdit, bir bilgisayarın ulaşmak istediği adrese ulaştığını zannederek, aslında saldırganın belirlemiş olduğu ya da kullanıcıya tanıdığı bir adresmiş gibi göstererek kandırmasıdır. Yöntem sayesinde pek çok kişi, bildiği biri ya da adresten geldiğini zannettiği, ancak bir saldırı olarak başkası tarafından gönderilen IP'yi, problem kendini gösterdikten sonra fark etmektedir. IP aldatmacası dışında buna yakın ancak aynı olmayan başka bir saldırı oltalama (phishing) saldırılarıdır.

Oltalama saldırıları bir çeşit aldatma yöntemi içerir. Genel anlamda; hedef alınan kişileri ikna ya da aldatmaca yöntemiyle, verilerinin ele geçirilip, kötü amaçla kullanılmasıdır. Amaç olarak; kullanıcıyı, bir bağlantı ya da uygulamayı açmaya ikna ederek, kişisel verilerini çalıp, bunları kötü amaçla kullanmaktır. Oltalama saldırıları altı alt gruba ayrılmaktadır. Zararlı yazılımlarla gerçekleşen,

[174] Bayraktar, *Siber Savaş ve Ulusal Güvenlik Stratejisi*, 87.
[175] Ünal, "Dağıtık Servis Dışı Bırakma (DDOS) Saldırıları: Güncel Yöntemler ve Mücadele," 27.
[176] Yılmaz ve Salcan, *Siber Uzay'da Güvenlik ve Türkiye*, 58.

kandırma, DNS temelli, Injection temelli, Content, arama motoru üzerinden, ortadaki adam şekillerinde isimlendirilmiş saldırılar bulunmaktadır.[177]

Oltalama saldırılarının türleri vardır. Siber alanda oltalama saldırılarının en çok üç türüne rastlanmaktadır. Clone phishing, yani istenen bir kurumdan geliyormuş gibi gösterilen e-postayla; rastgele, alıcılardan bir kısmının sahte olarak hazırlanmış web sayfasına girmelerinin beklenmesi şeklindedir. Spear phishing, belirli kişi ya da grupları hedef alan saldırılar olup, gönderilen e-postada zararlı yazılım bulunan dosyalarla saldırılması şeklindedir. Phone phishingse, örnekle açıklanacak olursa; e-postayı alan alıcının, banka, alışveriş gibi bir problemi var gösterilerek, bir numarayı aranması istenip, kart numarası, şifre gibi bilgilerin girilmesi sağlanarak saldırı yapılmaktadır.[178] Ancak saldırılar bu kadarla sınırlı değildir. Daha farklı oltalama yöntemi de bulunmaktadır. Genel anlamda oltalama saldırıları para üzerinedir. Sadece finansal kurumlar hedef değildir. Yapılabilecek her işlem, elektronik alışveriş siteleri, internet üzerinden ödeme şeklinde web sayfaları hedeftedir. Bazı kişilerin hesapları ele geçirilerek, kişiye ait bilgileri paylaşma ya da bunlar karşılığında kişiden para isteme şeklinde de bu saldırı gerçekleştirilmektedir.[179] İlk oltalama saldırıları; 1990ların başında, American Online (AOL) üzerinden, ağa sahte kimlik ve kart numaralarıyla üye olup, ücretli içeriklerden ücretsiz faydalanmaları şeklinde olmuştur. AOL bunun önüne geçmek için kimlik doğrulama yöntemine geçince gerçek üyelerin hesaplarını çalma yöntemi şeklinde ilk saldırılar yapılmaya başlanmıştır.[180] Oltalama saldırıları adından anlaşılacağı üzere; karşıdaki kullanıcıyı kandırma amaçlı, kendi oltasına ya da başka bir söylenişle kendi ağına düşürmektedir. Kullanıcının farkında olmadan kendi isteğiyle belirli bilgilerini, özellikle finansal bilgilerini paylaşmalarını sağlayacak tehditlerdendir. Bir aldatma yöntemi olan saldırı, günümüzde en yaygın biçimde karşılaşılabilen türlerdendir. Ancak oltalama saldırıları gibi yaygın başka tehditler bulunmaktadır.

En bilinen tehditlerden başka bir tanesi virüslerdir. Virüsler tehlikeli ve eski zararlı yazılımlardır. Amacı; bilgisayar belleğine yerleşerek, programlarda değişikliğe yol açıp, kendisini çoğaltarak bilgisayar verileri, hatta sistemin

[177] Hakan Hekim, "Oltalama (Phishing) Saldırıları," *Siber Suçlar: Tehditler, Farkındalık ve Mücadele*, ed. Fatih Tombul vd. (Ankara: Global Politika ve Strateji Yayınları, Ocak 2015), 57-64.
[178]Hekim, "Oltalama (Phishing) Saldırıları," 65.
[179]Hekim, "Oltalama (Phishing) Saldırıları," 72-73.
[180] Hekim, "Oltalama (Phishing) Saldırıları," 60.

çökmesine neden olmaktadır.[181] Virüsler; sitelerden dosya yüklemek, virüslü bir e-postayı açmak gibi pek çok biçimde bulaşmaktadır.[182] 1948'de John Van Nedman'ın oluşturduğu, bilinen virüslerin atası biçiminde söz edilen ilk virüs, kendisini kopyalama özelliği olan bir yazılım şeklindeki "automata"dır. İlk kullanımı fayda sağlamak olup, zamanla kötü amaçlarla kullanılmaya başlanmıştır.[183] Virüslerin maddi hasara yol açtığı örneklerden en önemlisi; Filipinli bir gencin yazdığı "i love you" isimli virüstür. 3 Mayıs 2000 tarihinde, virüs bir gecede pek çok bilgisayara bulaşmıştır.[184] Verilen zararın 10 milyar dolar olduğu tahmin edilmektedir.[185] Virüsler çok büyük problem değilmiş gibi görünmektedir. Ancak, örneğin bir bilgisayar sistemi için çok tehlikeli olabilmektedir. Virüsler gibi veriler için zararlı başka tehditler de vardır. Virüslerle birbirine benzerlik gösteren, ancak farklılıkları bulunan bir tehdit solucanlardır.

Solucan (Worm)lar, virüse göre daha karmaşık yazılımlardır. Bağlı olunan ağ üzerinde paylaşılmış dosya, web siteleri ya da e-posta ekleri benzer şekillerde yayılmaktadır. Bu yazılımlar, bulaştıkları sistemde, kullanıcının bir şey yapmasına gerek kalmadan veri kaynaklarını kullanmaktadır. Kaynak dosyaları hızlı şekilde başka kullanıcılara ulaştırabilirken, kendilerini çoğaltabilir, bununla aşırı yüklenme sayesinde ağ kaynaklarını kilitleyebilir, hatta web kaynaklarına erişilebilirlik hızını düşürebilir.[186] Bilinen ilk solucan; 1988 yılında, Robert Morris tarafından yazılan; "Morris Solucanı"dır.[187] Solucan ve virüsler yayılmak amaçlı tasarlanmıştır. Aralarındaki fark; virüslerde insan müdahalesi dediğimiz, dosya ya da bağlantı açmak gibi yöntemlerle bulaşırken, solucanlar buna gerek kalmadan, kendiliğinden yayılmaktadır.[188] Solucan ve virüsler yayılma amaçlı üretildiği için birbirleriyle benzerlik göstermektedir. Ancak yayılma yöntemleri; virüslerin insan müdahalesi ihtiyacı olması, solucanlarda buna gerek olmaması şeklindedir. İki yapı gibi çok bilinen ancak solucan gibi fazla karmaşık olmayan bir başka yazılım truva atı'dır.

---

[181] Eren, *Avrupa Birliği'nin Siber Güvenlik Politikası*, 43.
[182] Yılmaz ve Salcan, *Siber Uzay'da Güvenlik ve Türkiye*, 56.
[183] KURGAN, *Siber Mücadeleye Giriş*, 118.
[184] Eren, *Avrupa Birliği'nin Siber Güvenlik Politikası*, 43.
[185] "Tarihin En Etkili 50 Bilgisayar Virüsü," Chip, E.T.: 12 Temmuz 2018, url: https://www.chip.com.tr/galeri/tarihin-en-etkili-50-bilgisayar-virusu_2025_49.html.
[186] Eren, *Avrupa Birliği'nin Siber Güvenlik Politikası*, 44.
[187] KURGAN, *Siber Mücadeleye Giriş*, 123.
[188] Başaran, *Siber Savaş Cephesinden Notlar*, 32.

Truva atları siber olarak birçok alanda görülmektedir. Daha çok bankacılık işlemleri, kredi kartı bilgilerinin çalınması için kullanılan yöntemlerden biridir. İşleyişi; kişilerin indirmek istedikleri bir içerik şeklinde görünerek, içerisinde zararlı yazılım taşıyarak, indiren kişinin bilgilerini çalıp, başkalarına iletebilen, kullanıcılarınsa bilerek indirdiği yazılımlardır.[189] Kullanıcıları tuzağa düşüren; kendisini program olarak zararsız göstermesidir.[190] Truva atının birçok çeşidi vardır. Truva atlarından en çok kullanılanı; Bukalemun (Chameleon) yazılımlardır. Herhangi bir programın neredeyse tüm özelliklerini taklit ederek, girdiği sistemde her çeşit bilgiyi kopyalayıp gizlice saklayabilmektedir.[191] Başka bir Truva atı metoduysa mantık bombası (logic bomb)'dur. Bilgisayarlara kasten yerleştirilen, zarar vermek amaçlı, seri komutları ifade eden, bilgisayara gönderilen mantık dışı, normalden çok sürekli bilgi gönderilmesini kapsamaktadır. Ancak Truva atı gibi davranan program, belirlenmiş hedefi gerçekleştikten sonra Truva atından farklı davranmaya başlar.[192] Mantık Bombası saldırısı; bir programın içine yerleştirilerek, belirlenmiş olaylar ya da tarihte devreye giren saldırılardır. Solucan ya da virüs gibi belirli zararlı yazılımların devreye geçmesine yaramaktadır.[193] Truva atı tek bir biçimde değildir. Çeşitleri bulunduğu bilinmektedir. Her bir çeşidi farklı etki göstermektedir. Önemli olan; sisteme bulaşırken zararsız görünerek bulaşıp, sonrasında aktif hale gelerek, sistemde sorunlar oluşturmasıdır. Sisteme zarar verebilecek, Truva atı kadar zararlı olabilecek saldırılar da bulunduğu bilinmektedir.

Sıfırıncı gün saldırıları (Zero-day Attack) önemli zararlı yazılım saldırılarından biridir. Saldırıda kullanılan güvenlik sistemi, donanımların ve yazılımların bir kısmında belirli bir veri tabanında olan saldırıları tespit edebilmektedir. Önemli olan; önceden hiçbir güvenlik hâlinin veri tabanında olmayan, daha hiç duyulmamış güvenlik açıklarının kullanılmakta olduğu saldırılardır.[194] Saldırı, şekli sebebiyle, tehlikenin geleceği yer, yapılış biçimi kesin tespit edilemediği için, sonuçları sistemde büyük problem oluşturacaktır.

[189] Başaran, *Siber Savaş Cephesinden Notlar*, 31-32.
[190] Yılmaz ve Salcan, *Siber Uzay'da Güvenlik ve Türkiye*, 57.
[191] Bayraktar, *Siber Savaş ve Ulusal Güvenlik Stratejisi*, 86-87.
[192] İsmail Ergün, *Siber Suçların Cezalandırılması ve Türkiye'de Durum* (Ankara: Adalet Yayınevi, 2008), 25.
[193] Başaran, *Siber Savaş Cephesinden Notlar*, 30.
[194] Başaran, *Siber Savaş Cephesinden Notlar*, 32.

APT (Advanced Persistent Threats- Gelişmiş Sürekli Tehditler); sıfırıncı gün saldırıları ve belirli virüslerden tehlikeli olan bir saldırı türüdür. Belirlenmiş hedef için özel tasarlanıp, gerçekleştirilen, başarılı olana kadar çalışmayı durdurmayan saldırılardır.[195] Saldırıların amacı; girilen ağda uzun müddet kalarak, ağ ve kuruluşa zarar vermekle beraber, hedefleri ulusal savunma, finans, imalat sektörleri gibi yerlerdir.[196] APT önemli sektörleri hedef alır. Saldırı biçimi olarak; belirli bir hedefe kilitlenip, ona ulaşana kadar devam etmektedir. Bu saldırı biçimi sektör ve sistem açısından ciddi problemler yaratacağını göstermektedir. Saldırı olarak kullanıcı hedefli ve onun üzerinden yapıldığı bilinmektedir.

Spyware yazılımı, diğer adıyla; casus yazılım olarak geçmektedir. Amacı; bulaştığı cihazı kullanan kişi veya kişiler hakkında bilgi toplamaktır. Bulaşma şekliyse; girilen herhangi bir site üzerinden, kullanıcının onayına gerek olmadan, fark edilmeden sisteme yerleşmektedir. Kendini kopyalama gibi bir özelliği olmadığı için virüs olarak tabir edilemeyen yazılımlardır.[197] Casus yazılım bir virüs olarak tabir edilememektedir. Bir kopyalama özelliği yoktur. Ancak amacı; bulaştığı cihazdaki kullanıcıya ait veriler, bilgileri kullanıcının haberi olmadan ve onaysız, bir site üzerinden bulaşabilmesidir. Bu özelliklerinden dolayı virüslerle karıştırılmaktadır. Genellikle, casus yazılımlar sonradan reklam verenlere ve diğer ilgili taraflara satılan bir kullanıcı hakkında bilgi toplamak için bilgisayara yerleştirilir. Casus yazılım tarafından toplanan bilgiler bireylerin, aileleri, çalışma grupları, hatta tüm şirket profillerini oluşturmak için diğer veri tabanlarla birleştirilir. Bu tür profiller çoğunlukla doğrudan pazarlama amacıyla kullanılmaktadır.[198] Fakat casus yazılım tamamen başka bir amaç içinde olduğundan, başka saldırı çeşitlerinden ayrılmaktadır. Casus yazılımdan söz ettikten sonra, kullanıcılar, aynı zamanda siteler üzerinden yayılabilen başka bir saldırı türü olan adware'dan söz etmek gerekir.

Adware (reklam destekli bilgisayar yazılımı) yazılımlar, yayınladıkları reklamlardan para kazanan yazılımlardır. Kullanıcının girdiği siteler üzerinden bilgi sızdırarak, başka yerlerde kullanıcının karşısına kendi girmiş olduğu siteler

[195] Başaran, *Siber Savaş Cephesinden Notlar*, 32-33.
[196] Eren, *Avrupa Birliği'nin Siber Güvenlik Politikası*, 56.
[197] Başaran, *Siber Savaş Cephesinden Notlar*, 34.
[198] Michael Erbschloe, *Trojans, Worms, and Spyware* (ABD: Elsevier Butterworth–Heinemann Publisher, 2005), 26.

üzerinden reklamlar çıkartabilmektedir.[199] Bu yazılımlarla, internet ortamı olan hemen hemen her yerden, çoğu tarayıcı sayesinde, en az bir kere karşılaşılma imkânı bulunmaktadır. Rahatsız edici olan; aynı oturumdan, hem bilgisayar hem telefon gibi cihazlar üzerinden bağlı olunduğunda, herhangi birinden arama motorunda araştırılan bir site üzerinden olmaktadır. Çünkü başka bir cihazda, yine aynı oturum üzerinden bambaşka bir uygulama içerisinde reklam olarak gösterilmektedir. Kişiler üzerinde izlendiği hissi yaratmaktadır. Adware yazılımların amacı; kişileri reklamlara yönlendirerek, kullanıcının bir tıklaması sonucu para kazanılmasıdır.

Yapılan saldırılar içerisinde, diğer saldırılar dışında, özellikle kurumlarda kullanılabilecek çeşitleri vardır. Keyloggerlar (tuş kaydedici), daha çok kurumsal ağlarda tehlike oluşturmaktadır. Girdiği bilgisayarda kullanılan klavye hareketlerini kayda alan, bunu saldırgana bildiren, kullanıcının kişisel bilgilerinden yazılan raporlara kadar pek çok şeye ulaşılmasını sağlayan saldırılardır. Tuş kaydediciler sadece yazılımsal olarak değil, donanım olarak da klavye ve kasa arasına yerleştirilebilecek bir sistemdir.[200] Tuş kaydediciler yazılım ve donanımı tehdit eden türden bir saldırıdır. Bilgisayarda ya da cihazda yapılanları, özellikle klavye hareketlerini saldırgana bildirmesi, kurumlarda çok büyük tehdit haline gelmektedir. Saldırganın, cihazı kullanan kişinin her türlü kişisel veriden, kullanmış olduğu bütün sözcüklere kadar erişebilmesi ihtimali, kullanıcı için bireysel bir tehdit olmaktadır.

Tehditler sadece kişi ya da kurumlar üzerinden değildir. Sistem üzerinden daha farklı tehditler olduğu bilinmektedir. Kod kaynak istismarı (Code Exploit); sistemlerin kendi içindeki yazılımlarda oluşan şifreleme hatası gibi yazılım kusurlarıyla ortaya çıkmaktadır. Bilgisayar sisteminin beklenmedik biçimde çalışmayı durdurması ya da sistem kontrolünün başkasının eline geçmesine sebep olmaktadır. İnternette bir web sayfasında bulunabilen zararlı kodlar, tarayıcıda bulduğu bir güvenlik zafiyetinden yararlanıp, sistemden bilgi toplamaktadır.[201] Bir kusur sayesinde sistemin tamamen başkasının eline geçmesini sağlayabilen kod kaynak istismarı, özellikle kullanıcı açısından büyük sorun oluşturmaktadır.

[199] Başaran, *Siber Savaş Cephesinden Notlar*, 34.
[200] Başaran, *Siber Savaş Cephesinden Notlar*, 34-35.
[201] Bayraktar, *Siber Savaş ve Ulusal Güvenlik Stratejisi*, 89.

Ayrıca, söz ettiğimiz saldırılar siber suçlar için kullanılabilen, çok karşılaşılan yöntemler olduğu bilinmektedir.

Veri Aldatmacası (Data Diddling); siber suçlar için en çok tercih edilen, basit, güvenilirliği dışında ortaya çıkartılması zor olan bir yöntemdir. Verinin sisteme girilirken yanlış girilmesi, değiştirilmesi, kasten sistem içerisinde bırakılmasını nitelemektedir.[202]

Çöpe Dalma (Scavenging); artık toplama şeklinde bahsedilebilecek yöntemdir. Siber suçlar tarafından tercih edilen, bilgisayar sistemi çalışması sonrası arkasında bırakmış olduğu verilerin toplanmasıdır. Bilgisayar çıktısının herhangi bir çevreden toplanmasından, bilgisayardan silinmiş verilerin geri elde edilerek toplanmasına kadar çeşitleri vardır.[203] Yöntem, bilgisayar verisi ya da fiziksel biçimde, siber alandan fiziksel ortama geçebilmektedir. İstenilen verinin toplanmasını kapsamaktadır.

Siber alanda önemli yer tutan, biraz daha tehlikeli siber tehditler de bulunmaktadır. Stuxnet en güzel örnektir. Stuxnet adı verilen yazılım, bir siber silah şeklinde nitelendirilebilecek bir yazılımdır. 2010 yılında ortaya çıkan yazılım, İran nükleer programını hedefe almış, milyonlarca dolar zararın yanında, binlerce santrifüjü imha etmiştir. Siber anlamda tehlikenin ne derece olduğunu ortaya koymuş birkaç olaydan bir tanesidir. Olayın başlangıcı 2008 yılına dayanmaktadır. Amaç; İran'ın nükleer programını yavaşlatarak, bomba yapımında kullanılan uranyuma sahip olmasını engellemekti. Ancak, Stuxnet saldırısını kimin, nereden yapmış olduğu hala net şekilde bilinmemekte sadece belirli tahminler yapılabilmektedir.[204] Stuxnet'i önemli kılan başka bir nokta; hem yayılım tarzı hem politik olarak kullanılışıdır. Daha önemlisi, özellikle bir ana kartı hedef almak amaçlı programlanmış ve yöntem olarak çok rastlanılmıştır.[205] Stuxnet'te önemli başka bir durum daha vardır. P. W. Singer ve Allan Friedman'ın söz etmiş olduğu üzere; Mikko Hypponen'in bahsettiği çok önemli bir nokta vardır. Saldırının stratejilerde değişiklik olduğunun göstergesi olup, ülkelerin silah depoladıkları ve bu silahların bilinen silahlar dışında, siber silahları kapsadığından bahseder.[206] Stuxnet'le ülkelerin sadece fiziksel anlamda silah

[202] Bayraktar, *Siber Savaş ve Ulusal Güvenlik Stratejisi*, 90.
[203] Bayraktar, *Siber Savaş ve Ulusal Güvenlik Stratejisi*, 90.
[204] Alper Başaran, *Siber Kıyamet* (İstanbul: Arion Yayınevi, Ekim 2017), 61-62.
[205] Bıçakçı, *21. Yüzyılda Siber Güvenlik*, 41.
[206] Singer ve Friedman *Siber Güvenlik ve Siber Savaş*, 161.

rezervlerini doldurmaya çalıştıkları dönemin geride kalmaya başladığını, yavaş yavaş siber silahların ya da donanımların ön plana çıktığı görülmektedir.

Başka bir önemli olay; 1 Eylül 2011 yılında, Stuxnet'ten kısa süre sonra ortaya çıkmıştır. Duqu isimli yazılım, pek çok özelliğiyle Stuxnet'e benzemektedir. Duqu'nun farkı; endüstriyel kontrol sistemlerinin istihbaratını toplamak olup, şifre kopyalama, doküman çalma, ekran görüntüsü alma gibi yöntemler kullanmasıdır.[207] Yani; Stuxnet'e benzerlik göstermekte ancak amacında farklılaşmaktadır.

Stuxnet ve Duqu'dan sonra; 2012'de başka bir saldırı daha ortaya çıkmıştır. Saldırıya Flame adı verilmiştir. Flame; Duqu gibi ekran görüntüleri alabilen, mikrofonu uzaktan açabilen özelliklere sahiptir. Ayrıca yakındaki cihazlara Bluetooth gibi özelliklerle yayılıp Stuxnet'ten 20 kat daha çok kod içermektedir. Aynı zamanda Stuxnet ve Duqu gibi kim tarafından gönderildiği belli olmayan bir yazılımdır.[208]

Gauss; 2012 Temmuz ayında Flame'e benzer bir yapıda ancak bilgi toplama amaçlı ortaya çıkmıştır. Kişilerin banka hesap şifreleri, sosyal medya hesapları gibi özellikle kritik bilgilerini toplamaya yönelmiştir. Stuxnet, Duqu ve Flame saldırından farklı olarak, kendini şifreleyebilmekte olup, şifresi kendisinde bulunmamaktadır.[209] Genel olarak dört saldırıya baktığımızda; 2010 yılından sadece 2 yıl sonrasına kadar benzer yapıda, ancak her seferinde daha gelişmiş biçimde ortaya çıkmışlardır. Teknolojinin hızlı ilerlemesi, yapılan her saldırıda görülen eksiklerin bir sonrakinde tamamlanarak, daha gelişmişi şekilde ortaya çıkmasını sağlamıştır. 2012 yılından günümüze ciddi farklılaşmalar olduğu görülmektedir.

Genel anlamda; bilgisayar ortamındaki tehditler sadece bilgisayara hasar verebilecek, ufak tehditler gibi durmaktadır. Ancak son yıllarda ufak tehditler, daha büyük tehlikeleri kapsayacak konuma gelmiştir. Siber alanın her anlamda açık oluşu, sistem yapılarının gelişimlerinin kendi boşluklarını oluşturması, ufak tehditlerin uluslararası alana kadar tehdit oluşturabilmesine sebep olmuştur.

---

[207] Bıçakçı, *21. Yüzyılda Siber Güvenlik*, 42-43.

[208] Nicole Perlroth, "Researchers Find Clues in Malware," *The New York Times*, 30 Mayıs 2012, E.T.: 13 Temmuz 2018, url: https://www.nytimes.com/2012/05/31/technology/researchers-link-flame-virus-to-stuxnet-and-duqu.html.

[209] Boldizsar Bencsath , Gabor Pek , Levente Buttyan, and Mark Felegyhazi, "The Cousins of Stuxnet: Duqu, Flame and Gauss," *Future Internet* 4 (2012): 986, E.T.: 13 Temmuz 2018, doi: 10.3390/fi4040971.

Bilgisayar ortamındaki tehditlerin; özellikle belirli amaçlar için kullanımı, stratejik tehditlere dönüşmesini sağlamıştır. Stratejik anlamda tehditler, bu tehditlerden daha büyük sonuçlara yol açmaktadır. Bir tehdit tek başına güvenlik için yeterince sorun oluşturmaktadır. Bilgisayar ortamındaki tehditlerin stratejiyle birleşmesi, özellikle uluslararası alanda büyük problemlere yol açabilmektedir. Siber alanda oluşabilecek stratejik tehditlerse ayrıca incelenmesi gereken önemli konulardan biridir.

1.2.4.2. Siber Alanda Stratejik Tehditler

Bilgisayar ortamındaki tehditlerle birlikte oluşan, bunun üstünde sayılabilecek tehditleri stratejik anlamda düşünmek gerekir. Stratejik tehditler, bilgisayar ortamındaki tehditlerin kullanılarak, belirli amaçlarla uygulanması şeklinde düşünülebilir. Stratejik tehditler sadece kişiler arasında değil, devletler ya da belirli aktörler arasında da olmaktadır.

Stratejiden söz edildiğinde genel bir tanımı yapılmalıdır. Bir varlığın kendi varlığını sürdürmesi, koruması, geliştirmesi, kendi varlığına tehdit oluşturabilenin de ortadan kaldırılmasına yönelik tavır ve uygulamalar şeklinde tanımlanabilir. Stratejinin konusu; her bir aktörün çevresiyle arasındaki ilişkileri düzenleyip, rakiplerine belirli üstünlük sağlayabilmek amaçlı kaynaklarını kullanmasıdır.[210] Tanımlamalardan anlaşılacağı üzere; bir strateji varsa, bir güvenlik ve güvensizlikte vardır. Stratejinden bahsedildiğinde, aktörün kendi varlığı, onun tehdide düşmesinden korunması gibi uygulamalar içermektedir. Belirli bir hedef, amaç olmalıdır. Hedefe ulaşmak için uygulanan yöntemler olarak da düşünülebilir. Strateji tanımı sadece bireysel ya da aktörler üzerinden değil, uluslararası anlamda da yapılmaktadır. Uluslararası ilişkiler alanında strateji; uluslararası politikada var olan aktörlerin ilişkileri süresince kullanmış oldukları yöntemleri ifade etmektedir. Uluslararası sistemdeki bir aktörün stratejisi; aktörün amaçları ve gücünü kapsamakta, ayrıca bunun kimin için kullanıldığına dikkat edilmelidir.[211] Strateji; bir hedefe ulaşmak için izlenecek yol olarak düşünülebilir. Birey, devlet, uluslararası düzeylerde, amaca göre farklı şekiller ve alanlarda karşılaşılan strateji, genel anlamda; hedefleyen ve hedeflenene göre değişiklik göstermektedir.

---

[210] Dedeoğlu, *Uluslararası Güvenlik ve Strateji*, 93.
[211] Dedeoğlu, *Uluslararası Güvenlik ve Strateji*, 98-99.

Stratejiden söz edildiğinde en az birbiriyle ilişkili üç unsuru olması gerekmektedir. Hangi alanda olursa olsun, stratejide önemli üç unsur; araç, amaç ve yöntemi olmak zorundadır.[212] Stratejide, hatta pek çok konuda önemli bir kavram daha bulunmaktadır. Bu kavram güçtür. Yumuşak ve sert (askeri) güç olarak ikiye ayrılabilirken, gelişen teknoloji akıllı gücü de ortaya çıkarmıştır.[213]

Güçten bahsedildiğinde kabul gören tanımlardan biri; David A. Baldwin'in bahsettiği, Robert A. Dahl'ın ortaya attığı; iktidarda geçerli olan, bir aktörün başka bir aktör üzerinde yapamayacağı bir şeyi yaptırmasıdır.[214] Güç; istenilen, arzu edilen amaç ya da hedeflere ulaşabilme, başkalarını yaptıklarıyla etkileme becerisidir.[215] Gücü doğru yer ve şekilde kullanmak gücün kendisinden önemlidir. Yumuşak, sert ve akıllı güç; güçte önemli kullanım şekilleridir.

Yumuşak güç; "Siber Mücadeleye Giriş" kitabında geçtiği üzere; Joseph S. Nye'nin ifade etmiş olduğu gibi; ulaşmak istediğini zor kullanmadan, aktörün ideallerine hayran olunup, diğer aktörlerin istenilen amacı istemelerini sağlama yöntemidir. Kısaca; bir aktör ya da milletin akıl ve kalbini fethetmek için kullanılan güçtür.[216] Yumuşak güç; karşı tarafın kendi iradesiyle kabul ettiği, istenene zor kullanılmadan ulaşılabilmeyi sağlayan güçtür.

Akıllı güç yeni bahsedilen bir güç yapısıdır. Joseph S. Nye; akıllı gücü tüm imkânların doğru zaman ve mekânda değerlendirilmesi olarak görmüştür. Ayrıca dost ve düşmanı ortak paydada buluşturup, dış politikada sert ve yumuşak gücü beraber kullanabilmektir.[217] Akıllı güçten, yumuşak güçle sert gücün ortası olarak, hangi gücü, nerede, ne şekilde kullanabileceğini bilme şeklinde bahsedilebilir. Akıllı güç, adından anlaşılacağı üzere, akıllıca hamleler uygulanarak gücünü göstermektir. Aynı zamanda imkânları doğru şekilde kullanarak, doğru hamleler yapmayı içerir. Bu sebeple akıllı güç, bütün güçlerin bir arada, amaca göre şekillenip kullanılması olarak düşünülebilir.

Sert güç; bir hedefe ulaşılmak için gösterilecek zorlayıcı eylemler ya da tehditleri içermektedir. Ayrıca, nüfus büyüklüğü, ekonomik güç, askeri güç, doğal

[212] Hasan Basri Yalçın, *Ulusal Güvenlik Stratejisi* (İstanbul: SETA, Kasım 2017), 24.
[213] Darıcılı, *Siber Uzay ve Siber Güvenlik*, 46-47.
[214] David A. Baldwin, *Power and International Relations: A Conceptual Approach* (Amerika: Princeton University Press, 2016), 12, E.T.: 14 Temmuz 2018, ISBN: 978-1-4008-8100-0.
[215] Nye ve Welch, *Küresel Çatışmayı ve İşbirliğini Anlamak*, 55.
[216] KURGAN, *Siber Mücadeleye Giriş*, 72.
[217] Joseph S. Nye Jr., "Get Smart: Combining Hard and Soft Power," *Foreign Affairs* (2009), E.T.: 5 Ağustos 2019, url: https://www.foreignaffairs.com/articles/2009-07-01/get-smart.

kaynaklarla, bulunduğu bölge ve coğrafyayla ölçülebilecek bir güçtür.[218] Sert güç tanımı, bazı kaynaklarda askeri güç olarak da söz edilmektedir. Çünkü sert ve zorlayıcı eylemler askeri güç adı altında yapılmaktadır. Diğer güçleri içerisinde barındırıp, uygulanabilse dahi askeri güç, sert güç açısından daha ön plana çıkmaktadır. Askeri güç, uluslararası ilişkiler üzerinde hâlâ önemini korumakta olup, bilgi teknolojisiyle güç kullanımında etkileri olmaktadır. Eskiden pahalı gelen askeri teknolojilere, herkesin ulaşabilmesiyle küçük grup ya da devletlere güçlenme olanağı sağlanmış, büyük devletlerin korunmasızlığı artmıştır[219] Askeri anlamda gücün stratejiyle sağlandığı zamanlar da olmaktadır. Askeri strateji; Carl von Clausewitz'e göre; ulusal siyasette hedeflerini korumaya almak amacıyla, ulusun silahlı kuvvetlerini güç uygulama ya da uygulama tehdidi oluşturma yoluyla kullanılmasıdır. Clausewitz stratejiyi, savaşın operasyonel kısmıyla daha çok örtüştürmektedir. Bu açıdan savaşı politikanın başka araçlarla sürdürülmesi olarak tasvir etmiş, stratejilerin anlaşılmasıyla politikanın karakterinin anlaşılabileceğinden söz etmiştir.[220] Sert, yani; bir bakıma askeri güç, içinde zor kullanımı, hatta savaş durumunu barındırdığı için, zorunda kalınmadıkça günümüzde en son kullanılma niyeti olan güçlerdendir. Sert güçten önce kullanılabilecek yumuşak hatta günümüzde önemli bir yere sahip olmaya başlayan akıllı güç vardır. Yumuşak ve akıllı güce stratejik anlamda başvurulup, işe yaramadığında sert güce başvurulmaktadır.

Strateji üzerine düşünceler ilk M.Ö. 317-293 yıllarında, Maurya İmparatorluğunda, İmparatoru'nun danışmanlığını yapan Kautilya'nın döneminde ortaya çıkmıştır.[221] Beril Dedeoğlu'na göre; Kautilya'na; döneminde strateji olarak askeri kapasiteyi arttırmıştır. Bu stratejiyle devletin gücü için her yolu yasal görüp, inanç ve etiği sadece iç siyasal bütünlükte benimsemiştir.[222] Stratejik olarak, askeri alanı kuvvetli tutmanın faydalı olacağını düşünmüştür. Etik ve inançları sadece iç siyasal bütünlükte gerekli görüp, dışarıya bunları gerekli

[218] Giulio M. Gallarotti, "Smart Power: Definitions, Importance, and Effectiveness," *Division II Faculty Publications* 163 (2014): 4-5, E.T.: 14 Temmuz 2018, url: http://wesscholar.wesleyan.edu/div2facpubs/163.
[219] Nye ve Welch, *Küresel Çatışmayı ve İşbirliğini Anlamak*, 390.
[220] Carl von Clausewitz, *Savaşın Esasları*, Çev.: Gökhan Aydın (İstanbul: Doruk Yayınları, Nisan 2017), 66-87.
[221] Pravin Chandrasekaran, "Kautilya: Politics, Ethics and Statecraft," (2006), E.T.: 17 Temmuz 2018, url: https://www.researchgate.net/publication/24116687_Kautilya_Politics_Ethics_And_Statecraft.
[222] Dedeoğlu, *Uluslararası Güvenlik ve Strateji*, 126.

görmemesi, bakış açısının sert güçten yana olduğu ve stratejisini bu yönde geliştirdiğini göstermektedir.

Stratejik anlamda önemli değişimler Peloponnes Savaşı döneminde olmuştur. Beril Dedeoğlu'nun söz etmiş olduğu üzere Thucydides; benzerlerin savaşının, olumsuz sonuçlar doğuracağından bahsetmiştir. Çatışma ve güç arasındaki ilişkiyse, savaşarak güçlü olanın güçsüz üzerinde yaptırım olanağını ortaya çıkartıp, bir tehlike gören tarafında gücünü arttırarak savaş çıkma olasılığını arttırdığından söz etmiştir.[223] Thucydides savaş üzerinden inceleme yaparak, savaşla güçlünün karşı tarafa yaptırımda bulunabileceğinden bahsetmiştir. Karşı tarafın bunları gördükten sonra gücünü arttırmasıysa başka problemlere sebep olacağından söz etmiştir. Ona göre; bir taraf diğer taraftan zarar gördüyse ya da ihtimali düşünürse, kendisini korumak amaçlı, kendi imkânlarını arttırmaya yönelecektir. Bu da savaş çıkma ihtimalini yükseltir. Roma döneminde stratejiler; imparator birliğinin yayılmak için engelleri kaldırması şeklindeydi. Orta Çağda; St. Augustin strateji üzerine eğilerek, 'iyi'nin varlığını sürdürmesi düşüncesiyle güç ve iktidarın genişletilip korunmasını temel almaktaydı.[224]

14. yüzyılda Beril Dedeoğluna göre İbn-i Haldun; stratejinin sabit olmadığını gösterir. Her toplumun kendine has özelliği vardır. Ekonomik ve güvenlik sebepleriyle de bir arada yaşanması gerekliliği oluşmuştur. Ayrıca Dedeoğlu; Machiavelli'nin devlet stratejisinin devletin iyi yönetilmesine bağlı olduğundan söz etmiştir. Özellikle Machiavelli'nin Prens kitabında; bir hükümdara devleti yönetmesi için belirli stratejiler, yani belirli amaçlar için yöntemleri göstermiştir. Dedeoğlu; 17. Yüzyılda; Hugo Grotius'un stratejinin temelindeki rasyonalizmle, hesapların iyi yapılması anlamında uluslararası alanda, yani anarşik yapı içerisinde bir yol izlenmesi gerektiğinden söz etmiştir. Devletlerin savunma stratejisi üzerinde durmaları gerektiğinden bahsetmiştir. Başka bir rasyonalist olan Thomas Hobbes'unda Dedeoğlu'na göre; bir devletin temel stratejisini kendi benzerine göre düzenlediğinden söz etmiştir.[225]

19. yüzyıla; dış politika stratejileri çeşitlilik göstermeye başlamıştır. İşbirliği ve çatışma stratejileri kendini göstermeye devam etmiştir. Günümüzde

[223] Dedeoğlu, *Uluslararası Güvenlik ve Strateji*, 127-128.
[224] Dedeoğlu, *Uluslararası Güvenlik ve Strateji*, 128-130.
[225] Dedeoğlu, *Uluslararası Güvenlik ve Strateji*, 131-132.

hâlâ önemini taşıyan bir yaklaşım, Carl von Clausewitz tarafından ortaya atılmıştır. Daha çok savaş üzerinden, askeri stratejilerin savaşı kazanmada öneminden bahsetmiştir. Savaşı bir politika olarak ilk defa ele alan Clausewitz'tir. Karşı tarafa iradeyi kabul ettirmek amaçlı kuvvet kullanma şeklinde tanımlaması yapılabileceğinden söz etmiştir.[226] Clausewitz stratejiyi; savaş ya da seferin sonucuna ulaşmak için tek tek yapılan uğraşların toplamı olarak ifade etmiştir.[227] Ancak bu stratejiler önemli olmakla beraber, savaş üzerine farklı stratejiler olduğu da bilinmektedir.

19. yüzyılın sonu, 20. yüzyılın başında; jeopolitik yaklaşım etkili olmuştur. Devletlerin bulundukları coğrafyaya göre stratejiler belirlenmiştir. Dedeoğlu'na göre; Edward Hallett Carr; iş birliği stratejisiyle sisteme hâkim olmadan bahsederken, Hans Morgenthau; sistemin anarşik ve istikrarsız oluşuyla rekabetçi olduğundan söz etmiştir. Bunun için askeri kapasitenin iyi olması, bir avantaj sağlayabilmek içinse maddi ve moral kapasitelerinin buna göre yapılanmasını söyleyerek sıfır toplamlı stratejiyi öngörmüştür.[228]

Dedeoğlu; Raymond Aron'un; güç ve kuvveti birbirinden ayırarak, ekonomik, askeri moral kaynaklarını kuvvet, bunların bir amaç için birleşmesineyse güç dediğinden bahsetmiştir. Ayrıca Dedeoğlu John Herz'in saldırı ve savunmayı temel iki yapı olarak incelediğinden söz etmiştir. 1970'lerden sonra; strateji değişkenlere göre belirlenip, daha çok ekonomik temelli bağlılık, askeri güç, kendi bölgeleri dışında rakiplere ortak mücadele düşüncesi hâkim olmuştur.[229] Bu döneme kadar; stratejiler, savaşta eldeki güç ve kuvvet olarak ele alınmıştır. İlerleyen dönemlerde stratejiler değişiklik göstermiştir. Özellikle savaşın sonuçlarının değerlendirilmeye başlanmasıyla, farklı stratejilerle, güç başka alanlarla bölünmüştür. Çeşitli alanlar üzerinden stratejiler yürütülmeye başlanmıştır. Ancak yine güçten söz edildiğinde askeri kapasite, güçle orantılı şekilde değerlendirilmektedir. Bu düşünce geçmişten günümüze kalıcı bir biçimde devam etmektedir.

Her dönemde belirli dönüm noktaları vardır. Uluslararası ilişkiler çalışmalarında önemli dönüm noktalarından biriyse Soğuk Savaş'ın sona ermesidir. Soğuk Savaş'ın sona ermesiyle yeni güvenlik tehditleri ortaya

[226] Dedeoğlu, *Uluslararası Güvenlik ve Strateji*, 133-135.
[227] Clausewitz, *Savaşın Esasları*, 36.
[228] Dedeoğlu, *Uluslararası Güvenlik ve Strateji*, 136-138.
[229] Dedeoğlu, *Uluslararası Güvenlik ve Strateji*, 138-140.

çıkmıştır. Önceden dikkate alınmamış olan güvelik sorunları tartışmaya açılabilir konuma gelmiştir.[230] Soğuk Savaş sonrası, iletişim gibi belirli yapıların maliyetinin düşerek mesafelerin etkisinin azalması önemlidir. Bu sayede ekonomik bağlılıkların büyüyerek yeni bilgilerin ortaya çıkması, teknolojik gelişmelerle hükümet ve devletlerin belirli konularda tavırlarında değişimler ortaya çıkmasına sebep olmuştur.[231] Soğuk Savaş dönemi sonrası, siber anlamda stratejik tehditlerin gelişmesinde de etkili olmuştur. Çünkü dönemden sonra bazı gelişmelere daha çok eğilim gösterilmiştir.

Stratejik tehditlerin zamanla gösterdiği değişim daha çok savaş üzerinedir. Stratejik tehditler; tarih içerisinde sadece savaş, karşı tarafın kapasitesine göre kendini güvenceye alıp, karşılık vermesi ya da bir hedefe ulaşma amaçlı tavırlardı. Günümüzde; sadece savaş odaklı olmayıp, yeni çıkan tehditler, teknoloji gibi etkenlerle siber alanda varlığını göstermeye başlamıştır.

Tehditlerde stratejinin önemi; bir karşıt aktör olduğu kararı verildiği zaman, tehdit hakkında stratejik olarak düşünerek, karşı tarafın amaçları nelerdir, ne gibi problemler oluşabilir düşüncesi vardır. Ayrıca, savunma amaçlı, olası tehdit karşısında neler yapılabilir, sonucunda karşı tarafın değişebilecek tavırlarına uygulanabilecek davranış ve politikalar üretmeye yardımcı olmaktadır.[232] Tehditler karşısında stratejinin önemi; karşı taraf analiz edilerek, ondan gelebilecek tehditleri savunmaktır. Ayrıca üretilecek politikalara karar verilmesinde önemli rol oynar.

Siber anlamda stratejik tehditlerden bahsetmek günümüz için önemlidir. Genel anlamda siber saldırılar; yasadışı ya da yasal kuruluşların, yetkili hükümet organlarının, şahıs, şirket ya da teröristlerin stratejik, taktik ya da operasyonel amaçlarla, siber alanda uygulamış oldukları saldırılardır.[233] Siber alandaki özelliklerin kullanılarak, belirli amaçlarla tehditler oluşturulması, tehditlerin stratejik olarak siber anlamda savaş, terör, bunun için yapılabilecek istihbarat gibi uygulandığını göstermektedir. Savunmaysa beraberinde gelmektedir.

Stratejik anlamda siber tehditlere siber suç dâhil edilmektedir. Genel anlamda siber suçlar daha az tehlikeli tehditleri kapsamaktadır. Siber terör ve siber savaşsa uluslararası anlamda büyük sonuçlar doğurabilmektedir.

---

[230] Çıtak, *Güvenlik ve İstihbarat*, 157.
[231] Nye ve Welch, *Küresel Çatışmayı ve İşbirliğini Anlamak*, 341.
[232] Singer ve Friedman *Siber Güvenlik ve Siber Savaş*, 60.
[233] Çiftçi, *Her Yönüyle Siber Savaş*, 151.

Siber suç genel anlamda; bilgisayar ortamı üzerinden ya da bilgisayarların bağlı olduğu ağlardan, bunlara karşı hukuki açıdan yanlış olan eylemleri kapsamaktadır.[234] Her tür siber suç hızlı bir biçimde büyüme ihtimalini barındırmaktadır. Birçok şekilde uygulanılabilen siber suçlar, siber alanın her yapısının birbiriyle bağlantılı olmasından dolayı büyük sorunla açık görünmektedir.[235] Siber suçlar, siber alan için önemli ve önlem alınması gereken tehditlerdir. Siber suçlar da siber terör ya da siber savaş gibi tehlikeli boyutlara çıkabilmektedir. Ancak siber suçları, siber terör gibi tehditlerden ayıran nokta; eylemin amacının siyasi olmasıdır.[236] Siber suçlar daha çok kişisel sebeplerden ya da maddi amaçlı yapılmaktadır. Siber terör ya da savaştaysa siyasi amaçlar vardır. Bir veri hırsızlığı ya da kredi kartı bilgilerinin çalınması siber suçtur. Bu örnekteki suçu ve benzerlerini siber terör ve savaştan ayırmak gerekir. Siber suçlar ciddiye alınması gereken bir konu olsa da, siber terör ve siber savaş uluslararası alanda daha problemli sorunlar çıkartabilmektedir.

Genel anlamda; siber saldırıların, stratejiler uygulanarak, belirli amaçlar doğrultusunda, devlet ya da aktörlere, belirli eylemlerde bulunması, karşı taraf için bir sorun ya da zorluk teşkil etmektedir. Sorunlarsa stratejik anlamda siber tehditler olarak bahsedilmektedir. Siber suçlar pek çok aktör açısından problem oluşturmaktadır. Ancak genelde birey seviyesinde oluşu, uluslararası alanda daha farklı yeri olmasına sebep olmuştur. Siber terör, siber savaş, siber istihbarat devletler ve belirli gruplar açısından tehlikeyi ifade etmektedir. Belirli konuların anlaşılabilmesi içinse; öncelikle bunların ayrı ayrı incelenmesi, sonrasında siber savunmanın nasıl yapılacağı hakkında bilgi verilmesi gerekir.

1.2.4.2.1. Siber Terör

Stratejik olarak tehditler içerisinde, günümüzde en dikkatli olunması gerekenlerden bir tanesi siber terördür. Siber terörde en dikkat edilmesi gereken kısım; kuralsız bir biçimde, sivil ya da asker ayrımı yapmadan ortaya çıkmış olmasıdır. Daha çok, amaç odaklı saldırılardır. Bir siber saldırının terör şeklinde

[234] Ergün, *Siber Suçların Cezalandırılması ve Türkiye'de Durum*, 15.
[235] David Omand, "Understanding Digital Intelligence: A British View," içinde *National Security and Counterintelligence in the Era of Cyber Espionage,* ed. Eugenie de Silva (ABD: Information Science Reference, 2016), 116.
[236] Çakmak ve Altunok, *Suç, Terör ve Savaş Üçgeninde Siber Dünya*, 41.

bahsedilmesi için; politik sebeplerle yapılıp, sonucunun yıkıcı olması gerekir.[237] Ancak; siber alan da olsa, bir olayın terör olup olmadığına karar verilmelidir.

Siber terörden önce, terörden bahsetmek gerekir. Terör üzerine genel tanımlar yapılmış ancak tam bir uzlaşı sağlanamadığı için kesin yargılardan söz edilememiştir. Kavram üzerinde bir uzlaşı olamaması; siyasi anlamda içeriğinin, kişi, mekân ve zamana göre, devletten devlete, kişiden kişiye, toplumdan topluma değişim göstermesidir.[238] Tanımlardan bir tanesi; acımasızca yıkıcı, bazen tahmin edilebilir bir şekilde, sivilleri kasıtlı olarak hedefleyen politik şiddet olarak yapılmıştır. Aynı zamanda hükümetleri zorlama veya tehditle, bireylere, mülke yönelik şiddeti yasadışı bir şekilde, çoğu zaman politik, dini veya ideolojik amaçlara ulaşmak için kullanılmasıdır.[239] Terörizm başka açıdan; korku barındırarak bir siyaset yapma biçimidir.[240] Terör ve terörizm genel anlamda; siyasi amaçlarla, olağandışı şekillerde, korkuyu şiddetle kullanarak, davranışları etkilemektir. Kişi, grup ya da devlete, hatta sistemlere göre, terör ve terörizm tanımı, bakış açıları, bulunan taraf açısından değişmektedir.

Siber terörizm kısaca; siber alanda karşılaşılan terör hâlini ifade etmektedir. Siber terörizm ilk defa Barry Collin tarafından 1980'de kullanılmıştır.[241] Siber terörizm hakkında birçok tanımlama yapılmıştır. Ancak siber terörizmin tanımı yapılırken belirli güçlükler ortaya çıkmıştır. Tanımlamada oluşan güçlüğün en büyük sebebi 'terörizm' kavramının kendisinden kaynaklanmaktadır. Siber terörizm üzerine tanımlardan bir tanesi; siber alanda, siyasi içeriği olan, bilgisayar sistemlerine yönelik, sızma, bozma ya da ihlal etmeyi içermektedir. Bunların ihtimalinin tehdidinin dahi sebep olduğu engellemelerle, birçok insanın davranış ve günlük yaşam seyirlerini bozmayı hedeflerler.[242] Dorothy E. Denning siber terörizm üzerine ayrı bir tanımlama yapıştır. Denning'e göre; halk ya da hükümete karşı sosyal, politik içerikli saldırılar üzerinden, tehdit veya zorlamalar sayesinde, bilgisayar, ağ ve verilere karşı yapılabilecek saldırıları içermektedir. Aynı zamanda kişiler ya da mülke

[237] Çakmak ve Altunok, *Suç, Terör ve Savaş Üçgeninde Siber Dünya*, 88.
[238] Bayraktar, *Siber Savaş ve Ulusal Güvenlik Stratejisi*, 71.
[239] Renée Jeffery, *Evil and International Relations: Human Suffering in an Age of Terror* (New York: Palgrave Macmillan, 2008), 127-128.
[240] Doğu Ergil, "Uluslararası Terörizm," *Ankara Üniversitesi Siyasal Bilgiler Fakültesi Dergisi* 47-3 (1992): 139, E.T.: 21 Temmuz 2018, url.: http://dergiler.ankara.edu.tr/dergiler/42/457/5195.pdf.
[241] Bayraktar, *Siber Savaş ve Ulusal Güvenlik Stratejisi*, 70.
[242] Çakmak ve Altunok, *Suç, Terör ve Savaş Üçgeninde Siber Dünya*, 36-39.

karşı şiddet içeren, bunun korkusunu yaratacak şekilde zarara sebep olan saldırıları siber terörizm olarak adlandırmıştır.[243]

Siber terör eylemleri, yasadışı biçimde; sanal ağlar, bilgisayarlar ve depo sistemlerini hedeflemektedir. Eylem biçiminde; hükümet ya da kişilere, eylemi gerçekleştiren tarafın sosyal, politik ya da ideolojik niyetlerinin zorla kabul ettirilmesini kapsamaktadır. Eylemlerin sonucu; mal ve can bütünlüğüne zarar getirmek ya da en azından bunun korkusunu yaşatmaktır. Eylemler, siber ortam aracılığıyla, iletişim ya da ulaşıma zarar verilmesi, halk sağlığı hizmeti veren sistemlerin altyapılarına kast edilmesi, sabotajlar gibi vatandaşların aldığı kamu hizmetlerinin engellenmesi şeklindedir. Direkt can kaybı ya da yaralanmalar oluşması, şirket, kişi ya da kurumların maddi kayıplara uğraması amaçlı eylemleri kapsamaktadır.[244] Teknolojinin ilerlemesiyle siber alan, sıradan kullanıcılar dışında, terörist örgütlerinin dikkatini çekmiştir. Sağladıkları kontrol genişliği, rahat yayılma sayesinde iletişimin sınırsız olması, terörist örgütler için silah yerine geçmektedir.[245] Siber alanın getirdikleri, siber terör eylemleri için ortamı ilgi çekici kılmıştır. Kullanım kolaylığıysa istenilen hedefe teknoloji üzerinden rahat ulaşım sağlanabilmesi, ortamın daha çok dikkat çekici olmasını sağlamıştır.

Siber alanın örgüler için faydası; internet üzerinden birçok liderin, farklı ülkelerden, eş zamanlı faaliyetler gösterme imkânıdır. Kamuoyunu yanlı bilgiyle uluslararası alanda istismar edebilme özelliği varken, daha önemlisi maddi anlamda maliyetlerin düşük, etkilerin yüksek olmasıdır.[246] Örgütler ortamla az maliyet harcamaktadır. Ayrıca siber alandan personeli kolayca bulabilmekte, yöntemler kolaylaşmaktadır. Fazla ileri teknolojiye gereksinim duyulmaması, yapanın anonim kalması tespiti zorlaştırmaktadır. Uzak yerlere saldırma şansını vermesi, medyada kendilerini gösterebilme imkânı sunması en büyük hedef olan halka ulaşmayı hatta propagandayı gerçekleştirmeyi sağlamaktadır. Ek olarak; siber alanın merkezi bir kontrolü olmaması, sınırsız bir alan olması, herkese ulaşıma açık olup, bilgiye ulaşımın kolay olması önemlidir.[247]

---

[243] Dorothy E. Denning, "Cyberterrorism," *Naval Postgarduated School* (2000): 1, E.T. 20 Temmuz 2018, url: https://calhoun.nps.edu/handle/10945/55351.

[244] Murat Güneştaş vd., "Siber Terörizm: Motivasyon ve Yöntem," *Siber Suçlar: Tehditler, Farkındalık ve Mücadele*, ed. Fatih Tombul vd. (Ankara: Global Politika ve Strateji Yayınları, Ocak 2015), 89.

[245] Çakmak ve Altunok, *Suç, Terör ve Savaş Üçgeninde Siber Dünya*, 85.

[246] Çakmak ve Altunok, *Suç, Terör ve Savaş Üçgeninde Siber Dünya*, 86.

[247] Çakmak ve Altunok, *Suç, Terör ve Savaş Üçgeninde Siber Dünya,* 37-38.

Siber alanın özellikleriyle faaliyetlerin kolaylaşması, bazı gruplara göre avantajı olması, alanın cazip hale gelmesini sağlamıştır. Yapılan eylemler birebir terörizm denilemese bile, faaliyetler için bir araç olarak görülüp, eğitim gibi çalışmaları alan içerisinde yapabilme imkânları sunmaktadır. Ağ ve bilgisayar ortamlarına istenen amaçlar üzerinden saldırarak bir terör gerçekleştirmek, siber terör olarak adlandırılmaktadır. Terörizmle siber ortamın kesişebildiği noktalarda bu görülmektedir.[248] Bir terör olayı tamamen siber ortam üzerinden ciddi sonuçlar doğuracak biçimde uygulanmamıştır. Ancak avantajları kullanılmış, özellikle günümüzde eğitim ya da haberleşme olarak daha ön plana çıkmıştır.

Siber terör günümüzde kullanılmaktadır. Ancak klasik yöntemlerden vazgeçilmediği bilinmektedir. Siber terörle klasik anlamda terör arasında farklılıklar vardır. Siber terörü normal terörden ayıran temel farklılıklar; eylemleri gerçekleştirmek için bilgisayara ihtiyaç duyulmasıdır. Amaç ve araç açısından birbirine karışmıştır. Sanal şiddette siber alan, bir araç olmaktan amaca dönüşmüştür. Siber uzayda olaylar gerçekleşse bile, yansımaları gerçek dünyada görülüp, geniş kitlelere yayılmak suretiyle yıkıcı etkileri olmaktadır. Teröristlerin aldığı risklerin daha aza inmesi de siber terörü normal terörden farklı kılan özelliklerdendir.[249] Genel anlamda; siber terörün bilinen klasik anlamda terörden farkı; bilgisayar ortamında gerçekleşerek, siber alanda uygulanan şiddetle geniş kitlelere yayılıp, fiziksel dünyada yansımaları olmasıdır.

Siber terörizm iki sınıfa ayırılır. Sadece hedefte olan yapıyı zayıflatma, maddi kazanç, güvenirlikte sarsılma yaratmak amaçlı olan, şiddet içermeyen siber terör eylemleri vardır. Ayrıca, hedef alınan yapıyı yok etme, yıpratma ya da yıldırma amaçlı, şiddet içerikli siber terör eylemleri bulunmaktadır.[250] İkisi de terörü içerir, ancak şiddetin boyutu, yapılan eyleme göre değişir.

Siber terör kapsamına girecek eylemler, halkta endişe ve korku yaratma amaçlı olduğundan önemlidir. Sosyal medya üzerinden, devlet ya da hükümete ait sayfaların, resmi hesaplarının ele geçirilip, propaganda amaçlı yayınlar yapılması tehlikelidir. Özellikle; siyasi figürlere ait sayfalar üzerinden bunu yapmak, devlete karşı güveni kırıp, aynı zamanda halkta endişe duygusu oluşturabilecek bir yöntemdir. Sosyal medyada istihbarat amaçlı veriler toplamak, örgütler için

[248] Çakmak ve Altunok, *Suç, Terör ve Savaş Üçgeninde Siber Dünya*, 38.
[249] Bayraktar, *Siber Savaş ve Ulusal Güvenlik Stratejisi*, 76-77.
[250] Bayraktar, *Siber Savaş ve Ulusal Güvenlik Stratejisi*, 78.

eleman kazanmak amaçlı, belirli platformlar üzerinden eylemlerde bulunmaktadırlar. Ayrıca yapılan terör eylemlerini sosyal medya üzerinden duyurarak, bunu üstlendiğini göstermektedirler. Bir olay çıktığında kişi ya da kurumu hedef göstermek suretiyle kışkırtma yapmak, eylemler için kullanılacak materyalleri, eğitim faaliyetlerini alan üzerinden göstermektedirler. İletişimin kolaylığını alan üzerinden kullanıp, halkta korku ve panik duygusunu arttırmaktadırlar.[251] Siber alanın terör eylemlerinde kullanılması, eylemler için avantajlı görünmesine sebep olmuştur. Herkesin erişim kolaylığı, ortamın rahat kullanımıyla amaçlara istenilen şekilde hizmet edebildiğini göstermektedir. Eylemi gerçekleştirenin kim olduğunu bulmak zor olduğu için, eylemi yapana bir avantaj olmaktadır.

Siber terör olarak değerlendirilebilecek ilk saldırı; Sri Lanka'da gerçekleşmiştir. Ağustos 1998'de, Tamil Kaplanları (Liberatin Tigers of Tamil Eelam/Tamil Tigers [LTTE]) isimli örgütün kollarından bir tanesi olan, Kara Kaplanlar (Black Tigers)'ın yapmış olduğu eylemdir. Eylem Sri Lanka'nın kendi büyükelçiliğini hedef alarak yapılan yoğun e-posta saldırısıdır.[252] Saldırı iki hafta sürmüştür. Sri Lanka'nın yurtdışındaki temsilcilikleri hedef alınarak, yaklaşık günde 800 civarı e-posta gönderilmiştir. Bu yöntemle elçiliklerle kamuoyunda endişe ve korku oluşturmuşlardır.[253]

Siber terör üzerine yakın zamanda söz edilecek örneklerden bir tanesi; 13 Mart 2016 tarihinde olmuştur. Ankara'da yaşanan terör eyleminin iki gün sonrasında, sosyal medya hesaplarından, korku ve panik duygusu oluşturularak, tekrar bir saldırı olacağı söylentisi yayılmıştır. Söylenti sonrası Ankara ve İstanbul gibi yerlerde korku sebebiyle pek çok insan sokağa çıkmamıştır. Terör gruplarının korku yaratma konusunda başarılı olmalarını sağlamıştır. Bu konuda çıkan haberlerde[254]; bazı yerler yas tutuyor şeklinde yazılmıştır. Tunalı Hilmi Caddesi gibi Kuğulu Park'ta patlama olma ihtimali söylentileriyleyse, Ankara'nın en işlek

[251] Güneştaş vd., "Siber Terörizm: Motivasyon ve Yöntem," 98-103.
[252] Güneştaş vd., "Siber Terörizm: Motivasyon ve Yöntem," 88.
[253] Çakmak ve Altunok, *Suç, Terör ve Savaş Üçgeninde Siber Dünya*, 42.
[254] "Ankara'daki Terör Saldırısı Sonrası Sokaklar Boş Kaldı," *Hürriyet Haber*, 15.03.2016, E.T.: 20 Temmuz 2018, url: http://www.hurriyet.com.tr/kelebek/magazin/ankaradaki-teror-saldirisi-sonrasi-sokaklar-bos-kaldi-40069679.

caddelerinden biri gün boyunca boş kalmıştır.[255] Bu olayların önüne geçilmediği sürece son olmayacaktır. Siber anlamda zamanla örneklerin artacağıysa aşikârdır. Artık iletişim ortamının daha çok siber alan üzerinden olması, haberlerin buradan yayılması, siber terörün etki alanlarından bir tanesi olmasını sağlamıştır. Örnekler siber terörün hayatımızdaki etkileri ve ileride olabileceklere ışık tutmaktadır. Alınabilecek önlemlerle gidişatın şekillenmesinde dönemin koşulları ve yapılacak eylemler vardır.

Siber terörün geleceğiyle ilgili bazı düşünceler ortaya atılmıştır. Siber terörle gruplar güçlenerek daha yıkıcı ve korku verici eylemler ortaya çıkartabilir. En olumsuzu; yaşamı tehdit edici, kitlesel bir kesintiyle kritik altyapılara büyük zarar verici ataklarla, geniş bir nüfusta güvensizliğe yol açabilir.[256] Bir terör eylemi, hayati yapıları etkileyecek biçimde sistemlere zarar verip, güvensizlik oluşturabilir. Bu terör gruplarının hedeflerine ulaşması açısından önemlidir. Bir terör ortamı oluşturmak hedeftir. Siyasi olarak verilen zararsa eylemin temelini oluşturmaktadır. Siber alan üzerinden yapılmasıysa siber terörü ortaya çıkarır.

Genel anlamda; siber terör, bilinen anlamda terörle hem benzer hem farklılaşır. İkisinin ortak noktası korku ve endişe oluşturmaktır. Verilebilecek örnekler fazla olmakta ancak önemli olan neyin siber terör olup olmadığına karar vermektir. Hem terör hem siber terörde içerisine siyasi hedef barındırması gerekir. Farklılık gösteren noktaysa; eylemin yapıldığı ortamdır. Eylemin içerisinde teknoloji ve siber alanın kullanımı ya da bu ortamda yapılması, siber terörü işaret etmektedir. Klasik anlamda bilinen terör eylemleri; daha çok fiziksel anlamda, her türlü işlemin yapılmasını kapsar. Ancak tanımlamadaki karışıklıklar, teröre bakış açısı ve eylemden kaynaklıdır. Siber terörde başka bir nokta; kurallar dışında, olağandışı biçimlerde, var olan sistemin karşısında, terör oluşturabilecek eylemler gerçekleştirilmesidir. Siber alanda kurallar ve sınırlar içerisinde, savaş eylemlerini de barındıran yapılar; siber savaşlardır. Siber savaş, siber terörden farklıdır. Kurallar, sınırlar, uygulama biçimi, savaşan aktörler farklılık göstermektedir. Benzer noktalarıysa; karşıt bir taraf için belirli eylemler gösterilmesidir. Ancak

[255] "Ankara'da 'Bombalı Saldırı Olacak Söylentisi' Tunalı Hilmi Caddesini Boşattı," *SonDakika.com*, 15.03.2016, E.T.: 20 Temmuz 2018, url: https://www.sondakika.com/haber/haber-ankara-da-bomba-saldiri-olacak-soylentisi-tunali-8263166/.

[256] Bruno Halopeau, "Terrorist Use of the Internet," içinde *Cyber Crime and Cyber Terrorism Investigator's Handbook*, derleyen: Babak Akhga vd. (Amerika: Elsevier Yayınları, 2014), 127, ISBN: 978-0-12-800743-3.

aralarındaki farklılıklar daha fazladır. Daha iyi anlaşılması içinse siber savaşı ayrıca açıklamak gerekmektedir.

1.2.4.2.2. Siber Savaş

Siber terör dışında, devletler kendi aralarında belirli düzeyde problemler yaşamaktadır. Yaşanan problemlerin en üst sınırlarından biri savaştır. Yeni gelişen teknolojiyle savaş sadece klasik anlamda kalmamış, yeni bir türü ortaya çıkmıştır. Yeni çıkan savaş türüne; teknolojiyle beraber, siber alanda meydana gelmesinden dolayı, siber savaş denir. Artık bir savaş biçimi olan siber savaş, günümüzde yaşanan olaylarla, belirli bir öneme sahip olmuştur. Günümüzde siber alanla gelişen, devletlerin arasında oluşan gerginliklerden bir tanesini siber savaştır.

Genel anlamda; siber savaşı tanımlamak için önce klasik savaştan bahsetmek gerekir. Savaş üzerine pek çok düşünür kendi döneminde tanımlamalar yapmıştır. Bazı düşünürlerin yapmış olduğu tanımlamaların etkileri günümüz siber savaşlarına kadar uzanmaktadır.

Dedeoğlu; Thomas Hobbes'un savaş tanımının adaletle bağdaştırılmadan, çarpışma yöntemiyle mücadele süreci şeklinde oluğundan söz etmiştir. Aynı zamanda Dedeoğlu; G. Frederick Hegel'in savunduğu, çatışma durumunun savaş durumuna geçmesinin, siyasal iktidarda iç gücün pekişip, yeni hareketler sağlayacak zemini hazırlayacağından bahsetmiştir.[257] Yani savaş; Hobbes için bir mücadele yöntemiyken, Hegel için siyasal iktidarda yenilik ve gücün pekişmesini sağlayacaktır.

Savaş üzerine önemli düşünürlerden bir tanesiyse Sun Tzu'dur. Sun Tzu savaşı, bir devlette baş sorun, aynı zamanda ölüm kalım, yani; yok olma, var olma yolu olarak tanımlamıştır.[258] Savaşın pek çok ayrıntılı noktası üzerine düşüncelerini ifade etmiş olan Sun Tzu, savaşın seyrinde neler yapılması gerektiğinden bahsetmiştir. Aynı zamanda savaşın aldatma sayesinde başarılı olabileceğinden söz etmiştir. Siber anlamda, saldıranın bilinememesinin

[257] Beril Dedeoğlu, *Uluslararası Güvenlik ve Strateji* (İstanbul: Yeniyüzyıl Yayınları, 2014), 132-134.
[258] Sun Tzu, *Savaş Sanatı*, Çev. Pulat Otkan ve Giray Fidan (İstanbul: Türkiye İş Bankası Kültür Yayınları, Mart 2017), 1.

avantajları da vardır.[259] Siber alanda, saldırıyı yapanı saptamak zor olduğu için, Sun Tzu'nun bahsettiği aldatma bu düşünceyle örtüşmektedir.

Craig B. Greathouse'a göre; Antoine Henri Jomini'nin kendi savaş sanatında; belirleyici noktanın, zafere ulaşmak için ezici güç kullanımından geçtiğinden bahseder. Siber anlamda, bunun devlette hassas yapılar üzerinde yapılabilecek, sonuçlarının yıkıcı olması beklenen durumlar şeklinde söz etmektedir.[260] Yani; ne kadar sert ve yıkıcı olunursa, zafer ve ekti o kadar sağlanır.

Carl von Clausewitz savaşı birebir inceleme konusu yapmış, aynı zamanda ilk defa savaşı bir politika olarak değerlendirmiştir.[261] Clausewitz, savaşta en cesur ve en dikkatli olmanın öneminden bahsetmiştir.[262] Clausewitz, savaşı, düşmana karşı kendi iradelerini kabul ettirmek amacıyla zorlayarak, bilim ve sanatın birleşimiyle, güçlenmiş kuvvetin eylemini araç olarak kullanmayı içermektedir. Hedeflenen düşmanın silahsız kalmasıdır. Savaş somut bir eylemdir. Her zaman savaşın devamının geleceği bilinmelidir. Savaşın, keskin sonuçları olmayan, gerçek olasılıklarla devam eden, politik, en önemlisi ciddi amaçlar için araç olabilen, hatta politikanın başka araçlar üzerinden devamı biçiminde olduğundan söz etmiştir.[263]

Clausewitz, savaşın ani değil birikimle oluştuğundan söz etmektedir. Politik sebeplerden ortaya çıkmakta, şiddetininse halkın varlığı ve sebeplere bağlı olarak oluştuğundan bahsetmektedir. Savaş, politikanın sadece araçlarından bir tanesi olup, politik amaçlar barındırmakta, fakat politika her zaman savaş ortaya koymamaktadır.[264] Savaşlar genelde politikalar için bir araçken, politikalar her zaman bir savaş ortaya koymak zorunda değildir. Savaşlar belirli birikimlerle ortaya çıkmaktadır. Ayrıca savaş bazı politikaların sonucunda başvurulabilecek, politikanın sağlanması amacıyla bir araç olarak kullanılabilecek bir yapıdadır. Günümüzde yapılan tanımlamalar; var olan düşünürlerin temeliyle oluşmuştur. Savaş, daha çok hükümetlere bağlı ya da bunu oluşturmak amaçlı, meşru olan

[259] Craig B. Greathouse, "Cyber War and Strategic Thought: Do the Classic Theorists Still Matter?," içinde *Cyberspace and International Relations: Theory, Prospects and Challenges*, ed. Jan-Frederik Kremer ve Benedikt Müller (London: Springer Publishing, 2014), 31.
[260] Greathouse, "Cyber War and Strategic Thought: Do the Classic Theorists Still Matter?," 28.
[261] Dedeoğlu, *Uluslararası Güvenlik ve Strateji*, 134-135.
[262] Clausewitz, *Savaşın Esasları,* 15.
[263] Carl von Clausewitz, *Savaş Üzerine,* Çev. Selma Koçak (İstanbul: Doruk Yayınları, 2015), 30-45.
[264] Clausewitz, *Savaş Üzerine,* 46-722.

organize grupların kendi arasındaki büyük çaplı şiddet içerikli çatışmaları şeklindedir.[265] Savaş içerisinde her zaman bir çatışma vardır. Ancak savaşta önemli olan; sonucunda elde edilecek başarıdır.

Genel anlamda savaş; insanların varlığından beri kendisini göstermektedir. Ancak süreçler içerisinde ihtiyaca göre değişim göstermiştir. Soğuk Savaş Döneminde, iki blok ve onun dengesi üzerinden gerginlikler devam derken, çatışmaların nükleer bir sınırda, savaşa dönüşmeden, sınırlar erimeye başlamıştır. Ancak geliştirilen askeri teknoloji gibi gelişmeleri tamamen terk etmemişlerdir.[266] Daha eski çağlarda savaş sadece insan gücü üzerinden ilerleyebilirken, günümüzde daha farklı konuma gelmiştir. Esas olarak savaş, günümüzde pek çok çeşit içeren bir hale gelmiştir. Tek yönlü savaşların artık daha az kullanıldığı, çeşitli bir savaş biçimi ortaya çıkmıştır. Ekonomik tehditlerle devletlerarasında problemler çıkabilirken, bu ekonomiye bağlı olarak, teknolojik tehditlerde yetersizlikler de ortaya çıkabilmektedir. Aynı zamanda elektronik açıdan yaşanabilecek tehditler, politik gerginliklere yol açarak, herhangi bir savaş biçimine dönüşme ihtimali vardır. Günümüzde savaşı; iki devlet arasında ortaya çıkacak gerginliklerle, çeşitli yöntemler kullanılarak karşıt devleti zarara uğratmayla zorlayıcı bir güçle, diğer devlete karşı bir çeşit teslim olmaya zorlamayı içermektedir. Ancak kullanılan yöntem ve sonuçlarına göre savaşın nasıl bir savaş türü ve hangi yöntemler kullanılarak yapıldığından söz edilebilmektedir.

Günümüzde savaşta başarı sağlamak, daha çok teknolojik yapılardan geçmektedir. Bilgi teknolojilerinin askeri alanda sağladıkları, devrim niteliğindedir. Uzaydan yapılan doğrudan yayınlar, karmaşık yazılım ve yüksek hızdaki bilgisayarlar, geniş alanda meydana gelen karışık olaylar hakkında bilgi toplamak, işlemek, aktarmak, sınıflandırmak ve kolayca yayabilme imkânı büyük avantajlar sunmaktadır.[267] Savaş teknolojiyle yapısal biçimde kendisini geliştirmeyi başarmıştır. Özellikle savaş içerisine teknolojinin daha çok dâhil olması yeni savaş alanları oluşturmuştur.

Savaş uluslararası alanda sembolik çekişmelerden, silahlı çatışmalara kadar geniş bir yelpazede tanımlanabilir. Siber savaşsa; siber bozulma ve

[265] Çakmak ve Altunok, *Suç, Terör ve Savaş Üçgeninde Siber Dünya*, 44.
[266] Rupert Smith, *Utility of Force* (New York: Vintage, 2008), 230.
[267] Nye ve Welch, *Küresel Çatışmayı ve İşbirliğini Anlamak*, 391.

barbarlıktan, siber alanın gerçek bir savaşta kullanılmasına kadar genişlemektedir.[268] Savaş, çeşitlilik göstermektedir. Siber savaşsa günümüzde önem kazanmaya başlamış bir çeşididir.

Kişisel anlamda yapılabilecek çatışmalar siber savaş değildir. Belirli bir amaç ve iki devlet gibi aktörler arasında yaşanmaktadır. Başka önemli bir noktaysa siber savaşın siber alan üzerinden yapılıyor olmasıdır.[269] Siber alanda olan savaş biçiminde, tarafların otorite ya da devlet olması gerekir. Çünkü savaşın kimler arasında olduğu, onun savaş ya da başka bir çeşit eylem olup olmadığının belirlenmesinde önemlidir. Saldırılarda dikkat çeken genelde devlet altyapıları üzerinden, toplum ve ulusal güvenliğe karşı zarar verici olmasıdır. Ayrıca finansörlerin devletler olması, askeri anlamda bir stratejinin parçası olduğunu göstermektedir.[270] Siber savaşlarda taraflar genelde devletlerdir. Burada kullanılan stratejiler savaş içerisinde de bir strateji biçiminde düşünülebilmektedir.

Siber savaş; bir devlet tarafından, onun için ya da desteklemek adına, başka hedef bir devletin bilişim ağlarına yapılan saldırılardır. Veri bozmak, değiştirmek, eklemek, siber alanda bulunan cihazların kontrol etmiş olduğu nesnelere hasar vermek, yetkisiz giriş yapmak ya da kesintiye uğratmaktır.[271] Yani; politik, ekonomik, psikolojik, askeri amaçlarla, hedef devlete yapılan iletişim ve bilgi sistemleri üzerinden organize saldırıların tümünü kapsamaktadır.[272] Genel olarak siber savaş; siber alan üzerinden yapılan, devletlerarasında, belirli amaçlar üzerinden organize biçimde savaştır.

Siber savaş, klasik savaşla ulaşılabilecek sonuçları siber alanda başarmaya çalışmayı kapsar. Bir savaşın başka boyutlarını desteklemek, sonuca ulaşılmasını kolaylaştırmak şeklinde amaçlara da yardımcı olmaktadır. Siber savaş çeşitli faaliyetlerin bir arada ilerlemesini sağlayabilmektedir. Aynı zamanda, askeri olarak da eski yöntemlerin yeni yollarla sunulmasını sağlamaktadır.[273] Siber alanda etkili olan tarafın, karşısındaki aktöre asimetrik etki yaratma yöntemiyle sonuca ulaşabilmesini ayrıca kapsamaktadır.[274] Asimetrik biçimde siber savaşlar,

[268] Singer ve Friedman *Siber Güvenlik ve Siber Savaş*, 164.
[269] Çakmak ve Altunok, *Suç, Terör ve Savaş Üçgeninde Siber Dünya*, 44-45.
[270] Solange Ghernaouti, *Cyber Power: Crime, Conflict and Security in Cyberspace* (Switzerland: EPFL Press, 2013), 155.
[271] Clarke ve Knake, *Siber Savaş*, 119.
[272] Bayraktar, *Siber Savaş ve Ulusal Güvenlik Stratejisi*, 13.
[273] Richards, *Cyber War,* 25.
[274] Çakmak ve Altunok, *Suç, Terör ve Savaş Üçgeninde Siber Dünya*, 46.

klasik savaşlara destekleyici olması dışında, tek başına bir savaş olarak da kabul edilebilir. Asimetrik özelliğiyle birey seviyesinden karmaşık yapıdaki ulusal organizasyon yapılarına kadar uzanabilmektedir. Tehdit kaynağının tespitinin zor olmasıyla, büyük etki, düşük maliyet siber savaşın önemini arttıran sebeplerdendir.[275]

Klasik savaşlarla siber savaşlar arasında belirli farklılıklar vardır. Klasik savaşlarda; silah maliyeti yüksek, ölüm riski daha fazladır. Siber savaşlarda kaynak tespiti zor, saldırı fazlasıyla hızlı gerçekleşmektedir. Ayrıca hasarın anlaşılmamasını sağlayabilen, ölüm riski az saldırılardır. Kullanılan silahların maliyeti düşük, etkisi maliyetli ve zarar verici olmasıysa zengin devletlerin bu tip savaşlarda kazanma olasılığını arttırmaktadır.[276] Siber savaş yöntemi, günümüzde klasik savaş yöntemine göre daha tercih edilebilirdir. Maliyet üzerinden başarı ihtimalinin fazlalaşması, ekonomik olarak güçlü devletlerin başarılı olma ihtimalini yükseltmektedir. Ekonomisi zayıf olan devletlerinse şansı düşüktür. Bu yüzden, bazı devletlerin klasik savaşlarda kazanma ihtimali yüksekken, siber alanda ekonomisi zayıf olanların kazanma şansı tamamen düşüktür. Siber savaşlarla klasik savaşlar arasında farklılıklar olsa da, benzerlikler de vardır. İki türün belirli savaş seviyeleri vardır. Siber savaş bazen tek başına bir savaş biçimiyken, bazen de klasik bir savaşta yan bir alan olarak kullanılmaktadır.

Siber savaşlar; operatif, taktik, stratejik olarak tüm seviyelerde uygulanabilmektedir. Her seviyede etkili olarak; devletlerin kritik altyapılarını hedef seçip, altyapıların hizmet dışında kalması, askeri ya da sivil anlamda devlette kıymetli, hassas bilgilere ulaşıp, silip, çalabilmektedir. Etkilere maruz kalan halk ve yönetim, psikolojik olarak toplumun her noktasına erişilme şansı olduğu için rahatsız olmakta, rekabet ve çatışma ortamına zemin hazırlayabilmektedir.[277] Hedef alınan devletlerin önemli alt yapıları; iletişim, enerji kaynakları, ulaşım, finans şeklinde dörde ayrılabilmektedir. Bu altyapılara gelecek saldırılar, karar vericileri etkileyecek yapıdadır. Siber saldırılar sayesinde, savaş ortamında olan kişi ya da grupların iletişimini bozmak ya da irtibatlarını koparmak, birimler arası iş birliği ve koordinasyonu bozacağından, siber savaş

[275] Bayraktar, *Siber Savaş ve Ulusal Güvenlik Stratejisi*, 18.
[276] Bayraktar, *Siber Savaş ve Ulusal Güvenlik Stratejisi*, 49-50.
[277] Bayraktar, *Siber Savaş ve Ulusal Güvenlik Stratejisi*, 48-49.

açısından önemli bir araçtır.[278] Siber savaşlar, altyapıyı ve iletişimi bozmak için kullanılmaktadır. Ancak bunun dışında pek çok kullanım biçimi de vardır.

Kısaca siber savaşların kullanım şekli; taktiksel, operasyonel, stratejik düzeylerdedir. Taktiksel olarak; sistemleri etkilemek, rakipleri operasyonel düzeyde senkronize ve kitlesel olma yeteneklerini, üst düzey liderliğin açık durumsal farkındalığı sürdürme yeteneğini etkilemektir. Aynı zamanda, ulusal güvenlik ortamında stratejik etkilenmelere sebep olmaktadır.[279]

Operasyonel siber savaş; daha çok gerçek savaşlara destek vermek amaçlı kullanılmaktadır.[280] Rakibin silahlı kuvvetleri, askeri hedefleri, bunlara bağlı sivil hedeflerine yapılabilen siber saldırıları kapsamaktadır.[281] Yani; operasyonel amaçlarla bir siber savaş yöntemi kullanımıdır. Daha çok bir uygulama biçimi olmaktadır. Yardımcı bir yöntem olarak düşünmekte mümkündür.

Stratejik siber savaşın önemli noktası; askeri, havayolu trafiği, devletin elektrik altyapısı hedefli yapılabilmektedir. Sonuçlarındaysa; elektronik, fiziksel, diplomatik etkileri görmek mümkündür.[282] Hasan Çiftçi'nin bahsettiği üzere; Martin Libicki; devlet ya da topluma, devletin tutumunu değiştirme amaçlı yapılan saldırıların stratejik anlamda siber savaş olduğundan söz etmiştir.[283] Saldırılar belirli periyodlarda yapılır. Buna karşı stratejik anlamda birey, kurumların belirli bir ortak noktada buluşması, devlet ve olası savaş ihtimali için rakip devletlere karşı kolaylık sağlamaktadır.[284] Siber savaşta stratejik yöntemler, bir hedefe ulaşma amaçlı izlenen yoldur. Bir amaç üzerinden, onun için yapılan saldırıları kapsamaktadır. Siber alan üzerinden yapılan siber savaşların sonuçları sadece bu alan üzerinden değil, pek çok alanda görülebilecek biçimdedir.

Siber savaşta başka önemli noktalar da bulunmaktadır. Siber savaş politikanın ve yasal antlaşmaların ilerisindedir. Barış zamanı için bir çaredir. Coğrafya hala önemli olmakla beraber henüz siber savaş gelişimini tamamlamamıştır.[285] Siber savaşın çoğu özelliğinin oturması ve sonuçlarının daha

[278] Çakmak ve Altunok, *Suç, Terör ve Savaş Üçgeninde Siber Dünya*, 46.
[279] Brian M. Mazanec ve Bradley A. Thayer, *Deterring Cyber Warfare: Bolstering Strategic Stability in Cyberspace* (Basingstoke: Palgrave Macmillan, 2015), 16. doi: 10.1057/9781137476180.0005.
[280] Başaran, *Siber Savaş Cephesinden Notlar*, 44.
[281] Keleştemur, *Siber İstihbarat*, 158.
[282] Başaran, *Siber Savaş Cephesinden Notlar,* 43.
[283] Çiftçi, *Her Yönüyle Siber Savaş*, 19.
[284] Keleştemur, *Siber İstihbarat*, 158.
[285] Danny Steed, "The Strategic Implications of Cyber Warfare," içinde *Cyber Warfare: A Multidiciplinary Analysis,* ed.: James A. Green (New York: Routhledge Yayınları, 2015), 83-89.

açık görülmesi için daha pek çok olay ve süre geçmesi gerekmektedir. Siber savaş; yapılan antlaşmalar, barışın ötesinde oluşu, aynı zamanda anlık olaylar için barışı bozmadan, belirli politikaların yürütülmesinde kullanılmaktadır.

Siber alan kullanımı Soğuk Savaş'ın bitmesiyle artmış, geniş kullanıcı topluluklarına yayılmıştır.[286] İnternet ve teknoloji sayesinde siber alan daha çok kullanıcıya ulaşmıştır. Çeşitli kullanıcı ve artan kullanım sayısıyla siber alan küresel bir yapıya dönüşmeye başlamıştır. Siber alanın coğrafi sınırları aşan bir şekle dönüşmesiyse siber savaşları küresel düşünmeye sebep olmuştur. Çünkü dünyanın herhangi bir yerinde yaşanan bir siber savaş, başka bir yerdeki devleti etkilemektedir.[287] Siber alan ve internetin kullanımıyla uluslararası nitelikte iletişimi artmıştır. İletişim sayesinde yaşanan bir olay, dünyanın başka bir yerinde etki gösterebilecek konuma gelmiştir.

İnternet ve bilgisayar kullanımları çok yaygın bir konumdayken, bir bilgisayarın savaşta ilk kullanımı; İkinci Dünya Savaşı dönemi içinde olmuştur. 1943 yılında, İngiltere'de, Almanların mesajlarının deşifresi amaçlı geliştirilerek kullanılmıştır. İlerleyen dönemlerdeyse, teknolojik gelişmelerle daha çok bu alana girmeye devam etmiştir.[288]

Siber alan savaşlarda bir yöntem olarak kullanılmış, daha öncesinde de kendisini göstermiştir. Ancak siber savaşın tam olarak, ilk ortaya çıkışı; 1990'daki, Irak'ın Kuveyt'i işgali ve sonrasındaki Körfez Savaşına kadar dayanmaktadır. Savaştaki siber anlamda en önemli nokta; elektromanyetik yapıdaki sistemlerin, benzer şekilde, karşı tarafın aynı sistemleri kullanması sayesinde, kullanılamaz hale gelmesini kapsamaktadır.[289] Siber alan 1990 yılı sonrasında, önceki senelere göre daha etkin bir hâle dönüşmüştür.

1994 yılı Aralık ayında, siber alanda önemli bir başka örnek; Çeçenistan'ın başkentine giren Rus birliklerinin olayın kısa sürede çözüleceğini düşünmesiyle ortaya çıkmıştır. Ancak bu olayda; askeri çatışma ilk defa internet ortamına yansımıştır. Çeçenler medyayla birlikte interneti bir savaş alanı olarak kullanmış, daha çok propaganda ve bilgi üzerinden ilerlemiştir.[290]

---

[286] Bıçakçı, *21. Yüzyılda Siber Güvenlik*, 29.
[287] Keleştemur, *Siber İstihbarat*, 136.
[288] TÜBİTAK, *Elinizin Altındaki Gerçekler: Buluşlar ve Teknoloji, Savunma ve Güvenlik,* Ed.: Tom Jackon, Çev.: Fahri Öz (Ankara: TÜBİTAK Popüler Bilim Kitapları, Ekim 2014), 32.
[289] Ünal, *Siber Güvenlik ve Elektronik Bileşenleri*, 118.
[290] Bıçakçı, *21. Yüzyılda Siber Güvenlik*, 30.

1998 yılı Mayıs ayında, Endonezya'da ortaya çıkan, Çin'e karşıt gösterilere tepki amaçlı "China Hacker Emergency Meeting Center (Çin Hacker Acil Toplanma Merkezi)" isimli, ortalama 3000 civarında hacker, Endonezya hükümet web sitelerine saldırmıştır. 7 Mayıs 1999'da; NATO (North Atlantic Treaty Organization- Kuzey Atlantik Antlaşması Örgütü)'nun savaş uçağı, Yugoslavya-Belgrad'da bulunan Çin Büyükelçiliğini bombalamıştır. Akabinde 12 saat geçmeden, ABD hükümetinin yüzlerce sitesi Çin Halk Cumhuriyeti'nden gelen yoğun siber saldırılara maruz kalmıştır.[291] 2001 yılında; New York Times gazetesinde yayınlanan, dünyanın I. Dünya Siber Savaşı (World Web War I) olarak adlandırılan olay yaşanmıştır. Çin Halk Cumhuriyeti ordusunun bir uçağının, Güney Çin Denizi üzerindeyken, ABD'ye ait bir savaş uçağıyla çarpışması sonrasında ortalama 80.000 Çin asıllı hacker ABD hükümetine saldırmıştır.[292] Estonya'da yaşanmış olan, 27 Nisan 2007 tarihli saldırı önemli başka bir örnektir. Soğuk Savaş döneminin bitiminden sonra, Estonya'da artış gösteren Rus kökenli kişilerle, Estonlar ve Ruslar arasındaki gerginlik, iç politikada problemlere sebep olmuştur.[293] Estonya'nın başkenti Tallinn'de, 1947 yılında yapılmış olan, Kızıl Ordunun girişinin sembolü "Bronz asker" adlı heykelin 2007 Nisan ayında askeri mezarlığa taşınması olayı başlatmıştır. 1980 yılından beri ilk defa etnik bir ayaklanmaya sebep olmuş, Rus asıllı Estonyalılar sokaklara çıkmıştır.[294] 27 Nisan akşamında siber saldırılar kendini göstermiştir. Rus sitelerin, özellikle forumlarda teknik bilgiler öğretilmek suretiyle, Estonya adresleri işaret edilerek saldırılar daha ciddi boyutlara gelmiştir.[295]

2006 yılında, Suriyeli bir üst düzey yetkilinin, İsrailli bir ajan tarafından bilgisayarına girilip virüs bırakılması sonucu yeni bir olay ortaya çıkmıştır. Bilgisayar hafızasında bulunan bir fotoğrafla, Suriye'de nükleer bomba yapım amaçlı gizli bir tesisin inşa edildiği ortaya çıkmıştır.[296] Tespit üzerine İsrail harekete geçmiştir. 6 Eylül 2007'de Orchard Operasyonu başlamıştır. İsrail F15 ve F16'sı, Suriye'nin kuzey tarafında olan nükleer tesisi bombalamıştır. Önemli noktaysa; uçakların teknolojik radarlardan kaçabilecek kapasitede olmamasına

[291] Başaran, *Siber Savaş Cephesinden Notlar*, 37-38.
[292] Başaran, *Siber Savaş Cephesinden Notlar*, 38.
[293] Bıçakçı, *21. Yüzyılda Siber Güvenlik*, 33.
[294] Martin Ehala, "The Bronze Soldier: Identity Threat and Maintenance in Estonia," *Journal of Baltic Studies* 40/1 (2009): 139, E.T.: 22 Temmuz 2018, Doi: 10.1080/01629770902722294.
[295] Bıçakçı, *21. Yüzyılda Siber Güvenlik,* 34.
[296] Singer ve Friedman *Siber Güvenlik ve Siber Savaş*, 172-173.

rağmen, Suriye'nin hava savunma sistemleri tarafından tespit edilememiş olmasıdır. Başarının; saldırı öncesi Suriye radar sistemlerine girilerek, istenilen görüntüyü yüklemek kaydıyla, İsrail uçakları geçtiğinde uçakların fark edilmemesiyle sağlanmış olduğu düşünülmektedir.[297]

7 Ağustos 2008 yılındaysa; Rusya-Gürcistan arasında çıkan savaşın kabul edilen başlangıç tarihinden önce; ilk saldırı 20 Temmuz tarihinde yaşanmıştır. Dönemin Gürcistan Cumhurbaşkanı Saakashvili'nin internet sitesine büyük çaplı DDoS saldırıları olmuştur. Sonrasında hem siber hem fiziksel savaş devam etmiştir.[298] Pek çok örnek bulunmakla beraber, gün geçtikçe yeni olaylar ortaya çıkmaktadır. Ancak bu örneklerin siber savaş için özel olduğunu söylemek gerekir. Günümüzde siber saldırıların arttığı bilinmektedir. Ancak farklı biçimlere dönüşebilmektedir. Şu an bile devam eden ancak fark edilmeyen ya da çok dikkate alınmayan siber saldırılar vardır. Bir savaş biçimi olarak ya da savaşta yardımcı bir sistem olarak kullanılmasıysa verilen örneklerle daha iyi görülebilmektedir.

Genel olarak siber savaşlar; bir savaş biçimi olarak kullanılabilen ya da siber alanda tek başına var olabilecek savaşlardır. Günümüzde savaşın kendi içyapısında da değişimler yaşanmıştır. Artık yüz yüze savaşlar en az gerçekleşmesi beklenen bir hâle dönüşmüşken, bunun tamamen ortadan kalktığını söylemekte yanlıştır. Devletler içerisinde devam eden silahlı çatışmaların varlığı bilinmektedir. Ancak artık savaşlar tek boyutlu değildir. Bir savaş anında sadece askeri gücün varlığı yetersiz bir düşünce olacaktır. Çünkü askeri güç beraberinde bir teknolojik güç, ekonomik güç gibi, günümüzde önem kazanmış farklı yapıları da getirmektedir. Siber alan da artık savaş konusunda yeni bir alan olarak ortaya çıkmıştır. Siber savaşların ortaya çıkışı, teknolojiyle beraber başta yardımcı bir yapıda olsa da, artık tek başına bir savaş olarak görülmektedir.

Siber savaşlar; devletlerarasında belirli amaçlar için yapılan, siber alandaki ciddi boyutlarda saldırılardır. Aynı zamanda, bazı savaş yöntemlerinin teknoloji üzerinden uygulanabilmesini sağlar. Siber savaşlar, bilgi üzerine yapılabilmektedir. Ancak amaçlar devletten devlete değişir. Bazı siber savaşların sonuçları büyük çaplıdır. Bazılarıysa yaşanan olaya göre daha kolay çözülebilecek şekildedir. Ancak, tarihte pek çok savaşın arka planındaki sebep; bilgi

[297] Başaran, *Siber Savaş Cephesinden Notlar*, 40.
[298] Başaran, *Siber Kıyamet*, 42.

çalmaktır.[299] Bilgi her alanda önemlidir. Bir durumla alakalı en çok bilgiye sahip olan, diğerlerine göre o alanda daha üstündür. Sadece o bilgiyi elde etmek bazen yeterli olmamaktadır. Çünkü daha önemlisi bilgiyi işlemektir. Yine bilgiyi işlemek için bilgiye, belirli bir teknoloji ve ekonomiye ihtiyaç vardır. Bilgi edinmek için pek çok yöntem vardır. Bilgi karşı tarafın isteğiyle edinilse dahi, bilginin ne kadarının paylaşıldığı bilinemez. Karşı taraf bilgiyi kendi için saklı tutmak isteyebilir. Bilgiye ulaşmak, karşı tarafı tanıyıp, ona karşı politika izlemek açısından, karşı tarafın bulunduğu devlet ya da aktörün kendisine göre konumunu belirlemek amacıyla önemlidir. Günümüzde bilgiyi farklı bir biçimde, siber alan üzerinden elde etme imkânı vardır. Ayrıca bilgiyi doğru şekilde almak ya da çalmaya siber istihbarat olarak bakmak mümkündür. İstihbaratı sadece çalmak olarak düşünmemek gerekir. Bilgiyi farklı yöntemlerle elde etme metodu da denir. Siber savaşın daha iyi anlaşılması, ayrıca bilgi edinme şekillerini açıklamak için siber istihbarattan bahsetmek gerekir.

1.2.4.2.3. Siber İstihbarat

Siber savaşlarda en önemli noktalardan bir tanesi istihbarattır. İstihbarat sadece savaşlarda değil, belirli politikalar gibi pek çok alanda farklı bir yere sahiptir. Bu sebeple siber istihbarat ayrı bir başlıkta incelenmelidir. Önemli olan; istihbaratı toplayanın kim olduğudur. İstihbaratı bir devlet kendisi için topluyorsa, onun için olumludur. Ancak bir başka devlet, istihbaratı kendisinden topluyorsa, o zaman istihbarat çalışması yapılan devlet için olumsuzdur.

İstihbaratın tanımı; bilinmesi istenmeyeni ya da bilinmeyeni bilmektir. Ancak bu konuda az konuşulması, genel bir tanım yapılmasını zorlaştırmıştır. Yine de belirli bir çerçevede tanımlaması yapılmıştır.[300] İstihbarat bilgi toplama ve analizi sayesinde, karar vericilerin kararlarının gelişiminde önemli rol oynamaktadır. Karar vericilerin kendi politikalarıyla beraber toplumun algısını yönetmeyi kapsamaktadır.[301] İstihbaratta toplanan bilgiler, herhangi bir haber ya da bilgiden çok, ayıklanmış, yorumlanmış, analiz edilip değerlendirilmiş bilgilerdir.[302] Soğuk Savaş Dönemi'nden sonra istihbarat, karşı tarafın kabiliyeti, imkânlarını keşif, savaşta kullanılan araç ve silahlarını belirlemek şeklinde

[299] Keleştemur, *Siber İstihbarat*, 134.
[300] Çıtak, *Güvenlik ve İstihbarat*, 57.
[301] Bayraktar, *Siber Savaş*, 53.
[302] Çiftçi, *Her Yönüyle Siber Savaş*, 327.

algılanmaya başlanmıştır. Bu sayede askeri güç öncelik kazanmıştır.[303] Rakip ülkelerin kapasitelerinin bilinmesi, istikrara yarayabilirken, ani atakların önüne geçebilme ve tetikte olmaya yardımcıdır.[304] Bilginin güç olduğu döneme geçildiğinde, istihbaratı kuvvetli olan devletin gücünün belirleyici unsurlarından biri; istihbarat gücüdür.[305] Günümüzde; gelişen teknolojiyle istihbarat daha çok siber alana kaymaya başlamıştır.[306] Siber anlamda istihbarat, hem veri yakalama, hem kolay, ucuz, sonuçları açısından daha az tehlikeli olup, tercih edilebilirliği artmıştır.[307] İstihbarat, geçmişten beri vardır. Bilginin önemli olduğu her dönemde, her ortamda istihbarat vardır. Zaman içerisinde neyin bilgisinin toplanması gerektiği üzerine değişimler yaşanmıştır. Bilginin toplanma amacı; her zaman toplayan için, karşısındaki üzerinden, kendi konumu ve gücünü belirleyerek, kendini geliştirme ya da politika üretme şeklindedir. İstihbarat toplama şekilleri döneme ve içinde bulunulan duruma göre değişiklik gösterir. Günümüzde; siber alanın yükselişi, gelen kolaylıklarla, bazı eski yöntemlerden çok tercih edilerek, alan üzerinden istihbarat yöntemlerine yönelme başlamıştır.

İstihbaratın gelişimi teorik olarak, Sun Tzu'nun düşüncelerine kadar gitmektedir. Gökhan Bayraktar'a göre; Sun Tzu, savaş sanatında, hâkimiyetin aldatmacaya dayanması, zafere ulaşmak için bilgiye hâkim olmanın öneminden söz etmektedir. Bunu istihbarata bağlı şekilde vurgulamaktadır.[308] Sun Tzu; zafere ulaşmak için, yaşanacakları önceden bilmenin öneminden bahsetmiştir. Bunu ancak erdemli komutan ve akıllı hükümdarın başarabileceğinden, üstesindense zeki ve üstün kişilerin gelebileceğinden söz ederek savaşın önemli bir noktası olduğundan bahsetmiştir.[309] Yani Sun Tzu; savaşta başarılı olabilmek için bilgiye ihtiyaç olduğundan bahsetmiştir. Bunu doğru özelliklere sahip kişinin, belirli yöntemler içerisinde, istihbaratı kullanabileceği şekilde söz etmiştir. İstihbaratı yapan ve yapma şekilleri çeşitlenmektedir. Günümüzde tercih edilenler içerisinde siber istihbarat ayrı bir öneme sahiptir.

[303] Bayraktar, *Siber Savaş*, 53.
[304] Clarke ve Knake, *Siber Savaş*, 121.
[305] Çıtak, *Güvenlik ve İstihbarat*, 58.
[306] Bayraktar, *Siber Savaş*, 53.
[307] Clarke ve Knake, *Siber Savaş*, 123.
[308] Bayraktar, *Siber Savaş*, 55.
[309] Tzu, *Savaş Sanatı*, 41-43.

Siber istihbarat; dijital ortamda saklanan, kişisel ya da devlet kademesine ait bilgilere kadar önemli verilere ulaşılmak amaçlı yapılan istihbarat şeklidir.[310] Siber casusluk; kullanıcının haberi olmadan, siber saldırı yöntemleri sayesinde kurumsal, kişisel, gizli, hassas bilgilerin ekonomik, askeri, kişisel amaçlarla elde edilmesidir.[311] Siber istihbarat ve siber casusluk, birbirine karışabilse de aynı değildir. Casusluk ve istihbarat arasında farklılık bulunmaktadır. İstihbarat bir kurum, süreç, bilgi, ürünü nitelemektedir.[312] Casusluksa; açık istihbarat sayesinde ulaşılamayan, rakiplerin plan, faaliyet veya kaynakları hakkında bilgilerin gizli ve tehlikeli yollarla erişilip, toplanabilmesi şeklindedir.[313] Önemli olan; istihbarattır. İstihbarat yapılırken, özellikle günümüzde, siber alanda belirli yöntemler izlenmektedir. Genel anlamda; siber istihbarat yöntemleri elektronik, açık kaynak ve sosyal ağlara dayanan biçimde üçe ayrılmaktadır.[314]

Siber Elektronik İstihbarat; sistemler ve içerisindeki yazılımlar sayesinde bilgi toplamadır. En çok tercih edilen yöntemler; yazılımlar, e-postalar, elektromanyetik dalgalar gibi elektronik yapılar üzerindendir.[315] Siber elektronik istihbarat, genel anlamda; elektronik yapılar üzerinden, bilgi edinme amaçlı kullanılan, sistemler sayesinde bilgileri edinmeye yarayan istihbarat sistemidir.

Siber Açık Kaynak İstihbaratı; medya ve topluma sunulabilen kaynakların kullanımıyla yapılabilen istihbarat biçimidir. Sadece amaç bilgi toplamak değildir. Politik amaçlarla medya ve açık kaynakların kullanılabilmesine de yaramaktadır.[316] Açık kaynaklar genellikle; herkesin ulaşabileceği bir kaynak yapısıdır. Ana bilgi sadece buradan alınmamakta, elde edilen gizli bilginin doğruluğunu kontrol etmek amaçlı kullanılabilmektedir.[317] Siber açık kaynak istihbaratı, açık kaynak biçiminde, ulaşımı zor olmayan, herkese ulaşımı açık olan bilgiler üzerinden bilgi toplanmasını kapsamaktadır. Daha öncelikli olanıysa; bilginin kontrolü amaçlı kullanılabilen bir yöntem olmasıdır.

Sosyal Ağlara Dayalı Siber İstihbarat; daha çok sosyal mühendislik üzerindendir. Sosyal mühendislik "bir kişinin davranışını en iyi şekilde isteyerek

[310] Keleştemur, *Siber İstihbarat*, 75.
[311] Bayraktar, *Siber Savaş*, 51.
[312] KURGAN, *Siber Mücadeleye Giriş*, 199.
[313] K. Lee Lerner ve Brenda Wilmoth Lerner, *Encyclopedia of Espionage, Intelligence, and Security* (ABD: Thomson Gale, 2004), 413.
[314] Bayraktar, *Siber Savaş*, 62.
[315] Bayraktar, *Siber Savaş*, 62-66.
[316] Bayraktar, *Siber Savaş*, 66-67.
[317] Keleştemur, *Siber İstihbarat*, 55.

ya da istemeyerek etkilemeyi sağlamaktır."[318] Yani; insanların, kendi arasındaki iletişim ve davranış modellerindeki açıklıklardan yararlanarak, güvenliği atlatıp, kişilerin kendi hakkında sosyal medya gibi pek çok yerde paylaştığı bilgilere ulaşarak bilgi toplayama aracıdır.[319] Yöntem, kullandığımız sosyal medyadaki herhangi bir paylaşım, önemsiz bir konuşmada dahi geçerlidir. Bilgi toplama yöntemleri, birey ya da devlet seviyesinde, fark oluşturmaksızın yaşandığı bilinmektedir.

Bilgi toplama işlemleri, birey ya da devlet tarafından talep edilebilirken, bunu sağlayabilen sadece kurumlar değildir. Bazı şirketler aynı biçimde hizmet vermektedir. 'Sınır Tanımayan Gazeteciler' isimli bir birliğin yayımladığı; "İnternet'in Düşmanları" isimli raporda; birkaç firma için "siber paralı asker (cyber mercenary)" şeklinde bir tanımlama yapılmıştır. Siber anlamda istihbarat toplayan bazı firmalarsa; Trovicor (Almanya), Blue Coat (ABD), Amesys (Fransa), Gamma Group (İngiltere), Hacking Team (İtalya) şeklindedir.[320] Bu firmalar gibi günümüzde sayısı düşünülenden fazla olan pek çok firma vardır. Bazı firmalar devlet adına çalışmakta, bazısı bireysel çıkarlar için bilgi toplamaktadır.

Bilgi toplama, yani; istihbarattan söz ederken, belirli önemli olaylardan da söz etmek gerekir. İstihbarat üzerine, siber anlamda ortaya çıkmış olan önemli bir olay, 2009 yılında yaşanmıştır. 2009 Nisan ayında, ABD'nin sistemine izinsiz girilmiştir. F-35 uçağı üzerine, özellikle tasarım ve sistemle alakalı önemli bilgiler indirilmiştir. Aynı sistemde bulunmayan başka bilgilere sistemden bağımsız oldukları için ulaşılamamış, ulaşılabildiği kadarıyla en fazla eylemi gerçekleştiren olarak Çin Halk Cumhuriyeti hükümetine kadar izleri bulunmuştur.[321] Olay; yapılan bir istihbarat çalışması sonrası, siber alanın avantajı olan; kimin yaptığının izinin takip edilememesini gösterir. Ancak, iki rakip devletten birinin diğerinden ciddi derecede bir bilgiyi, kısa sürede sızdırmış olması, siber istihbaratın önemini göstermektedir.

2013 yılında ortaya çıkan başka bir olaysa; İngiliz Dijital İstihbarat Servisi (Government Communications Headquarters –GCHQ), Belçika'nın Belgacom

[318] Janine Kremling ve Amanda M. Sharp Parker, *Cyberspace, Cybersecurity, and Cybercrime* (ABD: SAGE Publications, 2017), 196.
[319] Bayraktar, *Siber Savaş*, 69.
[320] Başaran, *Siber Savaş Cephesinden Notlar*, 135.
[321] Clarke ve Knake, *Siber Savaş*, 124.

altyapısına sızmıştır. Şifreli e-postaları okuyacak şekilde bilgi toplamıştır. Belgacom'un konumunun Avrupa geneli ve Avrupa'nın internet bağlantısını Afrika, ABD, Ortadoğu ve Asya ile bağlayan internet ağ ve trafiğinin önemli bir kısmını bu bağlantı üzerinden geçmesinden dolayı, İngiltere dinleme işleminde pek çok yeri daha kolay dinlemiştir.[322] İngiltere yapmış olduğu istihbarat çalışmasında; tek bir işlemle birçok ülkenin bilgilerine erişimi sağlamıştır. Bilgi toplama işlemindeyse, siber istihbaratın hem önemini hem de normal bir istihbarat biçiminde elde edilemeyen bilgiyi tek seferde, kolayca elde ettiğini söylemek mümkündür.

İstihbarat açısından önemli yapılardan bir tanesi; ECHELON'dur. ECHELON, 1947 yılında, merkezi ABD'de, istihbarat amaçlı kurulmuştur. Askeri amaçlarla değil, daha çok siviller üzerinden istihbarat toplayan bir sistemdir.[323] Sistem içerisinde; ABD, Kanada, İngiltere ve Yeni Zelanda bulunmaktadır. Ortak bir girişimdir.[324] Sistem tek bir ülkede işlememektedir. Çalışma sistemi; hedefin seçilmesiyle belirlenen anahtar kelimeler gibi verilerin üzerinden, istihbarati girişimlerde bulunmaktır.[325] Anahtar kelimelerin belirlenmesi; işlemin kolaylaşması sağlamıştır. Siber ortamda büyük bir akış olduğu bilinmektedir. Dönem ve istihbarat biçimi fark etmeksizin, bilginin belirli sınırlar ya da anahtar kelimeler içerisinde yapılması, bilgi kirliliğinden korumaktadır. Günümüzde eskisinden daha çok bilginin, hatta yanlış ve karmaşık bilgilerin, her ortamda dolaştığı bilinmektedir.

İstihbarat genel olarak; bilgi toplamaktır. Politik ya da belirli amaçlar için kullanılmasıysa istihbaratı farklı kılar. İstihbarat bazen faydalı olabilmektedir. Bilgi toplanıp, kendi haberi olmadan özel bilgileri ele geçirilen taraf içinse olumsuzdur. Sadece istihbaratı bir savaş yapısı olarak düşünmemek gerekir. Normal kullanımı dışında, istihbarat, bir savunma sistemi olarak da kullanılır. Rakibin sistemi, yapısı bilindiğinde, gelecek bir tehdide karşı savunma rahat ve dikkatli olacaktır. Zafer elde etmekte önemli bir yeri vardır. Kısacası; istihbaratın savaş, savunma ya da her ikisinin bulunmadığı dönemlerde kullanılması, onu belirli bir yapı içerisine koymayı zorlaştırır. İçinde bulunan duruma göre; kullanım yöntemi ve yerleri değişebilmektedir. Genel anlamda istihbarat; bir bilgi

[322] Başaran, *Siber Kıyamet*, 49-51.
[323] Nedret Ersanel, *Siber İstihbarat* (İstanbul: Hayy Kitap, Ekim 2005), 100.
[324] Keleştemur, *Siber İstihbarat*, 87.
[325] Ersanel, *Siber İstihbarat,* 104.

toplama yöntemiyken, alınan bilginin kullanıldığı amaç, istihbaratın yapılma sebebini de değiştirmektedir. Bu sebeple istihbarat tek taraflı değildir. Bir aktörün savaşırken ihtiyaç duyacağı istihbarata, savunma sırasında da ihtiyaç olmaktadır. Savunmanın hem fiziksel hayatta hem siber ortamda özel bir yeri vardır. Savunmayı savaşın olmadığı zaman ya da olabilme ihtimalinde, hatta savaş içerisinde görmek mümkündür. Siber savunmanın özellikleri; hem bu konularla bağlantılı, hem ayrı incelenmesi gerekir. Bu konuların daha iyi anlaşılması için siber savunmadan ayrı bir başlıkta bahsetmek gerekir.

1.2.5. Siber Savunma

Siber alanda başka önemli kısım; savunmadır. İstihbarat sayesinde, bilinen başka deneyim ya da bilgilerle savunma sistemi, bir ülkede kendi kendine oturabilir. Ancak savunmanın güçlü olması bir saldırı karşısında en az zararla atlatılabilmesini sağlar.

Savunma genel olarak; bir zararı geri çevirmek, kovulmasını sağlamak şeklinde tanımlanabilir. Saldırıdan savunmanın farkı; savunmada her an bir hasarın gelme ihtimalinin beklenmesidir.[326] Savunma için genel esaslardan bahseden Carl von Clausewitz, saldırıya açık olmadan dolayı kuvvetleri dışarıya göstermeden savunmada olmak, eldeki kuvveti hemen tüketmeden yavaş yavaş kullanmayı savunmuştur. Aynı zamanda herhangi bir tehlikeye karşı her daim hazırlıklı olmaktan bahsetmiştir.[327] Ancak Clausewitz, savunmanın savaş alanıyla alakalı kısmından söz etmiştir. Teknoloji ve siber alanın ortaya çıkışıyla savunma bu alana uygulanabilecek yapılardan biri haline gelmiştir. Alan ve dönemine göre gelişme ve değişmeler göstermiştir.

Siber savunma, siber alandaki donanım, yazılım, iletişim ağlarının altyapısında oluşan bilgi sistemi, bunların bulunduğu her çeşit sistem, teçhizat ve altyapısını tehditlerden korumak amaçlıdır. Daha çok kötücül yazılım, bilinmeyen kullanıcılara karşı korumak amaçlı sistemler şeklinde tanımlanabilir.[328] İyi bir savunma için gerekli donanım ve yazılımların dışında, bunların nasıl kullanılması gerektiği, doğru bir strateji üzerinden bilinmelidir. Gerekli zamanlardaysa bir

[326] Clausewitz, *Savaş Üzerine*, 404.
[327] Clausewitz, *Savaşın Esasları*, 15-19.
[328] Bayraktar, *Siber Savaş ve Ulusal Güvenlik Stratejisi*, 92.

saldırganın neler yapabileceği düşüncesi üzerinden hareket edilmelidir.[329] Siber savunmanın önemli bir noktası; savunmanın bütünlüğünün gizliliğinin sağlamasıdır.[330] Siber savunma; siber alan üzerinden, o ortamın bulunduğu her türlü cihaz dâhil, gelebilecek tehditlere karşı belirli stratejilerle korunmasıdır.

Siber alanda bütün ihlallerin önüne geçmek mümkün değildir. Ancak, bazı konularda önüne geçebilmek için izlenebilecek belirli yöntemler vardır. Savunmaya verilen önem ne kadar çoksa, yapılabilecek saldırılara karşı savunma o kadar rahat olacaktır. Fakat ağın sürekli izlenmesi gibi faaliyetler mali açıdan yüksek, aynı zamanda sürekli teknolojinin takibini gerektirmektedir. Uluslararası siber tehditlerle en iyi başa çıkma yöntemi olarak savunma kabul edilmektedir.[331] Siber savunma, maliyetli görünse de, siber saldırının maliyeti beklenenden daha fazladır. İyi bir savunma sistemi sayesinde hasarlarla oluşabilecek maliyetin önüne geçilebilmektedir. Maliyetten daha önemlisi, korunması gereken bir verinin, hiç öğrenmemesi gereken aktörlerin eline geçmesiyle, aktöre ciddi derecede zarar verebilmesinden dolayı siber savunma önemli bir yerdedir.

Siber savunma yapılırken; bu amaçla ortaya çıkmış pek çok sistem vardır. Özellikle bilgisayar ortamında; sistemsel, donanımsal olarak pek çok çeşidi bulunan savunma sistemlerinden günümüzde rahat ulaşılabilecekleri mevcuttur. Yani; bir savunma sistemi kurmak için savunmanın gücüne göre maliyetli olabilmektedir. Ücretsiz ya da rahat ulaşılabilecek, sadece devlet düzeyinde değil, bireysel düzeyde de hizmet verebilecek, kullanımı kolay sistemler bulunmaktadır. Önemli olanlarından genel bir biçimde bahsetmek gerekir.

Anti-virüs yazılımlar; sistemleri solucan, virüs, truva atı gibi kötücül yazılımlara karşı korumak amaçlı, tespit ve temizleme için yazılmıştır. Sistemleri; bu yazılımları sınıflandırma, sezgisel (heuristic) biçimde yazılımların değişme ihtimaline karşın fark edebilme özelliğine sahip olmaktadır. Ayrıca şüpheli yazılımları belirli bir ortamda çalıştırarak takip etme koşuluyla, gerekirse sistemden ayırıp silme amaçlı yazılımlardır.[332] Sisteme sızmayı başarmış zararlı yazılımları temizlemektedir.[333] Anti-virüsler, zararlı yazılımlara ait virüs

[329] Keleştemur, *Siber İstihbarat*, 315.
[330] Çiftçi, *Her Yönüyle Siber Savaş*, 219.
[331] Sico van der Meer, "Defence, Deterrence, and Diplomacy: Foreign Policy Instruments to Increase Future Cybersecurity," içinde *Securing Cyberspace: International and Asian Perspectives*, ed.Cherian Samuel ve Munish Sharma (Hindistan: Pentagon Yayınları, 2016), 99.
[332] Bayraktar, *Siber Savaş ve Ulusal Güvenlik Stratejisi*, 92-93.
[333] Keleştemur, *Siber İstihbarat*, 320.

imzalarını kendi iç sisteminde bulundurup, bir virüsü tespit etmek için bunları kullanmaktadır.[334] Günümüzde en kolay ulaşılan sistemlerden bir tanesidir. Bir cihaz alındığında genellikle kendi içerisinde bir anti-virüsle satışa sunulmaktadır. Anti-virüs bulunmayan cihazlardaysa bu yazılımlar, internet üzerinden kolayca bulunmaktadır. Ancak bazı tehditler anti-virüsleri aşabilecek biçimdedir. Ek olarak; güvenlik duvarı gibi yazılımların bulunması, sistemin beklenen kapasitesinde çalışmasına yardımcı olmaktadır.

Güvenlik duvarları (Firewall); bilgisayar ağlarını, güvenli olup olmama biçiminde birbirinden ayıran, yetkisiz erişimlerin önüne geçebilen, belirli kriterler üzerinden çalışan sistemlerdir. Ayrıca hem yazılım olarak hem yazılım üzerinden çalışabilen bir donanım şeklindedir. Belirli filtreleme yöntemleriyle internet trafiğini kontrolde tutan sistemlerdir.[335] Güvenlik duvarı, aynı zamanda, gelen ve giden tüm veri paketlerinin içinden geçmesi gereken, kullanıcı ağının dışındaki internetle aralarında giriş noktasını oluşturan bir güvenlik sistemidir. Sistem için güvenli olan paketlerin geçişine izin verip, olmayanları sistem dışında tutar. Ancak pek çok güvenlik duvarı sorunlu bir yapıya sahiptir.[336] Güvenlik duvarları genellikle kullanıcılar, üst seviyelerdeki uygulamalar gibi sisteme bağlı otoritelerin izin verdikleri ölçüde, internet trafiği ve bilgi akışına izin verir.[337] Güvenlik duvarı çalıştığı sürede, cihaz ya da sistemin tehditlerden korunmasına, özellikle siber alandan gelebilecek tehditlerin önüne geçmeye çalışmaktadır. Ancak tam anlamıyla yeterli bir sistem koruması değildir.

Network erişim kontrolleri; bilgisayar ağında bulunan, çeşitli kullanıcılara erişimde farklı yetkiler sağlayan yazılımlardır. Ayrıca ağ çevresinde bir koruma yapısı kurarak, kullanıcılara yetkilerinin doğrulanması suretiyle sisteme girişlerine izin vermektedir.[338] Network erişim kontrolleri, cihazdaki onaylanmış kullanıcı dışında, onun izni olmadan bir erişim sağlanmasının önüne geçmek amaçlı yazılımlardır. Doğru bir kullanımla, belirli ölçüde koruma sağladığı bilinmektedir. Ancak bunun gibi başka koruma yöntemleri de vardır.

Saldırı tespiti ve önleme sistemleri (Intrusion Detection System-IDS, Intrusion Prevention System-IPS); güvenlik duvarında belirlenen kurallar

[334] Çiftçi, *Her Yönüyle Siber Savaş*, 231.
[335] Bayraktar, *Siber Savaş ve Ulusal Güvenlik Stratejisi*, 93.
[336] Alex X. Liu, *Firewall Design and Analysis* (ABD: World Scientific Publishing, 2011), 1.
[337] Grimes, *Hacking the Hacker: Learn from the Experts Who Take Down Hackers*, 95.
[338] Bayraktar, *Siber Savaş ve Ulusal Güvenlik Stratejisi*, 93.

çerçevesinde, bazı veri paketlerinin geçip geçmeyeceğine karar verme özelliğine sahiptir. Ancak bazı kötücül yazılımlar bunları aşmaktadır. Saldırı tespiti ve önleme sistemleri sayesinde güvenlik duvarını aşan kötücül yazılımlar için bilgi sistemi ve ağlarda oluşabilecekleri analiz etme gibi yöntemlerle, potansiyel zararları belirleyip, durdurmayı amaçlamaktadır.[339] Sistemler ağ trafiğini izlerken, şüpheli bir durumla karşılaştığında alarma geçen cihaz ya da yazılımlar şeklinde olduğunda tespit, saldırıyı durdurmak amaçlı bir sistemse önleme sistemleri olduğu söylenebilir.[340] Sistem; güvenlik duvarı gibi koruma sistemlerine yardımcı görünmektedir. Ayrıca bir koruma sağlayabilir. Hem uyarma hem önleme sistemi olarak iki farklı şekilde çalışması, kullanıcının bilgilenmesi ve alan üzerinde daha dikkatli ilerlemesini sağlamaktadır. Bunlarla beraber cihazlarda tarayıcı sistemler bulunduğu bilinmektedir.

Açık Tarayıcı Yazılımlar/Zafiyet Tarayıcı (Vulnerability Scanner); ağ, iletişim ve bilgisayar uygulama yazılımlarını içeren, bilgi sistemlerinde üretici, kullanıcı ya da sistem yöneticisi sebebiyle oluşabilecek zayıflıkları belirlemektedir. Aynı zamanda zayıflıkları düzeltmek amaçlı kullanılıp, tanımlanmış tüm cihazlar için sistem, güvenlik yöntemi ve izleme yapabilmektedir.[341] Tarayıcı yazılımların bazıları kullanıcının tercihine bağlı, bazılarıysa sistem içerisinde otomatik çalışabilmektedir. Önemli olan; oluşabilecek hataları belirleyip, bir kısmını düzeltme özelliğine sahip olmasıdır. Sistem dışında, kullanıcı müdahalesiyle çalışabilen koruma yöntemleri vardır. Bunlardan en önemlisi şifreleme yöntemidir.

Geçerli kullanıcı ve şifre yöntemi; sistemin kullanılmasında, sistem yöneticisinin sisteme giriş yapan kullanıcılar üzerinde, kullanıcıların sistem üzerinde sorumlulukları ve haklarını belirlemektedir. Ayrıca herkesin hak, yetki, öncelik ve kaynak kullanımlarını belirleyip, erişim izinlerinin şifreleme sayesinde denetlendiği, kötücül ya da yanlış kullanımlarda oluşabilecek problemler açısından bir savunma yöntemidir.[342] Şifreleme yöntemi verilerin okunamaması, bu sayede kötü amaçlı yazılım ve kullanıcıların erişimine engel olunması amaçlı çalışmaktadır.[343] Geçerli kullanıcı yöntemi; kullanıcılar üzerinden bir belirleme

[339] Bayraktar, *Siber Savaş ve Ulusal Güvenlik Stratejisi*, 94.
[340] Çiftçi, *Her Yönüyle Siber Savaş*, 230.
[341] Bayraktar, *Siber Savaş ve Ulusal Güvenlik Stratejisi*, 94.
[342] Bayraktar, *Siber Savaş ve Ulusal Güvenlik Stratejisi*, 94-95.
[343] Keleştemur, *Siber İstihbarat*, 327.

yapabilirken, şifreleme yöntemi; sadece şifre koyulan veri ve şifreyi koyan kullanıcıyla alakalı bir yöntemdir. Geçerli kullanıcı yöntemi kişiye sorumluluk verirken, şifreleme yöntemi şifre koyan kullanıcı tarafından, veriye zarar gelmemesi ya da ulaşılmaması amaçlı kullanılmaktadır.

Sanal özel ağ (Virtual Private Network- VPN); bilgisayar ağları arasında özel ve gizli bilgi akışında güvenlik donanım/yazılımları, tünelleme protokollerini kullanarak, oluşturulmuş özel veri hatlarıdır.[344] VPN, bir bilgisayarın, diğer bilgisayarlarla fiziksel olarak bağlı oldukları ortak ağ üzerinde, korumalı bir biçimde iletişimini sağlamaktadır.[345] Bu yöntemle kullanıcı, gezdiği ortamların herkesle paylaşımının önüne geçmektedir. Ağ üzerinden gönderilen bilgi, diğer gönderim yapılan ortamlara göre, farklı bir yerden iletilmiş gösterilip, başkaları tarafından takibin önüne geçilebilmektedir. Bu yöntem IP adreslerini gizlemek amaçlı kullanılmıştır. Dezavantaj olaraksa; bir saldırıda, kullanan kişi, yerinin bulunmaması için bu yöntemi kullanmaktadır. Sanal özel ağlar, kişinin IP adresinin yerinin korunmasına yardımcı olur. Buradaki tek problem kullanım amacıdır. Bir IP adresinin yerinin korunması farklı amaçlar için kullanıldığında sorunlar çıkabilecek düzeydedir.

Savunma yöntemlerinde, siber savunmaya yardımcı olan önemli yöntemlerden bir tanesi; kriptolamadır. Kripto cihazları; matematiksel algoritmalar üzerinden, şifrelemeyle haberleşme, bilginin güvenli iletilmesi, gerekli yerlerde trafik analizlerinde engelleme, kimlik belirleyip doğrulama imkânları sunan sistem ve cihazlardır.[346] Kriptoloji; M.Ö. 2000'li yıllarda, ilk Mısır'da Firavun mezarları için kullanılmış, ancak amaç bilgi saklamak olmamıştır.[347] M.Ö. 5. Yüzyılın başında; "Scytale[348]" isimli şifreleme cihazı, ilk defa askeri amaçla, Yunanlılar tarafından kriptografik cihaz olarak kullanılmıştır.[349] Kriptoloji ve çözümü için çalışmalar ilerleme göstermiştir. Amacı elektronik ortamların gelişmesiyle, sistemiyse matematiksel algoritmalar

[344] Bayraktar, *Siber Savaş ve Ulusal Güvenlik Stratejisi*, 95.
[345] Lerner ve Wilmoth Lerner, *Encyclopedia of Espionage, Intelligence, and Security,* 258.
[346] Bayraktar, *Siber Savaş ve Ulusal Güvenlik Stratejisi*, 95.
[347] Yılmaz ve Salcan, *Siber Uzay'da Güvenlik ve Türkiye*, 81.
[348] Yazılı bilgileri düşmanlardan saklama amaçlı, ilk Yunanlılar tarafından kullanılan silindir biçiminde ilkel bir araçtır. Ayrıntılı Bilgi için Bkz.: Zeynel A. Öztürk, "Şifreleme Nedir, Nasıl Çalışır?" *Chip,* 17 Mart 2015, E.T.: 17 Haziran 2019, url: https://www.chip.com.tr/haber/sifreleme-nedir-nasil-calisir_54659.html.
[349] KURGAN, *Siber Mücadeleye Giriş*, 225.

ve daha karmaşık sistemlere geçiş yapmıştır.[350] Kriptolama sistemi, bir bilginin başka bir yere iletiminde ya da saklanmasında özel şifreleme yöntemi olarak kullanılmaktadır. Siber bir bilginin güvenliği, o güvenliğin sağlanabilmesi için gelebilecek tehlikelere karşı savunma yöntemlerinden bir tanesi; bilgiyi bir yapı içerisinde saklamaktır.

Stenografi; bir veriyi, bir imaj içerisine gizleyen sistemdir. Sistem uygulandığında, başka birisi gördüğü zaman önemsiz bir görüntüyle karşılaştığını düşünmesi sağlanır. Ancak ulaşması gereken kişi, içine yerleştirilmiş bilgiyi görebilecek şekilde uygulanan gizleme işlemidir.[351] Stenografi ilk defa; M.Ö. 5. Yüzyılda, Heredot tarafından kullanılmıştır.[352] Bilgisayar üzerinden stenografi 2000 yılı itibariyle ortaya çıkmıştır. Şifreli bir mesajı gizlemekten çok, bir mesajın bile olmadığını gösterecek şekilde, zorunlu olmadan şifreleme biçimindedir.[353] Yöntem karmaşık bir biçimde işlenmekte, sadece haberdar olanların ulaşabilmesini sağlayacak bir yöntemdir. Kullanım açısı ve amacına göre farklı bir yer tutmaktadır. Şifreleme içerebilecek gizleme yöntemleri dışında farklı yöntemler de vardır.

Tuzak Sistemler (Honeypot); aldatma unsuru içeren, bilgi sistemlerine yapılan siber saldırılarda tespit, şaşırtma, etkisiz hale getirmeye yarayan sistemlerdir.[354] Genellikle bu sistemde, bilinçli açıklıklar bırakılarak, sisteme sızmaya çalışan ya da sızan saldırganları belirlemek amaçlı kullanılır.[355] Bal tuzağı olarak adlandırılabilen bu sistemler, kendilerini bir hedefe benzetmektedir. Bu yöntemle saldırganlar ve zararlı yazılımları üzerine çekip, izole bir ortamda sistemin çalışmasını sağlamaktadır.[356] Tuzak biçiminde işleyen bu sistemler, saldırganların yöntemlerini istenilen biçimde yakalamaktadır. Sistemi bu yönden savunma yöntemi olarak görmek mümkündür. Yöntem, saldırganı gerçek sistemden uzaklaştırmak amaçlı oluşturulmuştur. Ancak, oluşturulan sistem, sabit bazı teknik özellikleri olmasından dolayı saldırgan tarafından kolay anlaşılıp,

[350] Yılmaz ve Salcan, *Siber Uzay'da Güvenlik ve Türkiye*, 83.
[351] Keleştemur, *Siber İstihbarat*, 328.
[352] KURGAN, *Siber Mücadeleye Giriş*, 228.
[353] Merrill Warkentin, Mark B. Schmidt, ve Ernst Bekkering, "Steganography," içinde *Cyber Warfare and Cyber Terrorism*, ed. Lech J. Janczewski ve Andrew M. Colarik (Amerika: Information Science Reference, 2008), 51, ISBN: 978-1-59140-992-2, E.T.: 28 Temmuz 2018.
[354] Bayraktar, *Siber Savaş ve Ulusal Güvenlik Stratejisi*, 95.
[355] Keleştemur, *Siber İstihbarat,* 325.
[356] James Graham, Richard Howard ve Ryan Olson, *Cyber Security Essentials* (Amerika: CRC Press, 2011), 277.

kırılabilecek bir yapıya sahiptir.[357] Sistemde sorun çıkmadan çalışması amaçlı işleyen bu yöntem, tamamen önüne geçemeyeceği sorunlar dışında, sistem için istenilen ortamı oluşturabilmektedir.

Veri Kaçağı Önleme Sistemleri (Data Leakage Prevention-DLP); verilerin kullanımda, hareketli, geri kalan şekillerinde kritik düzeylerinin tespitiyle, koruma ve takibini sağlayabilen donanım, yazılım ve politikadan oluşmaktadır.[358] Bu sistem, verilerde kaçak oluşmasının önüne geçmek amaçlı ortaya çıkmıştır. Dışarıdan sızdırılmanın önüne geçebilecek bir savunma yöntemidir.

Genel olarak bu sistemler; önemli altyapılarda koruma sağlayıp, herhangi bir sızmada durdurabilme ya da savunmayı sağlayabilecek yapılardır. Savunma yöntemi; korunması gerekeni korumak amaçlı çalışmalardır. Korunacak olan; siber alan üzerinde olduğu zaman, bilinen savunma yöntemleri dışında, sistem içerisinde etkili yöntemlerle çalışmalar yapılması gerekmiştir. Bir siber alanda, alan dışında bilinen bir savunma yöntemi, sistem üzerinden yapılabilecek savunma yöntemlerinden farklı olduğundan, istenildiği biçimde bir koruma sağlayamamaktadır. Alan üzerinden oluşturulan savunma yöntemleri belirli bir düzeyde etkilidir. Ancak alanın belirli bir sınırı yoktur. Her geçen gün sistemin yenilenmesiyle savunma yöntemlerinin her zaman güncel ve yeni biçimlerinin takip edilmesi gerekir. Her yapıda olduğu gibi her sistemin, ortamın ya da şu an var olan her şeyin bir geçmişi vardır. Sadece savunma değil, genel olarak siber gelişmeleri daha rahat anlamlandırmak açısından tarihsel gelişimlerden söz etmek gerekir. Bir yapının gelişim süreci, onun günümüzde ve gelecekte nasıl şekilleneceği üzerinden en önemli bilgi vericidir. Genel bir çerçevede siber güvenliğin tarihsel altyapısından söz etmek; hem siber alanı, hem bu alandaki tehdit ve tehlikelerin ortaya çıkışına ışık tutacaktır. Aynı zamanda siber alanda savunma, savaş ve terör ihtimallerinin açıklanması açısından önemli bir yere sahiptir.

1.3. SİBER GÜVENLİĞİN TARİHSEL ALTYAPISI

Siber savunma sadece siber alanda değil, devletin temel güvenliği açısından da ayrı bir öneme sahiptir. Bilimsel ve teknik olarak, ortaya çıkan ya da

[357] Chee Keong Ng, Lei Pan ve Yang Xiang, *Honeypot Frameworks and their Applications: A New Framework* (Avustralya: Springer, 2018), 2.
[358] Çiftçi, *Her Yönüyle Siber Savaş*, 232.

yeni gelişen olgular, toplumlarda inanç, kurumsal, siyasal sistemlerde ciddi değişiklikler yaşanmasına sebep olmuştur. Bu değişmelerle toplumlara yeni güvenlik anlayışı, yeni kavram ve önlemleri getirmiştir.[359] Yeni gelişen teknoloji ve bilimsel olgularla toplum, kendileri için önemli, işlerine yarayacak olguları kendisine dâhil etmiş, tehlike oluşturabileceklere karşı önlem almaya çalışmıştır. Pek çok alanda olduğu gibi, güvenlik ve teknolojide devletler, olumlu gelişmeler dışında tehlikeli yapıların gelişimini aynı araçlar sayesinde görmüştür. Tehditlere engel olabilecek çalışmalarda bulunmuşlardır. Tehditler sadece belirli bir alanda oluşmayıp, çeşitli biçimlerde ortaya çıkmaktadır. Genel anlamda devletler; askeri tehditler dışında ekonomik, terörizm, çevresel felaket, hastalıklar, psikolojik savaşlar gibi konularda güvenlik üzerine politikalar yapmıştır.[360] Politikanın bu yönde gelişmiş olması; tehdidin nereden, ne şekilde gelebileceğinin tam tespit edilememesindendir. Özellikle siber alanın öne çıktığı bu dönemlerde, alanın bulunduğu her yerden tehdit çıkabilme ihtimali vardır. İlerleyen teknoloji, gelişen yapılarla her alan birbiriyle bağlantılı olmuştur. Alanların birbiriyle bağlantılı oluşu, tehdidin ciddi boyutlara çıktığı bir anda güvenlikle birbirini etkileyecektir.

Her devletin kendi içerisinde farklı özellikleri, beklentileri, ideolojileri, kimlikleri olması; kendine özel hedef ve tehdit algılarını getirir.[361] Devletlerdeki her sistem gibi siber alan da kendi içerisinde gelişmeler, tehlikeler ve önlemler geliştirmiştir. Siber alanın önemi, devletlerin özelliklerine göre belirli hedef ve tehditler barındırmasından kaynaklıdır. Güvenlik anlamında siber güvenlik, belirli bir yer edinmeye başlamıştır. Siber güvenlik tek başına bir güvenlik sistemi olmaktan çok milli güvenliğin parçasıdır.[362] Ancak ayrı bir önem gösterilmesi gerekir. Siber güvenlikten söz edildiğinde; altında yatan en önemli olgulardan bir tanesi; siber tehditler ve siber savaştan korunmaktır. Siber savaşların altında, bilim ve teknolojik yapılar kullanılarak oluşabilecek tehditler yatmaktadır. Bunların geçmişinde elektronik harp dönemi vardır. Elektronik harp, siber alan üzerinden ortaya çıkmış, teknolojinin dâhil olmasıyla, tarih içerisinde geçen bir savaş olmuştur. Günümüzdeki siber savaşla elektronik harbi aynı kategoride düşünebilir, hatta siber savaşın eski hali olarak bahsedilebilir. Siber alanda oluşan siber savaş ve olası tehditler; bir güvenliğin ortaya çıkmasının en temel

[359] Dedeoğlu, *Uluslararası Güvenlik ve Strateji*, 50.
[360] Çıtak, *Güvenlik ve İstihbarat*, 20.
[361] Yalçın, *Ulusal Güvenlik Stratejisi*, 18.
[362] Çiftçi, *Her Yönüyle Siber Savaş*, 249.

sebeplerindendir. Siber güvenliği daha iyi anlayabilmek için; temelini oluşturan elektronik harp gibi geçmişten günümüze kadar devam eden gelişmelerden bahsetmek gerekir.

Elektronik harbin gelişimi bir canlıya benzetilebilir. Ahmet Naci Ünal'a göre; doğuşu Birinci Dünya Savaşı olarak nitelendirilebilirken, çocukluğu İkinci Dünya Savaşı, ergenliği İkinci Dünya Savaşı Dönemi Sonrasıdır. Yetişkinliği Körfez Savaşı, olgunluk dönemiyse gelecek ve günümüz olarak adlandırılabilir.[363] Yapılan ayrım dışında, günümüz şartları üzerinden bunu üç bölümde incelemek mümkündür. Ayrım üç ana bölüm üzerinden yapılırsa, ilk dönemde ortaya çıkan siber tehdit ve gelişmeler Birinci ve İkinci Dünya Savaşını kapsayan; 1914-1947 tarihleri arasıdır. İkinci dönem; Soğuk Savaş Dönemini kapsayan; 1947-1991 yıllarıdır. Bu dönemi tehditlerin yükseliş dönemi olarak nitelendirmek mümkündür. Üçüncü ve son dönem; yakın dönem yani; 1991 ve günümüze kadar olan kısmı kapsamaktadır. Her an yaşanan gelişmeler sebebiyle son bölümü belirli bir tarihle sonlandırmak mümkün değildir. Ayrımı üç ayrı başlık altında incelemek özellikle dönemler açısından önemlidir. Teknolojinin ilerlemesiyle dönemin politikaları da ona göre şekillenmektedir. Gelişmelerin daha iyi anlaşılması için; siber alanın ilk dönemi olarak kabul edilen, 1914-1947 yılları arasını incelemek gerekir.

1.3.1. Siber Alanın İlk Dönem Kullanımı (1914-1947)

Siber tehditler, teknolojinin yapısı itibariyle pek çok gelişmeyle ortaya çıkmıştır. Genel anlamda tehdidi daha ciddi boyutlarda görme ihtimali bulunan yerler; savaşlar ya da devletlerin arasında yaşanan önemli dönüm noktalarıdır. Fiziksel ya da siber anlamda dönüm noktası olabilecek olaylar siber savaşlardır. Ancak dönemde daha farklı bir biçimde, günümüz hali kadar gelişmemiş şekilde karşımıza çıkmıştır. Siber bir savaş ya da ciddi bir noktada tehditlerin görülebileceği ilk yerlerden bir tanesi; 1914 yılı sonrası, Birinci ve İkinci Dünya Savaşı Dönemleridir. İki dünya savaşı süresince yaşanan olaylar; devletler, politikalar hatta teknoloji gibi birçok konuda önemli dönüm noktaları oluşturmuştur. İlk dönemlerde; siber alandan çok teknolojik cihazlar üzerinden uygulanan, elektronik harptan bahsedilmektedir. Siber alan sadece ortam değil,

[363] Ünal, *Siber Güvenlik ve Elektronik Bileşenleri*, 9.

cihazları da kapsamaktadır. Dönem içerisinde elektronik harp olarak bahsedilen olaylar, savaşlara destek amaçlı kullanılan yardımcı sistemlerdir. O dönemde sadece elektronik yapılar üzerinden bir savaştan çok, insan gücü önemlidir.

Genel olarak; 1918-1948 yılları arasında yaşanan savaşlar manevra savaşlarıyken, karadan ateş gücü, hava ve denizden teknoloji sayesinde, savaş alanı genişlemiştir.[364] İki dünya savaşı, diploması ve çatışmanın beraber yürütüldüğü ve her biçiminin görülebildiği örneklerden olup, belirli kırılmaların yaşandığı savaşlardır.[365] İki dünya savaşı sırasında hem teknolojik gelişmeler hem diplomasi ve çatışmaların bulunduğu, aynı zamanda dönüm noktalarının yaşanmış olduğu bir dönem şeklinde bahsedilmektedir. Birinci Dünya Savaşı sırasında orduların kullanmış oldukları telsizler, bunların dinlenmesi, buradan elde edilen bilgiler sayesinde savaşlarda zafer elde edilmiştir. İkinci Dünya Savaşı sırasında; RADAR (Radio Detecting and Ranging) sayesinde istihbarat kuvvetlenmiştir. Aynı zamanda şifrelemeler kullanılarak bilgi iletişimi sağlanmış, uçaklardan çekilen fotoğraflar; planlama açısından önemli bir gelişme olmuştur.[366] Dönem içerisindeki gelişmeler günümüzdeki bazı sistemlerin temelini oluşturmuştur.

Birinci Dünya Savaşı Döneminde genel yöntem; telsiz haberleşmesinde kullanılan yayın merkezinin tespiti, önlenmesi, faaliyetlerinin sonlandırılması, hatta aldatma biçiminde gerçekleşmiştir.[367] Birinci Dünya Savaşı Döneminde yapılan telsiz dinlemeleri, sinyal istihbaratı olarak nitelendirilmiştir. Telsiz dinlemelerinin bir savaşın sonucunu belirleyecek şekilde ilk kullanımı; 24 Ağustos 1914 yılında, Alman ordusunun Rus ordu grupları arasında Prusya'yı işgal emirlerini verdiklerini bu yöntemle öğrenip, önlemesidir.[368] Telsiz dinlemelerinin kullanımı, günümüzde haberleşme sistemleri üzerinden alınan istihbaratın temeli olup, tek farklılık amaç olmaktadır. Bu kullanımla, pek çok yöntemin gelişmesinde önemli bir adım atılmıştır. Telsiz üzerinden başlayan çalışmalar için belirli örnekler olduğu bilinmektedir. En bilinen örneklerden bir tanesi; Avusturya-Macaristan İmparatorluğu'nun İtalya'nın politika olarak Bosna-Hersek sorununda izleyecekleri yöntemi, İtalya'nın telsizlerini dinlemek suretiyle öğrenip, ilk haberleşme istihbaratını gerçekleştirmiş olmasıdır. Tanenberg

[364] Bayraktar, *Siber Savaş ve Ulusal Güvenlik Stratejisi*, 128.
[365] Dedeoğlu, *Uluslararası Güvenlik ve Strateji*, 122.
[366] KURGAN, *Siber Mücadeleye Giriş* (İstanbul: Kutlu Yayınevi, Ocak 2018), 86-87.
[367] Ünal, *Siber Güvenlik ve Elektronik Bileşenleri*, 9.
[368] KURGAN, *Siber Mücadeleye Giriş*, 200.

Zaferinin kazanılmasıysa; Almanların, Rus haberleşme sistemlerini dinlemesi yöntemiyle, verileri üst makamlara aktarmak şeklinde istihbarat yöntemiyle sağlanmıştır. Birinci Dünya Savaşının sonlarında, ABD, aldatma yöntemiyle sahte bir haberleşme sistemi kurarak Almanları aldatmıştır. Bu sayede Meuse-Argonne zaferini elde etmiştir.[369]

Genel olarak; Birinci Dünya Savaşında en önemli kullanımı olan, siber sistem adı altında telsiz haberleşmeleri olmuştur. Ancak, genelde istihbarat sistemi gibi kullanıldığından; dönemde bu sistemler istihbaratın alt kolu gibi kullanılmıştır.[370] Birinci Dünya Savaşı'nın seyri sırasında belirli örnekler ve devletler, siber alanda yeni girişimlere başlamıştır. Bunlara dönemde henüz siber adı verilmezken, elektronik bir yapı olarak destek amaçlı bahsedilmektedir. Gelişmelerle, günümüz sistemlerine temel oluşturmuştur. En yakın dönem olan 1930'lu yıllarda, farklı biçimlerde yeni sistemlerin kullanımına olanak sağlamıştır. Bu yıllarda siber artık bir alan olarak kullanılmaya başlamıştır. Birinci Dünya Savaşı sonrası 1930'lu yıllarda, Franklin Delano Roosevelt'in radyoyu kullanması, politik anlamda ABD'de büyük değişikliklere yol açmıştır.[371]

1939 yılında başlayan İkinci Dünya Savaşı'ndaysa; ilkine göre savunmada ileri fakat tehdit olarak kitlesel olmuş, tarafların daha farklı stratejiler izlediğinden söz edilmiştir.[372] Savunma, tehdit ve strateji açısından, ilk savaşa göre farklı bir yapıda olan İkinci Dünya Savaşı'nda; teknoloji bakımından ileri bir dönem olmuştur. İkinci Dünya Savaşı döneminde; teknolojinin gelişmesiyle ilerlemeler savunma sanayinde yaşanmıştır. 1935 yılında yaşanan başka bir gelişme; RADAR (Radio Detection and Ranging) sistemi kullanılmaya başlanmasıdır.[373] Ancak sadece radar sistemi değil, döneme göre başka yeni yapılar ortaya çıkmaya başlamıştır. Savaş dönemi boyunca gelişmeler devam etmiştir. Bu sayede dinleme/kestirme cihazları, elektronik karıştırma anlamında ilk kullanımın görülmesi, gelişimi, uçak trafiğinde sistemin aldatılması, kapsamlı şekilde ilk defa radar ikaz alıcısının kullanılması, chaff[374] kullanımı yenilikleri ortaya çıkmıştır.

[369] Ünal, *Siber Güvenlik ve Elektronik Bileşenleri*, 9.
[370] Ünal, *Siber Güvenlik ve Elektronik Bileşenleri*, 9.
[371] Nye ve Welch, *Küresel Çatışmayı ve İşbirliğini Anlamak*, 385.
[372] Dedeoğlu, *Uluslararası Güvenlik ve Strateji,* 197.
[373] Ünal, *Siber Güvenlik ve Elektronik Bileşenleri*, 10.
[374] Chaff; uçağın askeri hava uçaklarından, olumsuz hava savunma sistemleri tarafından tespit edilmesi ve saldırısını önlemek amaçlı kullanılan savunma mekanizmasıdır. Ayrıntılı Bilgi için Bkz.:

Artık bu sistemler harekât planlarına dâhil edilmeye başlanmıştır.[375] Harekât planlarının çeşitlenmesi savunma, hatta istihbarat sistemlerinde yenilikler ortaya çıkartmıştır. Savaşta istihbarat amaçlı kullanılan sinyal ve görüntülerin önemi geri plandayken, fark edilmesiyle teknolojik anlamda çalışmalar bunun üzerine olmuştur.[376] Savaşın sonunda, dönemin en önemli teknolojik gelişmelerden bir tanesi yaşanmıştır. Nükleer silah kullanılarak, Japonya'daki Hiroşima ve Nagazaki'ye 1945 yılı Ağustos ayında atılmış olan atom bombasıyla büyük ölçekli ölümler ve yıkımlar oluşmuştur. Japonya'nın teslim olmasıyla sona ermiştir.[377] Japonya'da yaşanan bu olayla, teknolojinin istenildiğinde ne kadar tehlikeli boyutlara çıktığı görülmüş, bunun üzerine ayrıca çalışmalara başlanmıştır.

Elektronik olarak, her iki Dünya Savaşında yaşanan gelişmeler, savaş alanında da sürmüştür. Günümüzdeki gelişmelerle, bu dönemdeki elektronik ilerlemeler, başka olayların gerisinde kalmıştır. Ancak belirli alanlardaki zaferlerin alınmasında ayrı bir yeri vardır. Elektronik gelişmelerin tırmandığı döneminse Soğuk Savaş Dönemi olduğunu söylemek mümkündür. Soğuk Savaş Döneminde yaşanan pek çok gelişme; önceki dönemde oluşan değişim ve gelişmenin kullanımıyla, teknoloji beraberinde hızla ilerlemiştir. Bu ilerlemelerin anlaşılması için; siber alanın Soğuk Savaş Dönemi'ndeki yeri üzerinden gidilerek, önemli olaylardan bahsetmek gerekir.

1.3.2. Soğuk Savaş Dönemi Siber Alan (1947-1991)

Birinci ve İkinci Dünya Savaşları sonrası, ikinci önemli dönem; Soğuk Savaş Dönemidir. Soğuk Savaş dönemi; 1947-1989 yılları arasında yaşanmıştır. 1947-1963 arası çok sert bir dönem olmuş, 70'ler ve 80'lerde özellikle 1985 yılında Gorbaçov'un iktidara gelmesi sonrası Soğuk Savaş'ın sonu gelmiştir. 1989'da Sovyet hegemonyası çökerken, 1991 yılında SSCB parçalanmıştır.[378] Genel olarak; Soğuk Savaş Döneminde, askeri güç, milli güç olarak algılanmış, bunları güçlendirmek amaçlı faaliyetler gösterilmiştir.[379] Ancak Soğuk Savaş

Ulusal Güvenlik Sistemi, *Chaff - Radar Countermeasures,* E.T.: 17 Haziran 2019, url: https://www.globalsecurity.org/military/systems/aircraft/systems/chaff.htm.

[375] Ünal, *Siber Güvenlik ve Elektronik Bileşenleri*, 10-15.

[376] Yılmaz ve Salcan *Siber Uzay'da Güvenlik ve Türkiye*, 25.

[377] TÜBİTAK, *Elinizin Altındaki Gerçekler: Buluşlar ve Teknoloji, Savunma ve Güvenlik,* 30.

[378] Nye ve Welch, *Küresel Çatışmayı ve İşbirliğini Anlamak*, 190.

[379] Bayraktar, *Siber Savaş ve Ulusal Güvenlik Stratejisi*, 58.

hiçbir zaman askeri bir olay olmamıştır. Daha çok politikacılar ve diplomatlar tarafından müzakere edilen politik ve ideolojik bir yüzleşme şeklinde geçmiştir.[380] Bu dönemde önemli noktalardan biri; bir dünya savaşı çıkması için ortamın hazır olmasıdır. Herkes kendini bir savaşa hazırlamıştır. Ancak sonuçlarının, İkinci Dünya Savaşının sonundan daha tehlikeli olacağı bilindiği için bir savaş patlak vermemiştir. Sadece ciddi derecede gerginlikler üzerinden geçtiği için Soğuk Savaş Dönemi olarak adlandırılmıştır.

Soğuk Savaş Döneminde önemli başka bir noktaysa; teknolojik açıdan gelişmeler üzerindendir. Elektronik olarak; 1945'te İkinci Dünya Savaşı'nın bitişi yepyeni bir dönemin başladığının işareti olmuştur. Neredeyse tüm müttefikler; elektronik savaş, personel ve ekipmanlarının kullanımını bırakırken, SSCB tam tersine bütün kuvvetlerini aktif tutmuştur. Soğuk Savaş'ın başlaması ve sonrasında gelişen Varşova Paktıyla, karşılıklı elektronik dinleme ve karıştırma faaliyetleri, başta SSCB olmak üzere başlamış, 1959 yılına kadar devam etmiştir.[381] Soğuk Savaş Dönemi içerisinde pek çok aktör, teknolojik bir tehdit olmadığı düşüncesiyle bu araçları kullanmayı bırakmış, SSCB tam zıt bir biçimde çalışmalar yürütmüştür.

1950-1953 yılları arasında yaşanan Kore Savaşı sonrasında, elektronik silahların önemi anlaşılmıştır. Faaliyetler bu yönde ilerlemiştir. İlk erken ikaz uçakları geliştirilmiştir. SSCB pek çok gelişme sağlamış, özellikle radar faaliyetleri hakkında bilgi eksikliklerini tamamlama girişimlerinde bulunmuştur. Bu dönemde aktörler, kendilerinde eksik olan teknolojileri tamamlama yönünde çalışmalar yapmıştır. SSCB 1949 yılı sonrasında ELNIT'e başlamış, bunun için alıcı, kaydedici, yön bulucu sistemler geliştirmiştir.[382] Dönem içerisinde diğer devletler de farklı gelişmeler yaşamıştır.

Vietnam Savaşı dönemi olan 1955-1975 yıllarında; hava destekli harekâtlarda füze ve radar sistemleri sayesinde Amerikan uçak kayıpları fazla olmuştur. Vietnamlılarda bulunan radar sistemlerinin Amerikalılarda olmaması, öncelik olarak uçaklara radar ikaz cihazları yerleştirmeleri ve füzelerin eklenmesiyle ilerlemeler yaşanmasına sebep olmuştur. Savaşın sonlarına doğru Vietnamlılar savaşı kazanacak görünürken, Amerikalıların şiddetli karıştırma

[380] Smith, *Utility of Force, 250*.
[381] Ünal, *Siber Güvenlik ve Elektronik Bileşenleri*, 16.
[382] Ünal, *Siber Güvenlik ve Elektronik Bileşenleri*, 17-18.

yapması, sonucu değişmiştir. İlk bilgisayar kontrolü olan radar ikaz alıcısı burada kullanımına başlamıştır.[383] Devletler bu sayede kendilerindeki teknolojik eksiklikleri görmüştür. Ancak bu dönemdeki teknolojik eksiklikler hızlı bir biçimde tamamlanmıştır.

1956 yılında; Orta Doğu'da kısa bir çatışma yaşanmış, 1967 yılında; büyük çaplı bir harekât olan Arap-İsrail savaşında, radar ve karıştırma sistemleri kullanılmıştır. İsrailliler öncelikle Mısır uçaklarını daha kalkmadan imha etmiş, aynı uygulamaları Suriye ve Ürdün'de uygulayarak "Altı Gün Savaşları"nda beklenenin üzerinde bir başarı kazanmıştır. Ancak 1967 yılında, gemilerde hava ikaz cihazlarına önem vermediği için, İsrail'in kuvvetlerine yapılan saldırı sonucu savaş farklı boyutlara taşınmıştır.[384] İki bloğun teknolojik savaşı gibi görülebilen bu savaş, Mısır ve İsrail arasında radarların ele geçirilmesi ve karıştırma cihazlarını geliştirilmesiyle ilerlemiştir. Ayrıca teknoloji ve taktiklerde gelişmeler yaşanmış, her çatışmada bunlardan faydalanılmıştır. Mısır'ın SSCB'den almış olduğu radarlar sayesinde "Yom Kippur"'da seyir değişerek, İsrail'in radar ikaz cihazlarının, bu radarı saptayamaması ve elektronik aldatma görülmüştür. İsrail, chaff sistemine geçerek zamanla gücünü kazanmış, savaşta başarı sağlamıştır. [385] Savaş sonrasında teknolojik gelişmelerle, savaşlar adına yeni düşünceler ortaya çıkmıştır. Orta Doğu'da yaşanan gelişmelerden bazılarında teknolojinin etkisi olduğu bilinmektedir. Pek çok olay tarih açısından bilinmekle beraber, kullanılan yöntemler olaylar kadar ön plana çıkmamıştır. Kullanılan yöntemler hem dönem hem siber alan açısından ayrı bir yere sahiptir.

1957 yılı, 4 Ekim'de, SSCB ilk yapay uyduyu göndermiştir. 3 Kasım'daysa Sputnik II'yi göndermiştir. ABD'de bu gelişmelerle teknolojisini ilerletmeye daha çok eğilmiştir.[386] 1958 yılı Şubat ayında ABD, ARPA (Advanced Research Projects Agency)'yı kurarak SSCB'nin teknolojisinin önüne geçmeyi amaçlamıştır. 1962'de; 1958 yılında kurulmuş olan, NASA'nın kritik araştırmaları için ihtiyaçlarını gidermek amaçlı ARPANET (Advanced Research Projects Agency Network) kurularak internetin altyapısı oluşturulmuştur.[387] Kısa süre içerisinde gelişmeler, siber ortamın günümüz biçimini almasında etkili

[383] Ünal, *Siber Güvenlik ve Elektronik Bileşenleri*, 18-19.
[384] Ünal, *Siber Güvenlik ve Elektronik Bileşenleri*, 20.
[385] Ünal, *Siber Güvenlik ve Elektronik Bileşenleri*, 21.
[386] Lerner ve Wilmoth Lerner, *Encyclopedia of Espionage, Intelligence, and Security,*89.
[387] Bıçakçı, *21. Yüzyılda Siber Güvenlik*, 5- 6.

olmuştur. 1982 yılında; İsrail'in Güney Lübnan'a yaptığı saldırıda elektronik anlamda koordineli biçimde bilgi toplanıp, değerlendirilip, hedeflere geri saldırılmıştır. Bu yapıların hepsinin bir arada kullanılması açısındansa ilk savaş olduğu bilinmektedir.[388] Stratejik açıdan, özellikle teknolojik alanın her şeklinin, kapsamlı bir biçimde kullanımı, savaş ortamı içerisinde sağlanabilecek konuma gelmiştir.

Birinci Körfez Savaşı; bilginin üretilip paylaşıldığı, aynı zamanda medya ve teknolojide ilerlemelerin görüldüğü bir savaş olmuştur. Savaş süresince, teknoloji sayesinde anlık iletimin sağlanması daha görünür bir hal almıştır.[389] Birinci Körfez Savaşı; elektronik kullanımın en yoğun olduğu, insan kaybınınsa bu sebepten daha az olduğu bir savaştır. Elektronik olarak, komuta kontrol ve haberleşmede önlemler almış, yoğun bir şekilde kullanılmıştır. İlk başta Irak'ın elektronik anlamda savaş düzeneğini öğrenme amaçlı hareketler yapılmış, sonrasında bu bilgilerle önlemler alınarak, karşı harekete geçilmiştir. Savaş, bu şekilde, yoğun elektronik sistemlerin kullanımı üzerinden ilerlemiştir.[390]

Soğuk Savaş Dönemi, elektronik ilerlemelerin en üst seviyeye çıkıp, tehditlerin büyük tehlikelere ulaştığı bir dönemdir. Soğuk Savaş Döneminin en önemli özelliği; tehditler tırmanırken, elektronik alanın daha çok ön plana çıkmaya başlamasıdır. Hızlı bir şekilde yaşanan gelişmelerle aktörler, teknolojik olarak aynı hızda kendilerini tamamlama çalışmalarına başlamıştır. Bu da bir silahlanma savaşına dönüşmüştür. Aktörler, sonuçları çok tehlikeli olacak teknolojiler üretmiştir. Ancak hiç biri bunu kullanmamıştır. Soğuk Savaş Döneminde yaşanan olaylar, bazı aktörler için dönüm noktası olmuştur. Günümüzdeki pek çok teknolojik sistem ve ortamınsa temelleri atılmıştır. Ayrıca yaşanan olaylar, devletlerin ilişkilerinde önemli rol oynamıştır. Günümüzdeki pek çok olay, yapı ya da sistemin temelleri ya da en azından şekillenmesi Soğuk Savaş Döneminde gelişmiştir. Günümüz olaylarının daha iyi anlaşılması, her iki dönemin yansımalarını görmek açısından, siber alanın yakın dönemde kullanımı ve günümüze en yakın biçimde gelişmiş halinden söz etmek gerekir.

[388] Ünal, *Siber Güvenlik ve Elektronik Bileşenleri*, 21.
[389] Jeanne Colleran, *Theatre and War* (New York: Palgrave Macmillan, 2012), 84.
[390] Ünal, *Siber Güvenlik ve Elektronik Bileşenleri*, 25.

1.3.3. Yakın Dönemde Siber Alanın Kullanımı (1991-Günümüz)

1917 yılında telgrafın Bolşevik Devriminde, 1979 yılında teyp kayıtlarının İran Devriminde, 1989 yılında faks makinelerinin devrimde oynadığı rolün yerini, günümüzde internet ve sosyal medya almıştır.[391] Bilginin bir devrim niteliğinde, ancak tehditlere açık olduğu, Birinci Dünya Savaşından itibaren dikkat çekici olmuştur. Bilginin elde edilmesi için kullanılacak yöntem ve teknoloji ayrı bir öneme sahiptir. Özellikle günümüzde, bilginin her an kolay ulaşılması, hızlı bir biçimde akışı, birçok alan için avantaj ve dezavantaj oluşturmaktadır. Bunu sağlayan en önemli yapı, teknolojiyle beraber günümüz şekliyle siber alan üzerinden olmaktadır.

Soğuk Savaşın sona ermesi, bilinen tehdit olgularının yeniden tanımlanmasına sebep olmuştur.[392] Soğuk Savaş sonrasında tanımlanan yeni tehditler, geleneksel yöntemlerin yetersiz kalmasına sebep olmuş, bu da devletleri etkilemiştir.[393] Bununla beraber devletler kendilerini yeni tehditlere hazırlama, geri kaldıkları teknolojileri görüp, tamamlama girişimlerinde bulunmuşlardır.

Soğuk Savaş Dönemi ve sonrasında öne çıkan alanlardan bir tanesi siber alandır. Soğuk Savaş sonrasında siber uzay, geniş kullanıcı kitlesi, paylaşım açısından yoğun bir alana dönüşmüştür. Devletlerin güvenlik amaçlı haberleşmeleri, kamusal hizmetler gibi pek çok bilgi bu alan üzerinden iletilmeye başlanmıştır. Siber alan hızlı bir biçimde, kamusal ve özel kullanımda kendini göstermeye başlamıştır. Daha önemlisi; devletin bilgisayar sistemine geçmesiyle; gaz, elektrik, su gibi dağıtımlar yapılan hizmetler, havayolları, deniz ve karayollarının kontrolünün sağlandığı sistemler bilgisayar ortamına taşınmıştır. Önemli altyapıların siber alana taşınması, siber tehditlere açık bir konuma gelmesine sebep olmuştur.[394] Siber alan her yapının içerisine girmiş, korunması gereken bir konuma gelmiştir.

Yeni teknolojilerle birlikte internet kullanımı, siber alan üzerinden yaygınlaşmıştır. İnternet, iletişim dışında, korunması gereken önemli bir alan olmuştur. Rus-Çeçen çatışmaları sonrasında, internetin alternatif tehditler sunduğunu gören uluslararası sistemdeki bazı devletler, bir saldırı ihtimaline karşı

[391] KURGAN, *Siber Mücadeleye Giriş*, 201.
[392] Dedeoğlu, *Uluslararası Güvenlik ve Strateji*, 55.
[393] Myriam Dunn Cavelty, *Cyber Security and Threat Politics: US Efforts to Secure the Information Age* (Amerika: Routledge, 2008), 66.
[394] Bıçakçı, *21. Yüzyılda Siber Güvenlik*, 29.

hazırlıklara başlamıştır.[395] 1994 yılında meydana gelen bu olay; bilgi ve propagandanın savaş alanında, internet üzerinden ilk kullanıldığı örneklerdendir. Askeri anlamda, Soğuk Savaş'tan sonra yaşanan çatışmanın internet ortamına taşınmasında bir ilk olmuştur.[396] Soğuk Savaş bitmiş görünse bile, aslında, yapı değiştirerek farklı bir ortamda ve farklı biçimde kendini gösterdiğini söylemek mümkündür.

1999 yılında, siber alan kullanılarak farklı olaylar ortaya çıkmıştır. 1999'da NATO, Yugoslavya'daki Sırp hedefleri bombalamaya başlamış, devamında siber saldırılar yaşanmıştır. Rus ve Sırp hackerlar, NATO ve üye devletlerin askeri haberleşme sistemlerine saldırılarda bulunmuş, en çok DDoS saldırıları ve virüs içerikli e-postalardan yararlanmıştır.[397] Kosova Savaşı olarak geçen olay; çatışmayla internet kullanımının, internet üzerinden ilk savaş olma niteliğini kazanmasını sağlamıştır.[398] İnternetin bir savaş yöntemi olarak kullanılması, bu tarihten itibaren daha net görülmüştür.

Yaşanan bu olaylar, güvenlik üzerine çalışmalara daha çok dikkat edilmesi gerektiğini göstermiştir. Güvenlik üzerine önemli tarihlerden bir tanesi; 11 Eylül 2001 yılındaki terör saldırıları sonrası olmuştur. Uluslararası sistemin güvenlik tanımları, gündemleri, tehdit algıları değişmiştir. Bazı yorumlar; bu olayı siber savaşla bağdaştırmış, çünkü saldırı yapıldığı zaman saldırganlar iletişimini internet üzerinden gerçekleştirmiştir.[399] Bu da internetin terör saldırı için önemli bir konumda olabileceği düşüncesini güçlendirmiştir. Siber alanın dezavantajlarından bir tanesi olan; terör amaçları için kullanımın, tehlikeli boyutlara gelebildiğini gösteren önemli olaylardan olmuştur. Yaşanan bu olay, güvenlik üzerine yeni tanımlamalar yapılabilecek derecede bir dönüm noktası oluşturmuştur. Teknoloji ve belirli yapıların gelişip değişmesiyle, her an, yeni güvenlik durumları ve tehlikeler artarak ortaya çıkmaktadır.

Günümüze yakın önemli olaylardan bazıları; 2000'li yıllardan itibaren, günümüz siber alanı kullanılarak olmuştur. 2007 yılında; e-devlet sistemi öncülerinden olan, Estonya, Rusya tarafından, bu sistem üzerinden siber

[395] Bıçakçı, *21. Yüzyılda Siber Güvenlik*, 30.
[396] KURGAN, *Siber Mücadeleye Giriş*, 172.
[397] Bıçakçı, *21. Yüzyılda Siber Güvenlik*, 31.
[398] Cavelty, *Cyber Security and Threat Politics: US Efforts to Secure the Information Age*, 74.
[399] Bıçakçı, *21. Yüzyılda Siber Güvenlik*, 32.

saldırılara uğramıştır.[400] DDoS saldırılarıyla ortaya çıkan bu savaş, sistematik anlamda ilk gerçek siber savaş olmuştur. Aynı zamanda, bu saldırılar sonucu pek çok Estonya vatandaşı sorun yaşamış, yapılan saldırıların o zamana kadar görülmüş en büyük DDoS saldırısı olmasıysa ayrı bir özelliği olmuştur.[401] Siber alan içerisinde artık bir siber savaştan söz edilmeye başlanmıştır. Ancak bu söz edilen siber savaş, bir savaş yöntemi biçimindedir. Teknoloji ilerledikçe, alanda yeni yöntemler ortaya çıkmıştır. Ancak teknolojinin ilerlemesi, yeni saldırı ve tehdit çeşitlerinin hızlı bir biçimde yayılmasına sebep olmuştur. Kısa süreler içerisinde pek çok saldırı gerçekleşmesine açık hâle gelmiştir. Çeşitli saldırılar içerisinde, 2010 yılında fark edilen Stuxnet virüsü, siber alan için önemli bir yere sahiptir. Virüs; İsrail ve ABD'nin, İran'ın nükleer çalışmalarını öğrenmesi sonrasında, engel olmak amaçlı sisteme bulaştırdığı iddia edilen kötü amaçlı yazılımdır.[402] Yaşanan bu olay; siber alan açısından en büyük tehlikelerden bir tanesinden geri dönüldüğünü göstermektedir. Ancak siber alandaki tehditler her sene gittikçe artmıştır. 2016 yılı, ABD başkanlık seçimlerinde; ABD'nin sistemlerine Rusya Federasyonu tarafından siber müdahale olduğu düşüncesi, Soğuk Savaş'tan günümüze, siber boyutlarda savaşı gözler önüne sermektedir.[403] Ayrıca siber alanın, politik olaylarda kullanımını açık biçimde göstermektedir.

2017 yılındaysa "WannaCry" isimli bir fidye yazılımıyla tüm dünyada etki gösterecek derecede bir saldırı yapılmıştır. Saldırı 150 ülkede etki göstermiştir. Saldırı; sistem dosyalarına erişimi şifreyle engelleyip, erişilmesi için para istemektedir. Ödenmediği takdirde dosyaları silmektedir. Saldırı yapıldığı süreçte, İngiltere'de Ulusal Sağlık Hizmetlerinin birçok kurumu, Reanult Bursa fabrikası, Rusya Demiryolları, Çin Halk Güvenliği Bürosu ve Rusya İçişleri Bakanlığı gibi pek çok önemli kurum da etkilenmiştir.[404] Birçok alana sıçrayan saldırı gibi, günümüzde çeşitli saldırılar yeni yapılarda devam etmektedir. Günümüzde en çok kimlik hırsızlığı, sosyal medya saldırıları ve bankacılık alanında saldırılar devam etmektedir. Devletlerarasındaysa, politik anlamda tehditler yükselmektedir.

[400] KURGAN, *Siber Mücadeleye Giriş*, 90.
[401] Thomas A. Johnson, "Cyber Intelligence, Cyber Conflicts, and Cyber Warfare,"içinde *Cyber Security,* ed. Thomas A. Johnson (ABD: CRC Press, 2015), 177.
[402] Richard Stiennon, "A Short History of Cyber Warfare," içinde *Cyber Warfare*, ed. James A. Green (Amerika: Routledge, 2015), 20.
[403] KURGAN, *Siber Mücadeleye Giriş*, 56.
[404] "WannaCry Saldırısının Ardında Yatan Gerçekler," *CNN Türk*, 16.05.2017, E.T.: 10 Ağustos 2019, url: https://www.cnnturk.com/teknoloji/wannacry-saldirisinin-ardinda-yatan-gercekler.

Sadece ilerlemeler tehdit ya da saldırı üzerine değildir. Yeni sistem ve altyapı çalışmaları yapıldığı bilinmektedir. Ancak, günümüzde henüz duyurulmamış pek çok proje vardır.

Genel olarak; klasik savaş dönemi şeklinde adlandırılan Birinci Dünya Savaşı'ndan günümüze kadar, tehditler ve gelişmelerde, uluslararası alanda yeni bir boyuta geçilmiştir. İlk dönemlerde siber alan saldırılara destek amaçlı kullanılmıştır. 1991 yılı sonrasındaysa siber alan önem kazanmaya başlamıştır. Günümüzde siber alan, artık bir güvenlik yapısı olarak da söz edilmektedir. Geçmiş dönemlerde yaşanan olaylar ve gelişmeler; günümüz ve gelecek için önemlidir. Devletlerin ve uluslararası kuruluşların siber güvenlik amacıyla belirledikleri politikaların oluşumunda tarihsel altyapının etkileri de vardır. Tarihsel altyapının incelenmesi hem siber alan ve güvenliği açısından önem taşırken hem de izlenecek politikalar için bir yol gösterici olmuştur.

1.4. BÖLÜM DEĞERLENDİRMESİ

Uluslararası sistemde, hatta insan hayatının her alanında en önemli konulardan bir tanesi güvenliktir. Birçok alanda; kişi, toplum hatta sisteme göre değişiklik göstermektedir. Önemli olan; güvenlik ihtiyacı duyan aktörün kendini güvende hissetmesidir. Güvenlikte aktöre göre değişen kısım; bir aktörün güvende olmasının, karşıt bir aktörde güvensizlik hissine sebep olmasıdır. Bu aynı şekilde bireysel, toplumsal hatta uluslararası alanda da geçerlidir. Günümüzde, uluslararası sistemde bazı alanlarda sınırlar azalmaya başlamıştır. Bunda etkili olan bazı sebepler; gelişen teknoloji, yapılan politikaların yetersizliği, ortaya çıkan yeni sistem ve politikalar, insan hayatında yaşanan değişimlerdir. Teknolojinin etkisiyle, pek çok alanda etkili yeni sistem ve alanlar ortaya çıkmıştır. Ortaya çıkan yeni alanlarla beraber, yeni güvenlik tanımlamaları yapılmasına ihtiyaç duyulmuştur. Günümüzde, özellikle güvenlik gibi pek çok alanda etkisini göstermeye başlayan alanlardan biri; siber alandır. Siber alan, hayatımızın her noktasında kendini göstermektedir. Bu sebeple; güvenlik konusunda yepyeni bir alan açılmıştır.

Siber alan genel anlamda; tüm cihaz ve cihazların bağlı olduğu ortamı kapsamaktadır. Kullanım alanı belirli sınırlar içerisinde değildir. Hayatımızın her yerindedir. Uluslararası sistemdeyse çeşitli şekillerde kullanılmaktadır. Kendisini

geliştirmeye devam eden bu alan, kendi güvenlik alanını oluşturmayı başarmış, ancak ayrı bir öneme ihtiyaç duymuştur.

Siber alanın önemini gösteren noktalardan biri; iletişimde önemli bir yeri olmasıdır. İletişimi sağlamak için günümüzde en çok internet üzerinden sistemler kullanılmaktadır. İnternetse tamamen ucu açık, siber alanın kendi özelliğinden dolayı bir sınırı olmayan, sonu bilinmeyen bir yapıdır. Her alanın avantajları dışında dezavantajları vardır. İnternetin en büyük avantajı; sınırlar olmadan, dünyanın bir ucundan öbürüne, günümüz şartlarında anlık iletişim kurulabilmesidir. Dezavantajıysa; ciddi derecede sonuçlar verebilecek kadar önemli tehditlere açık olmasıdır.

Siber alandaki tehditlerse çeşitlidir. Ancak tehditleri ortaya çıkarabilen belirli kullanıcılar da mevcuttur. İnternet kullanıcıları arasında özel bir yere sahip olan, hackerlar vardır. Hackerlar genel olarak üç çeşittir. Genel anlamda; bilgisayar sistemlerinin ve siber alanın, özellikle internetin her alanını bilerek, belirli amaçlarla, normal kullanıcılardan daha üst seviyede kullanım sağlayan kişilerdir. Amaçları kişiden kişiye değişmektedir. Biri için doğru olan diğeri için tehdit olabilir. Bir hacker grubu sadece bireysel seviyede değil, kendi istekleri üzerinden devletler seviyesinde olaylara yol açabilir. Yine yaşanan bir olayın algılaması üzerinden, tehdit düşüncesi ve buna karşılık savunmayla güvenlik oluşturulur.

Güvenlik ve savunma tehditler üzerinden oluşturulur. Tehditlerden siber alanda iki şekilde söz edilebilir. Bilgisayar ortamı üzerinden ve stratejik biçimde gerçekleşmektedir. Bilgisayar ortamında oluşan tehditler; virüsler gibi olup, sistem üzerinden, büyük ya da küçük sonuçlara yol açmaktadır. Bu tehditler kullanım biçimine göre kişisel ya da uluslararası boyuta çıkabilmektedir. Bir tehdidin stratejik kullanımıysa; yapılan stratejiye göre tehlikeyi arttırmaktadır. Bir virüsün bilgisayara kendiliğinden bulaşmasıyla başkası tarafından, belirli amaçlar için kastî bulaştırması arasında büyük fark vardır. Tehditleri ikiye ayırmak mümkün olsa da, önemli olan kullanım yeri ve şeklidir. Bilgisayar ortamındaki tehditleri, farklı amaçlarla kullanarak stratejik tehditler içerisinde görmek mümkündür. Ancak her iki tehdit biçimi birbirinden farklıdır. Bu tehditlerin daha büyük çaplı olanlarını uluslararası sistemde görmek daha büyük sorunlara yol açmaktadır.

Günümüzde uluslararası sistemde, belirli siyasi amaçlar üzerinden uygulanan stratejik siber tehditler vardır. Uluslararası alanda, belirli amaçlara hizmet ederek kullanım, farklı biçimde adlandırılmasına sebep olmuştur. Stratejik olarak en büyük tehditlerse; siber terör ve siber savaştır. Ancak ikisi karıştırılmamalıdır. İkisi de siyasi eylem içerikli davranışlar barındırır. Ancak aktörler ve yapılan eylemler üzerinden pek çok farklılık vardır. En önemli ayrım; siber terörde, insanlarda endişe ve korku oluşturmasıdır. Siber savaştaysa; devletlerarasında, belirli kurallar içerisinde meydana gelmesidir. Savaşta; en az sivilin hasar görmesine dikkat edilmektedir. Ayrıca siber anlamda özellikle devlet ya da hükümetler hedeftir. Terördeyse ayrım bulunmamaktadır. Terör için siber alanın kullanımı; sistem üzerinden, ihtiyaç duyulanlara kolay erişim, yapılan eylemlerde yerin tespitinin zorluğu gibi avantajları bulunmaktadır. Siber savaş; günümüzde devletler gibi aktörlerin, sistemler üzerinden savaşmasını içerir. Siber savaş tek başına can kaybı oluşturmamakta, bir savaş içerisinde yöntem olarak da kullanılmaktadır. Tek başına kullanımında daha çok devletlerin altyapılarına zarar vermek, bilgi toplamak amaçlıdır. Fiziksel savaşa yardım amaçlı kullanıldığındaysa daha çok bir savaş stratejisi konumundadır.

Siber alanın bir savaş biçiminde kullanılması; özellikle uluslararası alanda tehdit, hatta eylemler ve aktörlere göre daha büyük tehlikelere yol açabilmektedir. Siber savaş henüz ciddi boyutlarda can kaybına yol açmamış, ancak tehditler o boyutta yükselmiştir. Bu gibi olaylar, ne kadar ileriye gidilebileceğini de göstermiştir. Günümüzde önemli bir nokta; yaşananların sebebinin bilgiyi elde etme ihtiyacı olmasıdır. Bilgi, kendini yenilemekte, elde edenin amacına ulaşma ve başarılı olmasını sağlamaktadır. Ancak bilgi, yanında tamamlayıcı yapılara ihtiyaç duymaktadır. Bir bilgiyi işlemek için belirli bir teknoloji ya da ekonomi gerekir. Ayrıca bilginin kullanılacağı alanın ne olacağına karar verecek bir strateji, uygulama amaçlarının belirlenmesi için politikalar gibi tamamlayıcılar olmalıdır. Sadece bilgi edinmek tek başına, zayıf kalacaktır. Bu sebeple pek çok koşulu sağlayan aktörler, karşı tarafın özel bilgileri, hatta ekonomi, politika ve stratejilerini öğrenme amaçlı çalışmalar yapmaktadır. Çalışmalar; siber alan üzerinden istihbarat yapılması şeklindedir. Günümüzde her tür bilgi, bilgi akışı siber alan üzerinde bulunup, kullanılmaktadır. Aktörler, belirli bilgileri ve altyapıları gibi önemli sistemlerini siber alana aktarmıştır. Bu sebeple; bir saldırı ya da istihbarat için, hepsini kapsayacak siber savunma çalışmaları yapılmıştır.

Daha çok koruma amaçlı yapılan çalışmalar dışında, bir saldırı karşısında hazırlıklı olarak, saldırıya karşı savunma çalışmaları da yürütülmektedir. Siber savunmadaki tek problem; saldırılarla paralel gitmeyip, teknolojinin hızına göre daha geç çalışmalarına başlanmış olmasıdır. Bazı aktörler çalışmalarını hızlandırarak eksiklerini gidermiş, bazı aktörlerse ekonomik koşulların etkisiyle daha geç bir süreçte tamamlamamıştır.

Siber çalışmalar; belirli bir süreçte gerçekleşmiştir. Her yapı gibi siber alan da tarihi bir süreçten geçerek, günümüz halini almıştır. Özellikle Birinci Dünya Savaşı döneminden başlayan süreçle, pek çok aşama kaydetmiştir. Ancak, başta yardımcı konumda başlamış, zamanla, tek başına bir güvenlik konusu haline gelmiştir.

Siber alan ve güvenliğinden söz edildiğinde sadece teknoloji ve mühendislik alanı içerisinde düşünülmemelidir. Teknik olarak, teknoloji açısından mühendislik alanında olması, siber alanın sadece buraya ait olduğunu göstermez. Kullanım açısından politika, uluslararası alan gibi pek çok alanda faaliyettedir. Özellikle uluslararası alanda devletlerin kendini arasındaki ilişiklerde etkilidir. Uluslararası ilişkilerde her olayın etkileri büyük çaptadır. Sadece bir devleti ilgilendiren bir konu, siber alan üzerinden, devletlerin içerisinde yaşanan anlık iletişimle, dünyanın başka bir ucunda tepki gösterilmesini sağlamaktadır. Siber alan üzerinde sınırların kalkmış olması, artık daha farklı tepkilerin, daha karmaşık yansımalarına yol açabilmektedir. Yansıma ve tepkilerse, yapılabilecek saldırı ve karşılığında gelecek savunma biçimine bağlıdır. Teknik olarak alınabilecek önlemler daha belli olmasına karşın, stratejik açılardan daha çeşitli yöntemler vardır. Özellikle; siyasi ve uluslararası sistemlerde, pek çok çeşidi karşımıza çıkan siber olaylar için, siber güvenlik üzerine çalışmalar yapılmaktadır. Ancak genel tarih içerisinde süreç daha yakın tarihli çalışmalar olduğunu göstermektedir.

Genel olarak; uluslararası sistemde siber alan, önemli bir güvenlik alanı haline gelmiştir. Siber güvenlik, kendi özellikleri ve içerisinde barındırdığı tehditler sebebiyle önemini ortaya koymuştur. Aynı zamanda gelişim süreciyle günümüzdeki konumuna gelişi, pek çok güvenlik yapısına göre hızlı bir biçimde olmuştur. Ancak güvenliği aynı hızda ilerlememiştir. Siber alanın günümüzde de güvenliğinden hızlı ilerlemesi, pek çok soruna açık olmasını getirmiştir. Siber alanın kendi içerisindeki tehditler, güvenlik geliştirmelerinden hızlıdır. Ancak günümüzde bunun için önemli adımlar atılmaktadır. Bu bölümde verilen teorik

bilgi, sonraki bölümün temelini oluşturmuştur. Bir konunun gelişimini bilmek, yaşanan ve yaşanabilecek olayların daha anlaşılır olmasını sağlar. İkinci bölümde; yaşanan olayların ve siber tehditlerin, bir siber savaş biçiminden, fiziksel bir savaşa dönüşebilme ihtimalinden söz edilecektir. Hareket noktası; bazı devlet ve örgütlerin yaşamış oldukları önemli örneklerle, sonucunda ortaya çıkan politikalardır. Politikaların etkileri ve yeterliliği, siber alanda oluşabilecek yeni tehdit ve sorunlar için önem taşımaktadır. Yeterli olan politikalar sorunları en az seviyeye indirebilirken, yetersiz politikalar büyük problemleri de beraberinde getirecektir. Bu sebeple; bu bölüm, bir siber tehdidin, daha tehlikeli boyutlara çıkıp çıkmama üzerine ihtimalinde açıklayıcı olacaktır.

İKİNCİ BÖLÜM

SİBER ORTAMDA VAR OLAN TEHDİTLER FİZİKSEL SAVAŞA DÖNÜŞEBİLİR Mİ?

Geçmişten günümüze, özellikle genel tarih açısından siber alan; teknolojik gelişme, iletişim gibi konularda önemli bir yapı olmuştur. Birinci Dünya Savaşı dönemi ve sonrasında siber alan, özellikle elektronik olarak, savaş gibi olaylarda yardımcı bir konumdadır. Günümüzdeyse siber alan, tamamen kendine ait bir ortamdır. Siber alan, kendine ait bir ortamla ortaya çıkartmış, ayrıca her alanda ayrı çalışılması gereken bir konuma gelmiştir. Yaşanan gelişmeler olumlu olmakta, ancak olumsuzlukları da beraberinde getirmektedir. Siber alanda, bazı alanlara göre daha çok tehdit bulunmaktadır.

Siber tehditler hem bilgisayar ortamında, hem stratejik olarak kullanıldığında, önemli boyutlarda tehditler oluşturmaktadır. Tehditlerin ortamın kendisinden ya da kendi yapısıyla çıkmış olması problem oluşturmaktadır. Bir tehdidin sınırları belirli olduğunda, alınabilecek önlemler o ölçüde kolay olur. Ancak alanın ne tür tehditler getireceği bilinemezken, alınabilecek önlemler, teknolojinin ilerlemesiyle zayıf kalmaktadır. Teknolojinin her geçen gün hızlı ve büyük atılımlar yapması, güvenlikte problemler oluşturmaktadır. Clausewitz'in bahsettiği üzere; bir savaşta bulunan engel büyük önem taşımaktadır.[405] Siber alanda, özellikle fiziksel bir savaşta görülecek şekilde engel mümkün değildir. Görülemeyen bir engel, kendini savunacak taraf için en büyük olumsuzluktur. Savaş anlamında klasik savaşlardan farkı; siber alanda savaşın daha farklı algılanmasıdır. Bunun sebebi savaş alanının değişmesidir. Siber alanda sadece ağ sistemi üzerinden, gözle görülemediği için önem atfedilmeyen olaylar, çok tehlikeli boyutlara çıkabilmektedir. Örneğin; Stuxnet olayı, o dönemde daha ileri gitmemiş olduğu için, fiziksel bir tehlike ortaya çıkmamıştır. Ancak hem siyasi

[405] Clausewitz, *Savaşın Esasları*, 31.

gerginliklere sebep olmuş, hem siber anlamda, istenildiğinde ne kadar ileri gidilebildiğini göstermiştir. Günümüzde siber savaşlar, ağlar ve elektronik yapılar üzerinden ilerlemektedir. Yaşanan olayların sadece bir kısmından bahsedilirken, bu alan sayesinde, daha açıklanmamış pek çok bilgiye ulaşmak daha kolaylaşmıştır.

Bilgi ve teknolojilere rahat erişim hem olumlu hem olumsuz olmuştur. Devletler seviyesinde teknolojik gelişmeler, güvenliği hissettirirken, başka devletler için tehdit niteliği taşımaktadır. Bir devlet ne kadar maddi imkâna, bilgiye sahipse, kendini var olan teknolojinin en üst seviyesine kadar çıkarmaya çalışacaktır. Bu, başka bir devletin, özellikle ekonomik anlamda zayıf bir devletin, daha fazla tehdit hissetmesine neden olur. Benzer olaylar Soğuk Savaş Dönemi'nde de görülmüştür. Başka açıdan bakıldığında siber tehdit ya da savaşlar; Dijital Soğuk Savaş olarak da düşünülebilir. Belki de Soğuk Savaş'ın bitmediği, bunun zamanla başka bir ortama taşınarak devam ettiğini söylemek de mümkündür.

Teknoloji ve her türlü bilgiye kolay ulaşmak, kötü amaçlı bir birey ya da grup için de rahat olacaktır. İnternetle terör örgütleri ya da bireysel boyutlarda siyah şapkalı hackerlar, istedikleri bilgiler ve teçhizatları kolaylıkla elde etmektedir. Terör örgütleri, uluslararası anlamda, sınırları belli olmayan bir alana rahatça ulaşıp, pek çok sisteme girebilmek için açıklıkları bulmaktadır. Ayrıca sadece internet üzerinden araştırma ve eğitimlere bağlı olması, tehlikenin ne kadar yüksek olduğunun bir göstergesidir. Hackerlar; belirli çıkarlar ya da kendilerine göre belirli doğrular üzerinden hareket ederler. Hedefleri; masumlardan çok, belirli kişi ya da politik yapılardır. Bu şekilde, büyük fiziksel zararlar olmayacak ölçüde, kendi amaçlarını gerçekleştirmektedirler. Aynı sistem üzerinden, çözüme ulaşmak ya da kendini savunmak amaçlı kullanımda mevcuttur.

Çeşitli tehditlerin bulunduğu, sınırları olmayan, teknolojik anlamda altyapıların yer aldığı bu alan, belirli devletler ve uluslararası kuruluşlar için önem teşkil etmiştir. Bu sebeple; yakın dönemde politikalarına siber alanı ilave etmiştir. Yapılan çalışmalar günümüzde devam etmektedir. Alanın gün geçtikçe kendini yeniliyor olması, her geçen gün yeni bir açıklıkla sistemlerin problem oluşturması, yapılan politikaların devre dışı kalmasına sebep olur.

Devletlerin belirledikleri politikalar, siber savaşların ya da tehditlerin, fiziksel bir savaşa dönüşmesine yakın dönemde engel olsa da, bu her zaman

geçerli değildir. Günümüzde birebir örnek yoktur. Ancak bu hiçbir zaman ortaya çıkmayacağını garantilemez. Yapılan politikaların yakın dönemde etkisinin de tam bir garantisi yoktur. Atılan adımlar önemlidir. Bazı devletler belirli politikalarla, kontrolsüz bazı sistemlerin kullanımının önüne geçmiştir. Bu, her devlet ya da kuruluş için geçerli değildir. Her devletin politikası, ekonomik kaynaklarının farklı oluşu, kendi içyapılarının farklılığı etkilidir. Yapılan politikalar ve günümüzdeki alanın oluşmasında etkisi olan olaylar önemlidir. Hiçbir olay bir anda ortaya çıkmamıştır. Belirli birikimler sonucu patlak vermiştir. Bunları açıklamak için öncelikle bazı devletlerin, sonrasında bazı önemli kuruluşların, birkaç örnekle, günümüzde belirledikleri politikalarına eğilmek gerekir. Bu sayede, günümüzde bahsedilen I. Dünya Siber Savaşı'nın birikimlerini anlamak rahat olacaktır. Buna ek olarak; siber savaşın, sonradan bir fiziksel savaşa dönüşme ihtimalinin olup olmadığını anlamaya yardımcı olacaktır.

2.1. BAZI DEVLETLERİN SİBER ORTAMDA OLUŞABİLECEK TEHDİTLER ÜZERİNE BELİRLEDİKLERİ POLİTİKALAR

Tehditler; bireysel, ulusal, uluslararası seviyesinde olmak üzere üç şekilde ortaya çıkar. Uluslararası alanda tanımlı olan; uluslararası sistem, alt sistem, devlet, toplum, toplumsal alt grup ve birey birebirine bağlıdır.[406] Kapsayıcı her yapı, diğerini etkileyecektir. Genel anlamda; bir sistemde çıkan tehdit, bireyi de etkileyebilir. Ancak bir bireyin yaptığı olumsuzluk, üst yapıyı etkileyebilecek güçteyse, uluslararası yapıya kadar ciddi derecede problem oluşturabilir. Uluslararası sistemler için örnekler çoktur. Günümüzde yaşanan bir ekonomik problem bile bireyin yapacağı alışverişi etkileyecek dereceye gelir. Uluslararası alanda birey etkisini en açık şekilde gösterebilecek örneklerden biriyse; bir terör örgütünün başındaki kişinin vermiş olduğu emirdir. Bir kişinin vereceği bir emir, tüm dünyada huzursuzluk yaratabilir.

Uluslararası alandaki tehditler, ana aktörlerden biri olan devletleri, hatta sistemi etkilemiştir. Devletler, öncelikle, kendi içyapılarına gelecek tehditlerin önüne geçmek amaçlı girişimlerde bulunur. Bir devletin kendi iç bütünlüğü ve güvenliğini sağlaması, kendi var oluşunu koruması anlamına gelmektedir. Bunun için; gelebilecek tehditlerin önüne geçmek, belirli politikalar izleyerek, içeriden ve

[406] Dedeoğlu, *Uluslararası Güvenlik ve Strateji*, 38.

dışarıdan gelebilecek tehdidin ortaya çıkmadan ya da büyük zarar vermeden engellenmesi gerekir.

Tehditler günümüzde; fiziksel ya da teknolojilerle, siber alanda ortaya çıkmaya devam etmiştir. Tehditler, fiziksel görünmese dahi, siber alanda yapılan saldırıların bazıları fiziksel savaşa dönüşebilecek kadar ciddi boyutlara ulaşmıştır. Günümüzde tek başına bir siber saldırı ya da savaşın, ciddi bir fiziksel savaşa dönüştüğü örnek yoktur. Ancak, ciddi biçimde devletlerin kendi bütünlüğüne tehditler vardır. Bu sebepten; devletler kendi yapılarına gelebilecek tehditleri, özellikle günümüzdeki gelişmeleri daha yakından takip etmelidir. Çünkü tehditlerin sonuçlarının hangi boyutlara çıkabileceği tam anlamıyla öngörülememektedir.

Günümüzde tehditlerin siber alana taşmış olması, devletlerin önemli adımlar atarak, büyük sorunlar ortaya çıkmasının önüne geçmek için politikalar belirlemesine sebep olmuştur. Bu politikalar, yakın zamanda ortaya çıkmış ya da çıkmasına rağmen hâlâ tam oturmamıştır. Bu alan için yapılan çalışmalar, bir siber tehdidin, daha ciddi bir savaşa dönüşmemesi için yapıldığı düşünülmektedir. Bir siber tehdidin ne zaman bir savaşa dönüşeceği tahmin edilememektedir. Ancak günümüzde yaşanan devletlerarasındaki gerilimler ve siber saldırılar, özellikle gergin olan uluslararası ilişkilerde farklı boyutlarda sorunlar çıkmasına sebep olabilecektir. Oluşacak tehditlerin, gergin olan ilişkilerde, savaşa dönüşebilme ihtimali vardır. Ancak, birikme sürecine bağlı olarak ortaya çıkacağı bilinmektedir.

Genel olarak; devletlerin, siber tehditlerin önüne geçmek amaçlı yaptıkları politikalar vardır. Bu politikalarla tehditler, tehditten tehlikeye, tehlikeden belki savaşa dönüşmeden önce durdurulabilmektedir. Siber alan için belirli adımlar atılmıştır. Bu adımların daha iyi anlaşılması için; bazı devletler incelenerek, belirli örnekler üzerinden politikalarını anlamlandırmak gerekir.

2.1.1. ABD (Amerika Birleşik Devletleri)

ABD, kurulduğu tarihten bugüne kadar savunma dâhil çeşitli alanlarda politikalar izlemiştir. Günümüzde ciddi bir yer tutmaya başlamış olan siber alandaki tehditler için de ayrıca politikalar belirlenmiştir. Herhangi bir politika gibi bu alan için belirlenen politikalar, yaşanan olaylarla gelişmeler göstermiştir. Her tehlike bir tehditken önlemler alınmakta, ancak tehditler tehlikeye

dönüştüğünde daha büyük önlemlere ihtiyaç duyulmaktadır. Siber alan ortaya çıktığında, üzerine bir politika üretilmesi gereken büyüklükte tehditler görülmemiştir. Günümüzde, siber anlamda yaşanan herhangi bir savaş da henüz ciddi, fiziksel bir savaşa dönüşmemiştir. Ancak bu hiçbir zaman dönüşmeyeceğini göstermemektedir. Bu sebeple, sahip oldukları ölçüde, siber alanda, tehditlerin önüne geçebilmek amaçlı politikalar üretilmiştir.

ABD, siber alanda önemli örneklerden biridir. İnternetin, aynı zamanda, siber alanın en önemli yapılarından birinin ortaya çıktığı yer ABD'dir. Bu sebeple, ABD, belirli tehditleri bazı devletlere göre daha erken görmüş, bunların önüne geçebilmek amaçlı çalışmalar yapmıştır.

Bir tehdidin kritik altyapılara zarar vermemesi önemlidir. Herhangi bir kritik altyapıya gelecek zarar, ciddi aksaklıklara yol açmaktadır. ABD, kritik altyapı tanımını ayrıca belirlemiştir. Kritik altyapılar ortadan kalkar ya da yetersiz bir konuma gelirse problemler ortaya çıkar. Özellikle; halkın emniyet ve güvenliğini, ekonomik ya da sağlık açısından, birbirine bağlı yapılardan birine zarar verildiğinde, sorun çıkabilecek sanal ya da fiziksel yapılar vardır. Ticari tesis, kimya, iletişim, barajlar, kritik üretim, savunma sanayi, finans, enerji, tarım ve gıda, yönetim (devlet) tesisleri, bilgi teknolojileri, sağlık, nükleer, su ve taşıma tesisleri kritik altyapı olarak söz edilmektedir.[407] Altyapıların önemi her dönem geçerlidir. Alınacak önemlerse özellikle siber alanda, var olan teknolojik seviyeye göre değişiklikler göstermektedir. Teknolojiler ABD'de, özellikle siber alanda, Soğuk Savaş Dönemi'nde yaşanan olaylarla beraber, belirli gelişmeler göstermiştir.

ABD, Soğuk Savaş Dönemi'nde, daha çok SSCB ile yaşananlar üzerinden gelişmeler göstermiştir. Soğuk Savaş Dönemde, SSCB ile yaşanan ağ teknolojileri üzerine, ilk nesil olarak kabul edilen teknolojilerle rekabet içerisinde olan ABD, 1960'lı yıllarda büyük atılım göstermiştir. Soğuk Savaş sonrası dönemde; internetin, ticari ve sivil alana geçmesiyle sağlanan teşviklerle ABD, bu alanda önemli yatırımlarda bulunmuştur.[408] İlk atılım olarak ABD; bilimsel alanda SSCB ile rekabet amaçlı; 1958 Şubat ayında, ARPA (Advanced Research Projects Agency- İleri Araştırmalar Projeleri Ajansı)'yı kurmuştur. 1972 yılındaysa adı

[407] "Critical Infrastructure Sectors," Homeland Security, E.T.: 15 Ağustos 2019, url: https://www.dhs.gov/cisa/critical-infrastructure-sectors.
[408] Darıcılı, *Siber Uzay ve Siber Güvenlik*, 63.

DARPA'ya dönüşmüştür.[409] Bu proje, internet tarihinin başlangıcı olarak sayılmaktadır. Çünkü ARPA'da yapılan çalışmalarla bu çalışmalarda bulunan kişilerin ortak ağda bulunması, internetin temelini teşkil etmiştir. Bu sebeple; ARPA projesi, ARPANET'in ortaya çıkmasını sağlamıştır.[410] Aynı zamanda ARPANET; askeri savunmayla alakalı konularda, araştırmacıların kaynaklarını fiziksel iletim dışında paylaşmalarını sağlayarak, daha verimli araştırmalarını sağlanmıştır.[411] Yaşanan gelişmeler internetin başlangıcı olarak kabul edilmiş, siber alanın gelişmesinde en büyük adımlardan biri olmuştur.

1962 yılı, Küba Füze Kriziyle, olası bir nükleer savaş karşısında, ARPANET'in etkilenmemesi için, farklı sistemler üzerinden çözüm önerilerinde bulunulmuştur. Küba Füze Krizi döneminde hissedilen tehdit, siber alana da yansımıştır. Belirli önlemler alınması ihtiyacı, ARPANET'in kullanım oranıyla, başka çözümlere gidilmesi gerektiğini göstermiştir. 1982 yılında ARPANET; teknoloji, kullanıcı sayısı, tehditlerle, ABD Savunma Bakanlığı askeri anlamda kullanılan verilerin iletişim ağını farklı bir altyapıdan yönlendirme kararı almıştır. ABD, Militarynet (MILNET) şeklinde farklı bir ağ kurmuş, ARPANET'in yetersiz kalmasıyla, yeni ve nitelikli ağlara yerini bırakarak, 1990 yılında kullanıma kapatılmıştır.[412] Sonrasında; günümüzdeki internet yapısı ortaya çıkmıştır.

İnternetin gelişiminde yapılan çalışmalarla, güvenlik amaçlı önlemler dışında, farklı çalışmalara başlandığı bilinmektedir. 1988 yılında ortaya çıkan bir solucan sayesinde, internete bağlı bilgisayarların bir kısmı çalışamaz hale gelmiştir. DARPA tarafından, kısa bir süre sonra, güvenlik amaçlı; Bilgisayar Olaylarına Müdahale Ekibi Kontrol Merkezi (Computer Emergency Respons Team Control Center (CERT CC)) kurulmuştur. Kuruluşun hedefiyse; Amerikalıları daha güvenli ve güçlü bir internete sahip kılmaktır. Aynı zamanda tehditleri analiz edip, güvenilir kaynaklarla siber güvenlik bilgi alışverişi yapabilmektir.[413] Kurulan kontrol merkeziyle, ABD açısından, artık siber olayların daha ciddiye alındığı görülmektedir. 1990-91 yılları içerisinde, I. Körfez

[409] Kremling ve Sharp Parker, *Cyberspace, Cybersecurity, and Cybercrime*, 31.
[410] Darıcılı, *Siber Uzay ve Siber Güvenlik*, 65.
[411] Shefali Virkar, "The Mirror Has Two Faces: Terrorist Use of the Internet and the Challenges of Governing Cyberspace," içinde *National Security and Counterintelligence in the Era of Cyber Espionage,* ed. Eugenie de Silva (ABD: Information Science Reference, 2016), 3.
[412] Darıcılı, *Siber Uzay ve Siber Güvenlik*, 66-68.
[413] Kremling ve Sharp Parker, *Cyberspace, Cybersecurity, and Cybercrime*, 57.

Savaşı'nda, ağ teknolojileri etkin bir biçimde kullanılmıştır. İletişim teknikleri ve kitle iletişim araçlarının hızlı bir biçimde olayı aktarmış olması önemli olmuştur.[414] Siber olaylar artık kendini daha etkin bir biçimde göstermektedir. Aynı zamanda olayların aktarımı, iletişim açısından geçen bir on yıl öncesine kadar büyük adımlar atıldığının göstergesidir. Avantaj olarak; iletişim ve aktarımın hızlanması, anlık iletişimde büyük bir adımdır. Siber anlamda dezavantaj ise; tehdit ve saldırılar açısından tehlikenin daha çok artmasına sebep olmuştur.

1990'lı yıllarda, teknoloji hızla ilerlemiştir. Bu sebeple; teknolojik olaylar artmış, artık siber anlamda hızlı bir döneme girilmiştir. Çöl Fırtınası (Desert Storm); ABD'nin icadı olan, Irak'a yönelik bir harekâttır. Nisan 1991'de, bazı Hollandalı hackerlar tarafından ABD kuvvet komutanlıkları ve Savunma Bakanlığı birimine siber saldırı yapılarak sızmıştır.[415] 1994 yılında, ABD istihbarat organizasyonları ve Savunma Bakanlığı "Ortak Güvenlik Komisyonu" ile ağ teknolojilerinin yayılmasıyla gelebilecek riskleri incelemiştir. Sonuç olarak; bilişim teknolojisinin güvenlikten hızlı ilerlediği, eğitimin yeterli olmadığı, hem özel sektörün hem Pentagon'un bu sistemlere bağlı olmasından dolayı devletin zayıflığını göstermiştir.[416] Yapılan incelemelerle ABD eksik alanlarda çalışma yapmaya yönelmiştir.

1995 yılında, ABD Ulusal Savunma Üniversitesi, olası bir siber savaşta görev alacak, bunu komuta edecek, siber savaşçı isimli ilk subay mezunlarını vermiştir.[417] Aynı yıl, ABD, siber güvenlik alanı için, Temmuz ayında ilk resmi belge olan; 13010 No'lu Başkanlık Direktifi (Presidential Directive 13010)[418]'ni yayımlamıştır.[419] ABD, siber alanla alakalı hem eğitim hem önlemler alınması için yapılması gerekenler üzerine çalışmalarda bulunmuştur. İlerleyen yıllarda, bazı yaşanan olaylar, eksiklerin görülmesiyle siber alanda yapılan çalışma ve politikalara yön vermiştir.

1998 yılı Şubat ayında Solar Sunrise (Güneşin Doğuşu) yaşanmıştır. DoS saldırı çeşitleri kullanılarak, ABD donanması, deniz ve hava kuvvetlerine siber

[414] Darıcılı, *Siber Uzay ve Siber Güvenlik*, 70.
[415] Bayraktar, *Siber Savaş ve Ulusal Güvenlik Stratejisi*, 147.
[416] KURGAN, *Siber Mücadeleye Giriş*, 107.
[417] Darıcılı, *Siber Uzay ve Siber Güvenlik*, 70.
[418] Federation of American Scientists, *Executive Order EO 13010 Critical Infrastructure Protection,* E.T.: 15 Eylül 2018, url: https://fas.org/irp/offdocs/eo13010.htm.
[419] Darıcılı, *Siber Uzay ve Siber Güvenlik*, 71.

saldırılar yapılmıştır. Pentagon, Kaliforniya'da iki çocuk tarafından hacklenmiştir.[420] Ay Işığı Labirenti (Moonlight Maze) isimli siber saldırıysa; 1998'de, ABD Savunma Bakanlığı ve önemli bazı üniversitelere ait bilgisayarlara yapılmış saldırılardır. Bu saldırıyla önemli bilgiler alınmış, daha önemlisi bilgiler içerisinde füze güdüm sistemleri, gizli denizcilik kodlarına ait bilgiler de vardır.[421] ABD açısından, önemli belgelere ulaşılmış olması, çok tehlikeli boyutlara çıkabileceğinin göstergesi olmuştur. Alınan önlemlerin yetersiz kalmasıyla yeni çalışmalar yürütülmüştür.

Bill Clinton'un başkanlık yaptığı dönemde, PD-63 isimli Başbakanlık Direktifi yayımlanmıştır. Başkanlık Direktifinde; sektörel zayıflıklar, olabilecek siber terör saldırıları, askeri önlemlerden bahsedilmiştir.[422] Direktif 63 (63 No'lu Başbakanlık Direktifi- Presidential Directive-63)[423]; Clinton döneminde, 1998 yılının 22 Mayıs tarihinde yayımlanmıştır. Dijital anlamda stratejik, önemli devlet ve özel kurumlarda geçerli olacak şekilde, insan hatası, makine arızası, doğa ve terör saldırıları ihtimaline karşı hazırlanmış direktiflerdir. CIA (Central Intelligence Agency – Merkezi İstihbarat Teşkilatı), FBI (Federal Bureau of Investigation – Federal Araştırma Bürosu) gibi ulusal güvenlik kurumları, bir saldırı ihtimaline karşı yetkili kılınmıştır. Stratejik nitelikte olan, sektörleri korumak amaçlı Ulusal Altyapıyı Sağlama Planlarıyla birimler bilgilendirilip, risk ve tehditlere karşı önleyici çalışmalar yapılmıştır.[424] Aynı zamanda direktif, resmi anlamda ABD'nin kritik altyapılarını tanımlamış olduğu ilk dokümandır.[425] Direktif sayesinde, hem altyapıların tanımı yapılmış, hem de siber alan ve onunla alakalı olabilecek dijital tehdidin adı geçmesiyle, artık siber alan bir güvenlik alanına dönüşmeye başlamıştır. Çalışmalar; bu tanımlamalarla, ABD'nin kendi ulusal güvenlik kurumları üzerinden yapılmıştır. Artık, siber alanı ilgilendiren çalışmalara, önceki dönemlere göre daha önem verilmeye başlanmıştır. Çalışmalar dönemin ilerlemesiyle bu kadarla kalmamış, ilerlemeler göstermiştir.

---

[420] Ashfaq Ahmad Malik, Athar Mahboob, Adil Khan ve Junaid Zubairi, "Application of Cyber Security in Emerging C4ISR Systems and Related Technologies," içinde *Cyber Security Standards, Practices and Industrial Applications: Systems and Methodologies*, ed. Junaid Ahmed Zubairi ve Athar Mahboob (Amerika: Information Science Reference, 2012), 235.

[421] Bayraktar, *Siber Savaş ve Ulusal Güvenlik Stratejisi*, 147-148.

[422] Çakmak ve Altunok, *Suç, Terör ve Savaş Üçgeninde Siber Dünya*, 104.

[423] Federation of American Scientists, *Presidential Decision Directive/NSC-63*, E.T.: 15 Eylül 2018, url: https://fas.org/irp/offdocs/pdd/pdd-63.htm.

[424] Çakmak ve Altunok, *Suç, Terör ve Savaş Üçgeninde Siber Dünya*, 104.

[425] Darıcılı, *Siber Uzay ve Siber Güvenlik*, 72.

ABD, Temmuz 2002'de, Donanma Savaşı Akademisinde, simülasyon şeklinde yapılmış olan 'Dijital Pearl Harbor' ile olası bir terörist saldırısının sonuçlarıyla ortaya çıkma ihtimali olan maliyetleri belirlemiştir.[426] 2003 yılı Şubat ayında, Siber Uzay'ın Korunmasına Yönelik Ulusal Strateji (The National Strategy to Secure Cyberspace)[427] belgesiyle; geniş kapsamlı bir siber uzay tanımı, hedefleri, planları, korunması ve tehditleri açıklamış, bu konuda ilk doküman olmuştur.[428] 2003 yılında, II. Körfez Savaşı (Irak Savaşı), fiziksel bir savaşla beraber siber saldırının ilk defa kullanıldığı savaş olarak kabul edilmiştir.[429] 2003 yılından itibaren ABD, Ekim ayını Siber Güvenlik Farkındalık Ayı olarak ilan etmiştir.[430] Ekim ayında siber güvenlik üzerine farkındalık oluşturmak amacıyla, özellikle Barack Obama döneminde belirli etkinlikler düzenlenmiştir.[431] Artık siber alan tamamen kendine özel bir alan olarak bahsedilmeye başlanmıştır. Hatta üzerine farkındalık oluşturulması gerekecek kadar önem verilmiştir.

Yapılan çalışmalarla alınan önlemler, bir süre etkili olsa da, çok uzun sürmemiştir. Kasım 2004 yılında, başta ABD'nin askeri sistemleri olmak üzere pek çok kurum ve firmanın bilgisayarlarına "Titan Yağmuru (Titan Rain)" isimli siber saldırılar gerçekleşmiştir. Devlette önemli ve hassas bilgilerin bulunduğu pek çok korumalı bilgisayara Truva atıyla sızılmış, saldıranınsa Çin Halk Cumhuriyeti olduğu söylenmiştir.[432] Titan Yağmuru adlandırması; saldırıların yağmur gibi yağmasından kaynaklanmıştır. Titan Yağmuru saldırısıyla siber anlamda yeni kavramlar ortaya çıkmıştır.[433] Siber alan yenilenip gelişmeye devam etmiştir. Siber alanda ABD, bilgi ve askeri alanda saldırı açısından önemli hedeflerden biridir. Ancak, saldırılar tek taraflı olmamıştır. Yaşanan olaylardan bazıları ABD için politikalarını geliştirme açısından önemli olmuştur. ABD geliştirme çalışmalarında, sadece teknolojik değil, kurumlarında da çalışmalar yürütmüştür.

---

[426] Erbschloe, *Trojans, Worms, and Spyware,* 167.
[427] The White House, *The National Strategy To Secure Cyberspace* (Washington: Şubat 2003), E.T.: 15 Eylül 2018, url: https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf.
[428] Darıcılı, *Siber Uzay ve Siber Güvenlik*, 73.
[429] KURGAN, *Siber Mücadeleye Giriş*, 179.
[430] Center of Internet Security, *October: National Cybersecurity Awareness Mont,* E.T.: 15 Eylül 2018, url: https://www.cisecurity.org/blog/october-national-cybersecurity-awareness-month/.
[431] KURGAN, *Siber Mücadeleye Giriş*, 157.
[432] Bayraktar, *Siber Savaş ve Ulusal Güvenlik Stratejisi*, 148.
[433] Keleştemur, *Siber İstihbarat*, 142.

2005 yılı Mayıs ayında, CIA bir savaş oyunu simülasyonu "Silent Horizon"'u geliştirmiştir. ABD, olası bir siber savaş karşısında, savunma amaçlı oyunla, risklere karşı alınabilecek önlemleri göstermek için ortaya çıkartmıştır.[434] 2006 yılındaysa, yayımlanan ulusal güvenlik belgesinde; yapısında istikrarsızlık bulunan teröre karşı mücadeleden söz edilmiştir. Genel anlamda belgede; liberal amaçlara ulaşmak için realist araçların kullanıldığı bir strateji tanımlaması yapılmış, başka açıdan da tam tersi olduğu söylenmiştir.[435] Siber alanda yapılan çalışmalar, her geçen yılda, bir sonrakine göre yetersiz kalmıştır. Yeni gelişen saldırılarla daha büyük tehlikelerin ortaya çıktığı görülmüştür.

2009 yılı Nisan ayında; hackerlar ABD Savunma Bakanlığı sistemlerine girmiş ve F-35 savaş uçağı bilgileriyle birçok hassas askeri bilgiyi ele geçirmiştir.[436] Aynı yıl, dönemin başkanı Barack Obama, Siber Uzay Politika Revizyonu'nu (Cyberspace Policy Review)[437] yayımlamıştır. Yayımlanan belgede; siber savunma için alınabilecek önlemler, problemlerin giderilmesi, alanla ilgili tüm kurum ve kuruluşların beraber hareket etmesi gerektiğini belirtmiştir.[438] 2010 yılında yayımlanan ulusal güvenlik belgesinde, uluslararası alanda yaşanabilecek değişim ve dönüşümle, gelebilecek istikrarsızlığın önüne geçmek amaçlı yöntemler öngörülmüştür. Bu belgede tüm boyutlar ele alınmıştır. Ekonomi ön plana çıkmış, liberalizm araç olarak kullanılarak, izolasyoncu hedefle, ekonomik anlamda büyüyüp güvende olunacağı düşüncesi ortaya atılmıştır. Bu belgeyle, yeni bir güvenlik alanı olarak kabul edilen siber alanla, burada oluşabilecek herhangi bir saldırı, tehdit olarak görülmektedir.[439] Siber alan, daha dikkat edilmesi ve korunması gereken bir yapı haline gelmiş, özellikle bu dönemde daha önemli bir yere sahip olmuştur. Kurumların beraber çalışması; siber alanın her yapı içerisine yayıldığını göstermektedir. Aynı zamanda 2010 yılında; ekonominin bu alanda öneminden söz edilmesinin siber alana da etkisi vardır. Teknolojiyi en iyi biçimde kullanmak için ekonomik olarak da güç önemlidir. Bu da pek çok alanda güçlü olmayı sağlayacaktır.

---

[434] Haydar Çakmak ve Taner Altunok, *Suç, Terör ve Savaş Üçgeninde Siber Dünya* (Ankara: Barış Platin Yayınevi, Mayıs 2009), 105-106.
[435] Yalçın, *Ulusal Güvenlik Stratejisi*, 39-74.
[436] Bayraktar, *Siber Savaş ve Ulusal Güvenlik Stratejisi,* 148.
[437] Homeland Security, *2009 Cyberspace Policy Review,* E.T.: 15 Eylül 2018, url: https://www.dhs.gov/publication/2009-cyberspace-policy-review.
[438] Darıcılı, *Siber Uzay ve Siber Güvenlik*, 76.
[439] Yalçın, *Ulusal Güvenlik Stratejisi*, 39-135.

2010'da, dönemin ABD senatörü Joseph Lieberman ve Susan Collins'in hazırlamış olduğu " Siber Uzayın Milli Değer Olarak Korunması Kanun Taslağı" Amerika Başkanı'na bir tehlike anında interneti kapatma yetkisi vermiştir. Bu yetkiyi sadece "Milli Siber Acil Durumları (National Cyber Emergency)"nda kullanabileceğini belirtmiştir.[440] 2010 yılı 21 Mayıs tarihinde, ABD Siber Komutanlığı resmi olarak kurulmuştur.[441] 31 Ekim 2010 tarihinde resmi olarak faaliyete başlamıştır.[442] Kurulan Siber Komutanlık, ABD'nin, siber alan için artık savaş alanı kadar önem vermeye başladığını gösterir. Aynı zamanda siber alan artık bir kuruma ihtiyaç duyacak düzeye gelmiştir. 2010 yılında ayrıca; Stuxnet solucanı ortaya çıkmıştır. Stuxnet sebebiyle, İran ve ABD arasında neredeyse bir savaş çıkmak üzereyken, bunun eşiğinden dönülmüştür.[443] Stuxnet olayı daha çok ilerleseydi, fiziksel savaşa dönüşme ihtimali vardı. Saldırılan tesisin bir nükleer tesis olması, hatalı bir işlemle ciddi zararlara sebep olabileceğini göstermektedir. Ciddi zararlar ortaya çıkmamış olması, İran'a farklı açılardan zararlar geldiği gerçeğini değiştirmemektedir. İki devlet arasında gerginlik yaşanması dahi uluslararası alanda soruna sebep olmaktadır. Ancak ABD'nin saldırıyı kabul etmemiş olması, ilişkilerin daha fazla gerilmemesine sebep olmuştur. Yaşanan Stuxnet olayı, siber savaşın uluslararası ilişkilerde ayrıca ele alınması gerektiğini göstermiştir. Ayrıca en büyük ve tehlikeli örneklerinden biri olmuş, ABD sonrasında çalışmalarıyla belirli stratejiler belirlemeye devam etmiştir.

2011 yılında ABD "Siber Alan için Uluslararası Strateji (International Strategy for Cyberspace)"[444]'yi, aynı yıl "Savunma Bakanlığı Siber Alan Harekât Stratejisi (DoD Strategy for Operating in Cyberspace)"[445]'ni yayımlamıştır. İlk belgede; siber strateji, siber güvenlik politikası, ortamın geleceğinden

[440] Bıçakçı, *21. Yüzyılda Siber Güvenlik*, 11-12.
[441] "The Creation of U.S. Cyber Command," ABD Siber Komutanlığı, E.T.: 16 Ağustos 2019, url: https://www.cybercom.mil/About/History/.
[442] "About Us," ABD Siber Komutanlığı, E.T.: 16 Ağustos 2019, url: https://www.cybercom.mil/About/
[443] Keleştemur, *Siber İstihbarat*, 147.
[444] The White House, *International Strategy for Cyberspace* (Amerika: Mayıs 2011), E.T.: 17 Eylül 2018, url: https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.
[445] ABD Savunma Bakanlığı, *DoD Strategy for Operating in Cyberspace* (Amerika: Temmuz 2011), E.T.: 17 Eylül 2018, url: https://csrc.nist.gov/CSRC/media/Projects/ISPAB/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf.

bahsedilirken, ikinci belgede; siber alan faaliyetleri için beş stratejik girişim hakkında bilgi verilmiştir.[446]

2012 yılında; ABD'nin gizli hazırlamış olduğu siber harekât politikasını, NSA (National Security Agency- Milli Güvenlik Teşkilatı) çalışanı olan Edward Snowden internet ve basına sızdırmıştır.[447] Bu şekilde ortaya çıkan doküman, "Başkanlık Politika Direktifi 20-ABD Siber Harekât Politikası (Presidential Policy Directive 20 (PPD-20)-U.S. Cyber Operations Policy)"[448] şeklinde yayımlanmıştır.[449] Gizli belgelerin ortaya çıkması, ABD için problem oluşturmuştur. Siber alanın her yerden istenildiği anda ulaşıma açık olması, istense bile bazı şeylerin gizli kalamadığının en önemli göstergesidir. Gizliliğin azalmasıysa özellikle bazı devletlerin önemli bilgileri açısından, kendi politikaları için tehlike oluşturmaktadır.

ABD tehditlerin boyutlarını gördükçe kritik altyapılar üzerine ayrı çalışmalar yürütmüştür. Altyapılar, siber alanın getirdikleriyle, korunması gereken önemli yapılardan olmuştur. Özellikle siber alana bağlı olması, tehdide açık olması anlamına gelmiştir. 12 Şubat 2013 yılında "Kritik Altyapıların Geliştirilmesi (President's Executive Order on Drawing up a Strategy for Improving Critical Infrastructure Cybersecurity)" başkanlık direktifi yayımlanmıştır. 12 Şubat 2014 yılındaysa, "Kritik Altyapıların Geliştirilmesi için Taslak Plan (Draft Strategy for Improving Critical Infrastructure Cybersecurity)" hazırlanmıştır. İki belgeyle; resmi kurum ve özel sektör iş birliğine dayanan, kritik altyapıların korunması amaçlı ortak standart ve yöntemler geliştirilmesi hedefi belirlenmiştir.[450] 23 Nisan 2015 yılında, ABD "Savunma Bakanlığı Siber Stratejisi (The Department of Defence Cyber Strategy)" adlı belgeyi yayımlamıştır.[451] 24-25 Eylül 2015 yılında, Çin Halk Cumhuriyeti ve ABD başkanları görüşmüş, siber silah kontrolüyle, saldırılarda sınırlama yapılabilmesi için çalışmalarından söz etmişlerdir.[452] Siber alanın silah olarak kullanımında,

[446] Çiftçi, *Her Yönüyle Siber Savaş*, 75.
[447] Johnson, "Cyber Intelligence, Cyber Conflicts, and Cyber Warfare," 183.
[448] Federation of American Scientists, *Presidential Policy Directive/PPD-20* (Amerika: 2012), E.T.: 17 Eylül 2018, url: https://fas.org/irp/offdocs/ppd/ppd-20.pdf.
[449] Çiftçi, *Her Yönüyle Siber Savaş*, 75.
[450] Darıcılı, *Siber Uzay ve Siber Güvenlik*, 78-79.
[451] "The DoD Cyber Strategy," ABD Savunma Bakanlığı, E.T.: 16 Ağustos 2019, url: https://archive.defense.gov/home/features/2015/0415_cyber-strategy/final_2015_dod_cyber_strategy_for_web.pdf.
[452] Çiftçi, *Her Yönüyle Siber Savaş*, 136.

güvenlik açısından belirli sınırlar içerisine sokulması istenmiştir. Artık tehditler ufak boyutlardan, büyük tehlikelere gitmeye başlamıştır.

2016 yılında yapılan başkanlık seçimlerinde, Rusya'nın ABD seçimlerine siber yöntemlerle müdahale ettiği yönünde iddialar ortaya atılmıştır. Ortaya atılan iddialar, Soğuk Savaş sonrasından günümüze kadar savaşın, siber anlamda nerelere geldiğini gösterir.[453] Günümüz ABD başkanı Donald J. Trump, siber bir saldırı karşısında, eskiye göre sert cevaplar verileceğini gösteren bir belge imzalamıştır. 2018 Ekim ayında Trump, "Ulusal Siber Güvenlik Strateji Belgesini"[454] imzalayarak yasal ve sistem üzerine düzenlemede bulunacağını belirtmiştir.[455] Bu belge, 15 yıl sonra ilk defa siber strateji üzerine başkanın imzaladığı belgedir. Ayrıca belgede; siber alan bağımsız görülmeden, her alanla bağlantılı şekilde dikkate alınarak stratejiler izleneceği belirtilmiştir.[456]

2019 yılındaysa, pek çok politika üretilmekte, yeni sorunlar aynı hızda ortaya çıkmaktadır. Yakın dönemde ABD bir seçim sürecine girecektir, ancak 2016 yılında konuşulan, Rusya'nın ABD seçimlerine müdahalesi iddiaları üzerine çalışmalar yaptıklarından söz edilmektedir. ABD'nin gelecek 2020 seçimleri için önlemler alınmaya başladığı haberlerde yer alırken, olası bir müdahale karşısında siber bir saldırı hazırlığı da planlandığı bahsedilmiştir. Bu planlamalarla, geçmiş siber saldırılara bakılarak dijital bir biçimde Soğuk Savaşın artma riskinden de söz edilmiştir.[457]

Siber alan, politikaları etkileyecek bir konuma gelişmiş, hayatın her alanındaki yapılara yayılmıştır. Önemli çalışmaları beraberinde getirmiş, ancak, yeni geliştirilen yöntemler kısa sürede yetersiz kalmıştır. Siber alanın hızlı ilerlemesiyle, yapılan herhangi bir çalışma, kısa sürede yine yetersiz kalacaktır. Stratejik olarak, belirli belgeler hazırlanmış ve çalışmalar yürütülmüştür. Gelecek

[453] KURGAN, *Siber Mücadeleye Giriş*, 56.
[454] The White House, *National Cyber Strategy of the United States of America* (Amerika: Eylül 2018), E.T.: 21 Eylül 2018, url: https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.
[455] Habertürk, *Trump'tan Yeni Siber Güvenlik Stratejisi,* E.T.: 21 Eylül 2018, url: https://www.haberturk.com/trump-tan-yeni-siber-guvenlik-stratejisi-2149858.
[456] Grant Schneider, "President Trump Unveils America's First Cybersecurity Strategy in 15 Years," *The White House* (Eylül 2018), E.T.: 21 Eylül 2018, url: https://www.whitehouse.gov/articles/president-trump-unveils-americas-first-cybersecurity-strategy-15-years/.
[457] "ABD ve Rusya Arasında Dijital Soğuk Savaş," *Hürriyet Haber*, 17.06.2019, E.T.: 16 Ağustos 2019, url: http://www.hurriyet.com.tr/dunya/abd-ve-rusya-arasinda-dijital-soguk-savas-41246160.

dönemler için de yeni çalışmalar yapılmaktadır. ABD'nin siber güvenlik alanında, siber anlamda güvenlikten sorumlu belirli kurumları bulunmaktadır. ABD'nin siber güvenlik alanında çalışma yürüten kurumlarından kısaca söz etmek gerekir.

Siber Komutanlık (U.S. Cyber Command-USCYBERCOM); siber saldırı, askeri anlamda ağ ve sistemlerin korunması, savunma, gerektiğinde saldırı yapabilme kabiliyetine sahiptir.[458] Savunma Bakanlığı içerisinde bulunan, 2010 yılında kurulan CYBERCOM, siber kaynakları düzenleme, bilgisayar ağlarını, özellikle askeri olanları savunma amaçlı faaliyet göstermektedir.[459] Milli Güvenlik Teşkilatı (National Security Agency-NSA); ABD'nin istihbarat teşkilatlarından biridir. Aynı zamanda ulusal güvenliği sağlamak, çıkarların korunması, esas görevlerindendir. NSA; kriptoloji, bilgisayar ağ işlemleri, bilgi güvencesi ve istihbarat sinyallerinden sorumludur.[460] Siber alanda koruma amaçlı istihbarat desteğini İç Güvenlik Bakanlığı'na yapmaktadır. Savunma Bakanlığı'nın kriptografik istihbarat birimi adı altında geçmektedir. Sinyal ve iletişim istihbaratı için görev yapmaktadır.[461]

İç Güvenlik Bakanlığı (Department of Homeland Security-DHS); sivil ve devlet ağlarını koruyup, kritik altyapı ağlarını güvende tutmaktadır. Bu amaçla özel sektör desteğini düzenleyip, siber saldırı karşısında koordinasyonu sağlamaktadır.[462] İç Güvenlik Bakanlığı 11 Eylül 2011 saldırısı sonrasında kurulmuştur.[463] Görevleri geniş ve çeşitlidir. Ancak esas başlangıçta terörle mücadeleye yoğunlaşmıştır. Kuruluşunun ileri dönemlerinde deniz ve sınır güvenliği beraberinde, hükümetin doğal afetlere müdahalesini koordine etmeye kadar birçok alanı kapsamıştır. Alt birimlerinde siber güvenlik çalışmaları da yürütülmektedir.[464]

Federal Araştırma Bürosu (Federal Bureau of Investigation-FBI); siber istihbaratta en yetkili kurumdur.[465] Siber alanda, bir siber saldırının araştırılması ve engellenmesinden sorumludur. Siber alan dışında terör saldırıları, istihbarat operasyonları, yolsuzluk ve birçok önemli suçla mücadeleyi kapsayan bir çalışma

[458] Çiftçi, *Her Yönüyle Siber Savaş*, 32.
[459] Darıcılı, *Siber Uzay ve Siber Güvenlik*, 89.
[460] Johnson, "Cyber Intelligence, Cyber Conflicts, and Cyber Warfare," 183.
[461] Keleştemur, *Siber İstihbarat*, 182.
[462] Çiftçi, *Her Yönüyle Siber Savaş*, 33.
[463] Darıcılı, *Siber Uzay ve Siber Güvenlik*, 94-96.
[464] "In Focus," Homeland Security, E.T.: 16 Ağustos 2019, url: https://www.dhs.gov/focus.
[465] Hasan Çiftçi, *Her Yönüyle Siber Savaş* (Ankara: TÜBİTAK Popüler Bilim Kitapları, Temmuz 2017), 33.

alanı bulunmaktadır.[466] Kurum içerisinde yapılan faaliyetler gizli bilgi olarak geçmekte, belirli sebepler olmadığı sürece dışarıyla paylaşılmamaktadır.[467]

Kurumlarda yapılan çalışmalar, siber alanın korunması gereken bir güvenlik yapısı olduğunu gösterir. Ayrıca siber alanın tehlikesi, yapılan çalışmalara yansımıştır. Siber alan, savaş ihtimali ve bir bölgede aynı anda pek çok yapıya zarar verilmesini sağlayacak güçtedir. Güvenlik çalışmaları, diğer devletler gibi ABD'de de zarar oluştuktan sonra ortaya çıkmıştır. Siber alan, her alan ve devleti, hatta her bireyi kapsamaktadır. Bu sebeple eskisinden daha ciddiye alınması gereken bir alan olmuştur.

Genel anlamda ABD, siber alanda pek çok çalışmada bulunmuştur. Belirli örneklerin etkili olduğu çalışmalar, güvenliğin yeterli olmadığı dönemlerde ortaya çıkmıştır. Çeşitli saldırılar ve güvenlik ihlalleri, devletin yeni politikalar izlemesi ve çalışma alanları oluşturmasına sebep olmuştur. Günümüzde çalışmaları devam eden projeler vardır. Siber alan üzerinde çalışmalar ve politikalar geliştirilmektedir. Ancak, geri planda tutulması ya da gizli yürütülmesi, dışarıdan, kapasitenin altında çalışmalar olarak yorumlanmaktadır. Aynı zamanda örnekler ve politikalar, siber alanda, devletlerarası ilişkilerde gerginliklerin, olası bir siber saldırıda ortaya çıkabileceğini göstermektedir. Günümüzde politik, hatta henüz dijital bir Soğuk Savaş şeklinde görülen bu saldırılar, kritik bir yapıya yapıldığı anda, büyük sonuçlara dönüşebilme ihtimalini barındırdığı görülmektedir. Ancak, ABD'nin çalışmaları kendini koruma amaçlıdır. Başka devletler de bu konuda önemli adımlar atmıştır. Çalışma yapan önemli örneklerinden bir tanesi; Çin Halk Cumhuriyeti'dir. Günümüzde siber alandan söz edildiğinde akla gelen önemli devletlerden biri olması; çalışmalar açısından, ciddi adımlar atması sebebiyle kendinden söz edilesi için yeterlidir. Siber çalışmaların iyi anlaşılması için Çin Halk Cumhuriyeti'nin yapmış olduğu çalışmaları ayrıca incelemek gerekir.

2.1.2. Çin Halk Cumhuriyeti

Çin Halk Cumhuriyeti, günümüzde siber alanda önemli ülkelerdendir. Hızlı bir şekilde ekonomik olarak ilerlerken, teknolojide de aynı ölçüde ilerlemiştir. Özellikle ABD başta olmak üzere, siber dünyada bir tehdit olarak

[466] "Mission & Priorities," Federal Bureau of Investigation, E.T.: 16 Ağustos 2019, url: https://www.fbi.gov/about/mission.
[467] Ali Burak Darıcılı, *Siber Uzay ve Siber Güvenlik* (Bursa: Dora Yayıncılık, Aralık 2017), 100.

görülmüştür.[468] Çin Halk Cumhuriyeti'nin alışılmışın dışında yöntemler izleyen bir devlet olması, onu önemli kılar. Dışarıya açık bir devlet değildir. Her konuda diğer devletler kadar açık olmaması, bir olay karşısında nasıl tepkiler göstereceği ya da izleyeceği yöntemleri tahmin etmeyi zorlaştırır. Karşı taraf açısındansa davranışlarını belirlemek zorlaşır. Çin Halk Cumhuriyeti'nin dışarıya kapalı oluşu internet gibi ortamlarda da etkili olmuştur. Dış dünyaya hızlı bir biçimde bağlantı sağlayan yapı için ayrı düzenlemeler getirmiştir.

Çin Halk Cumhuriyeti, internet kullanımı üzerine, diğer devletlerden farklı çalışmalar yapmıştır. İnternet kullanımında, yabancı sitelere erişimi engellemiş, sorguları filtrelemiştir. Sansürler uygulayarak, vatandaşların belirli ölçüde internet kullanımını sınırlamıştır. Uygulanan sınırlamalara sebep; devlet güvenliği, gücün ve ulusal birliğinin bozulmaması için tehditleri dışarıda bırakmak gösterilmiştir.[469] Çin Halk Cumhuriyeti, interneti kendi eline almak için belirli yöntemler izlemiştir. Yöntemlerden iki tanesi olan; "Great Firewall of China (Çin Büyük Güvenlik Duvarı)" ve "Green Dam (Yeşil Baraj)" isimli güvenlik sistemlerini kurmuştur. Güvenlik sistemlerinin özelliği; siber savaş tehdidi karşısında, sistemini bloke ederek, kendini dışarıya kapatmaktır.[470] Great Firewall of China; teknik savunmanın ilk kısmıdır. Devletin internet trafiğini izleyerek, dışarıdan gelecek tehditler ya da saldırıları engellemeyip, gereken yerde girilen sayfaları incelemesi şeklinde işler. Green Dam; 2009 yılında, Çin Halk Cumhuriyeti'nde satılan bütün bilgisayarlara kurulması istenmiş bir yazılımdır. Belirli sitelerde görüntü ve sitelerin kendisini engellemek için programlanmış, ancak bireysel bilgisayarlarda tartışma yaratmış, sonucunda da iptal edilmiştir.[471] Çin Halk Cumhuriyeti, bir tehdidin önüne geçmek için, kontrolün elinde olması gerektiğini savunmuştur. Farklı açılarda değerlendirirsek; özgürlüklerin kısıtlanması açısından olumsuz, tehlikeyi önceden görüp durdurmak açısından olumludur. Önemli olan; sistem izlenirken, kısıtlamaların toplumu ne şekilde etkileyeceğine dikkat etmektir.

[468] Çakmak ve Altunok, *Suç, Terör ve Savaş Üçgeninde Siber Dünya*, 130.
[469] Roger Hurwitz, "A New Normal? The Cultuvation Of Global Norms As Part Of A Cybersecurity Strategy," içinde *Conflict and Cooperation in Cyberspace,* edit. Panayotis A. Yannakogeorgos ve Adam B. Lowther (Amerika: Taylor & Francis Group, 2014), 239.
[470] Clarke ve Knake, *Siber Savaş,* 35.
[471] Dean Cheng, *Cyber Dragon* (Amerika: PRAEGER, 2017), 67-71.

Çin Halk Cumhuriyeti, 1980'li yılların başında, bilgi teknolojisine dikkat etmeye başlamıştır. 1986 yılında; "Çin Ulusal Yüksek Teknoloji Araştırma ve Geliştirme Planı (Chinese National High-Technology Research and Development Plan)" olan; "Plan 863", teknolojik alanlarda yeteneklerin teşvik ve hızlandırılmasını amaçlamıştır. 1991 yılındaysa ilk olarak İnternet'e katılmıştır.[472] 1990'lı yılların ortalarına geldiğinde, Körfez Savaşı sonrası stratejisinde değişiklik yapmıştır. Orduda küçülüp, teknolojiye yatırım yaparak, 1990'lı yılların sonlarına doğru siber savaş birliklerini kurmayı amaçlamıştır.[473] Çin Halk Cumhuriyeti 1990'ların başından itibaren, siber savaşla alakalı sistemli biçimde çalışmalar yapmış, internet altyapısı için koruma yöntemleri geliştirmiştir.[474] Çin Halk Cumhuriyeti, siber alanla ilgili çalışmalarına, internete katılımın hemen sonrasında başlamıştır. 1990'lı yıllarda siber alanın kendini geliştirdiği, günümüz yapısına evirildiği süreçte, devlet ileriye yönelik çalışmaları hedeflemiştir. Altyapı çalışmalarınaysa, olası bir siber savaşa hazırlıksız yakalanmamak için başlamışlardır.

Şubat 1994 yılında, Çin Halk Cumhuriyeti Devlet Konseyi "Bilgisayar Bilgi Sistemlerinin Güvenlik Koruması Yönetmeliği" isimli 147 sayılı kararı yayımlamıştır.[475] Yayımlanan kararla, Kamu Güvenliği Bakanlığı (MPS), devletin bilgisayar bilgilerini denetleme sorumluluğunu üstlenmiş, 1996 yılında, 195 sayılı Devlet Konseyi Kararıyla[476] desteklenmiştir.[477] Çin Halk Cumhuriyeti, çalışmalarını sıkı bir şekilde ilerletmesine rağmen teknolojik ilerlemelerle bazı konularda yetersiz kalmıştır. Ancak bu, çalışmalarına daha çok eğilmelerine sebep olmuştur.

1998 Mayıs ayında, Çin Halk Cumhuriyeti'ne karşı Endonezya'da gösteriler başlamıştır. Gösterilere tepki olarak "Çin Hacker Acil Toplanma Merkezi (China Hacker Emergency Meeting Center)" ismi altında bir çok hacker bir araya gelerek, Endonezya hükümeti internet sitelerine saldırmıştır.[478] 7 Mayıs 1999 tarihinde, NATO savaş uçağı, yanlışlıkla Yugoslavya'ya ait Belgrad

[472] Cheng, *Cyber Dragon*, 2-3.
[473] Clarke ve Knake, *Siber Savaş,* 33.
[474] KURGAN, *Siber Mücadeleye Giriş*, 155.
[475] Cheng, *Cyber Dragon*, 63.
[476] Federation of American Scientists, *Regulations on Safeguarding Computer Information Systems*, E.T.: 27 Eylül 2018, url: https://fas.org/irp/world/china/docs/computer_code.htm.
[477] Cheng, *Cyber Dragon*, 63.
[478] Başaran, *Siber Savaş Cephesinden Notlar*, 37.

şehrindeki Çin Büyükelçiliği'ni bombalamıştır.[479] Hemen sonrasında, ABD hükümeti internet sitelerine, Çin Halk Cumhuriyeti kaynaklı yoğun saldırılar yapılmıştır.[480] 2001 yılı Nisan ayındaysa, Çin Halk Cumhuriyeti ve ABD ordularına ait iki uçak, Güney Çin Denizi sınırlarında çarpışmıştır.[481] Çin Halk Cumhuriyeti içerisindeki hackerlar, ABD hükümetine siber saldırılara başlamış, bu "I. İnternet Dünya Savaşı" şeklinde isimlendirilmiştir.[482] 1 Nisan tarihinde gerçekleşen olay, ABD ve Çin Halk Cumhuriyeti arasında politik ve siber gerginliklere sebep olmuştur.[483] "Honker Union of China" isimli hacker grubu olayı üstlenmiş, yaptıkları saldırıları ilan etmiştir.[484] Yaşanan olayın adı; Çin Halk Cumhuriyeti'ne ait uçağın düşmesiyle, ABD uçağının ağır hasarla Hainan Adasına zorunlu iniş yapması sebebiyle, Hainan Adası Olayı denmiştir.[485] Bunlar, siber alan açısından büyük önem taşıyan olaylardandır. Ayrıca önemli başka bir nokta; geçmişten gelen birikimlerle, günümüzde, siber alanda, fiziksel yansıması görünmeyen I. Dünya Siber Savaşı devam etmektedir. Devletlerarasında yansımaları vardır. Ancak anında bir yansımadan çok birikmeler ya da daha büyük, fiziksel bir sonuç çıkartacak olaylar yaşandığı, toplumlarda etki gösterdiği bilinmektedir. Ancak 2000'li yılların başında olaylar bu kadarla kalmamış, yeni olaylar yaşanmıştır.

Siber istihbaratın ortaya çıktığı dönemlerden olan 2002 yılındaki olaylardan bir tanesi; Titan Yağmuru (Titan Rain)'dur.[486] Çin Halk Cumhuriyeti, ABD'nin savunma şirketlerine saldırarak, belirli bilgileri toplamayı amaçlamıştır.[487] Siber anlamda istihbarat yaşanırken, siber savaş da ortaya çıkmıştır. Çin Halk Cumhuriyeti "Wang Dian Yiti Zhan" isimli Entegre İletişim Ağ Teknolojik harbiyle, resmi bilgi savaşı için stratejik bir yol belirlemiştir. Bilgisayar ağı üzerinden yapılacak bir saldırıya karşı ordu birimleri kurmuş, siber

[479] Kevin Ponniah ve Lazara Marinkovic, "The Night the US Bombed a Chinese Embassy," *BBC News*, 07.05.2019, E.T.: 16 Ağustos 2019, url: https://www.bbc.com/news/world-europe-48134881.
[480] Başaran, *Siber Savaş Cephesinden Notlar*, 38.
[481] Patty Davis, Kelly Wallace ve Lisa Rose Weaver, "U.S. Spy Plane, Chinese Fighter Collide," *CNN News*, 01.04.2001, E.T.: 16 Ağustos 2019, url: http://edition.cnn.com/2001/US/04/01/us.china.plane.02/index.html.
[482] Başaran, *Siber Savaş Cephesinden Notlar*, 38.
[483] Yılmaz ve Salcan, *Siber Uzayda Güvenlik ve Türkiye*, 46.
[484] Çakmak ve Altunok, *Suç, Terör ve Savaş Üçgeninde Siber Dünya*, 93.
[485] Keleştemur, *Siber İstihbarat*, 141.
[486] Keleştemur, *Siber İstihbarat,* 142.
[487] Paul J. Springer, *Cyber Warfare* (Amerika: ABC-CLIO, 2015), 41.

savaş kabiliyeti için adımlar atılmıştır.[488] Siber savaş günümüz yapısıyla ortaya çıkmıştır. Çin Halk Cumhuriyetiyse belirli çalışmalar için adımlar atmıştır.

2003 yılında siber güvenlikle ilgili büyük politikaları, ulusal stratejileri içeren, aktif savunma temelli "Belge 27 (Document 27)" yayımlanmıştır.[489] 2005 yılında, Çin Halk Cumhuriyeti hükümeti, "Ulusal Bilgi Geliştirme Stratejisi 2006-2020"yi duyurmuştur. Bu stratejiyle; bilgi teknolojisinde geliştirme ve derinleşme çalışmaları yapılmış, öncelik ulusal ekonomi ve toplumun bilgi düzeyinde gelişmeye verilmiştir. Altyapılar bilgi teknolojisiyle düzenlenip, küresel alanda bilgi üzerine gelişerek gücünü yükseltmeyi hedeflemiştir.[490] Çin Halk Cumhuriyeti, siber alanda önemli yeri olan; ekonomi, bilgi, altyapılar ve teknolojiye özel olarak yönelmiştir. Hedeflerini tamamladıklarında, Çin Halk Cumhuriyeti, siber alanda en güçlü devletlerden bir tanesi olacaktır. Ancak, Çin Halk Cumhuriyeti gelişmelere devam etmekte, siber alan da aynı hızda ilerlemektedir.

2009 yılında, GhostNet isimli siber saldırı, 103 devletin, özellikle devletlerarası ilişkilerde önemli makamları hedef seçilmiştir.[491] Saldırının kaynağı; Çin Halk Cumhuriyeti olarak belirlenmiş, ancak Çin Halk Cumhuriyet suçlamaları kabul etmemiştir.[492] Ancak sonradan Çin Halk Cumhuriyeti, saldırıların kaynağı olarak tespit edilmiştir. Çin Halk Cumhuriyeti'nin saldırıyı kabul etmemiş olması; bir yaptırım ya da saldırının önünü kesmiştir. Ancak, siber alanda, Çin Halk Cumhuriyeti'nin kaynakları üzerinden, başkalarının saldırı yapmış olma ihtimali de bulunmaktadır.

2011 yılında, yeniden bir belge yayımlanmıştır. Yayımlanan belge; ulusal güvenlik belgesidir. Çin Halk Cumhuriyeti hazırladığı belgeyle; büyüme ve gelişmeden kaynaklı bir tepki ve onun getireceği istikrarsızlığın oluşmasını istemediği için çalışmada bulunmuştur. "Çin'in Ulusal Güvenliği Belgesi (2011)" uluslararası sistemde fırsat ve tehditleri belirleyerek, bir strateji oluşturulmasından

[488] Çiftçi, *Her Yönüyle Siber Savaş*, 95.
[489] Mikk Raud, "China and Cyber: Attitudes, Strategies, Organisation," *NATO CCDCOE* (2016): 11, E.T.: 29 Eylül 2018, url: https://ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_CHINA_092016_FINAL.pdf.
[490] Cheng, *Cyber Dragon*, 6.
[491] Ron Deibert ve Rafal Rohozinski, *Tracking GhostNet: Investigating a Cyber Espionage Network* (ABD: Munk Centre International Studies, 2009), 40.
[492] Keleştemur, *Siber İstihbarat*, 146.

bahseder.[493] Fırsat ve tehditlerin belirlenmesi, bir devlet için en önemli stratejilerdendir. Fırsatları değerlendiren devlet, belirli konularda daha çabuk atağa geçebilir. Tehditlerin belirlenmesiyse; saldırılara karşı korunmada önemlidir. Ancak belirlenen her tehdidin çözümü aynı olmamaktadır. Bu sebeple; her an yeni gelişen tehditler, daha farklı ve büyük tehlikeler ortaya çıkarabilmektedir. 2011 yılında, "Night Dragon" isimli bir enerji raporu sızdırılmıştır. Bu raporla; Çin Halk Cumhuriyeti'nin istihbarat yaparak, enerji piyasasında başarı sağlamak amaçlı planları olduğu açığa çıkmıştır.[494] Çin Halk Cumhuriyeti siber istihbaratın avantajlarından faydalanarak eline geçen fırsatı değerlendirmiştir. Ancak, belirlediği stratejilerin ortaya çıkması, Çin Halk Cumhuriyeti için sisteminde açıklar olduğunu gösteren bir olay olmuştur.

2014 yılı Eylül ayında, siber anlamda askeri stratejilere ihtiyaç olduğu fark edilmiştir. Aralık ayında siber güvenlik için yeni güvenlik düzenlemeleri yapılmış, Mayıs 2015'de, siber güvenlikten söz edilen yeni Askeri Strateji yayımlanmıştır.[495] Çin Halk Cumhuriyeti'nin ulusal güvenlik belgeleri bir askeri strateji belgesine benzemektedir. Devlette güvenlik savunmaya bağlıdır, savunmaysa askeri sisteme dayanır.[496] Çin Halk Cumhuriyeti için; ulusal güvenlik, sert bir biçimde savunulup, korunması gerekir. Savunma yöntemlerinin sert olması; askeri alanın çeşitli sistemlere yayılmış olmasıdır.

Çin Halk Cumhuriyeti savunma amaçlı kanunlar belirlemiştir. "Çin Siber Güvenlik Kanunu" Çin Halk Cumhuriyeti'ndeki bilgi güvenliği ve siber alanda savunma amaçlı bilgi akışını kontrol etmeyi içerir.[497] 2017 yılında yürürlüğe giren kanun, ülkedeki bilginin dışarı çıkışında denetim ve kişisel bilgilerin korunması amacıyla yapılmıştır. Ulusal çıkar ya da kişilere zarar gelme ihtimali olan zamanlarda, Çin Siber Uzay İdaresi tarafından değerlendirilmeye alınacağı belirtilmiştir.[498] Düzenleme, siber alanda dolaşım, kullanım özgürlüğüne engel görünür, ancak, bireyleri koruma amaçlıdır. Uygulamanın olumlu ya da olumsuz olmasını değerlendirmek için hangi bakış açısında olunduğuna karar verilmelidir.

[493] Yalçın, *Ulusal Güvenlik Stratejisi*, 42-105.
[494] Keleştemur, *Siber İstihbarat*, 147.
[495] Greg Austin, "Middle Powers and Cyber-Enabled War: The Imperative of Collective Security," içinde *Securing Cyberspace,* edit. Cherian Samuel ve Munish Sharma (Yeni Delhi: Pentagon Press, 2016), 28.
[496] Yalçın, *Ulusal Güvenlik Stratejisi*, 104.
[497] Cheng, *Cyber Dragon*, 66.
[498] "Çin'in Siber Güvenlik Kanunu Yürürlükte," *Milliyet Teknoloji*, 02.06.2017, E.T.: 29 Eylül 2018, url: http://www.milliyet.com.tr/cin-in-siber-guvenlik-kanunu-teknoloji-haber-2461609/.

Yapılan çalışma, ulusal çıkarları korumak amaçlıdır. Aynı zamanda bilginin dışarı çıkmaması için yapılan politikalar önemlidir.

2019 yılında yapılan politikalar ve çalışmalar, önceki politikalardaki gibi dışarıya kapalı bir biçimde olmuştur. Ancak kendini korumak amaçlıdır. Aynı sene içerisinde yapılan bir habere göre; Çin Halk Cumhuriyeti, askeri sistemlerinden Windows programını kaldırıp, kendi geliştirecekleri bir sistem üzerinden çalışmaları sürdüreceklerdir. ABD bağlantılı olan Windows'un, günümüzde var olan siber saldırılardan dolayı dezavantaj oluşturacağını düşünmüşlerdir. Bu sebeple; kendi birimlerine bağlı bir askeri sistem oluşturacaklardır.[499]

Geçmişten günümüze; Çin Halk Cumhuriyeti'nin politik, askeri, ekonomik, bilimsel çalışmalarının altındaki düşünceler, belirli bir felsefeye dayanmaktadır. En önemli örnekse; Sun Tzu'nun Savaş Sanatı isimli askeri stratejisidir.[500] Savaş Sanatı'nda; belirli tehditler, savaşlar, savunma üzerinde uygulanabilecek taktikler 13 bölüm şeklinde verilmiştir.[501] Genel olarak; Çin Halk Cumhuriyeti'nde stratejiler, askeri stratejilere yakındır. Sun Tzu'nun yazmış olduğu kitap; askeri stratejinin ilk çıkış noktalarından olan, savaşın kazanılmasında izlenecek bir rehber niteliğindedir. Günümüzde hâlâ önemli kaynaklardan biridir. Birçok stratejinin ortaya çıkışında bu düşünceler vardır. Belirli düzenlemelerle stratejilerin izlenmesi önemlidir. Ancak, kurumların önemi daha büyüktür. Bir strateji ya da düzenleme, resmi kurumlar üzerinden hareket edilerek uygulanmaktadır. Çin Halk Cumhuriyeti'nde siber alan için ayrı kurumlar bulunmaktadır. Siber çalışmalar yürüten birimlerinden kısaca bahsetmek gerekir.

Çin Halk Kurtuluş Ordusu (PLA- The Chinese People's Liberation Army); 3. Ordu, 2. Büro, Birim 61398 Şangay Grubu olarak da söz edilen ordusudur.[502] Bu birim; pek çok bilgiyi toplamayı başarmıştır. Genelkurmay 3. Dairesi'nde, siber anlamda, yabancı askeri güçlerin iletişiminde kontrol, savunma, istihbarat faaliyetlerinin yapıldığı birim olduğu bilinmektedir.[503] Ancak, Çin Halk

[499] "Çin Ordusu Bilgisayarlarından Windows'u Kaldırıyor," *Hürriyet Haber*, 29.05.2019, E.T: 17 Ağustos 2019, url: http://www.hurriyet.com.tr/teknoloji/cin-ordusu-bilgisayarlarindan-windowsu-kaldiriyor-41229612.
[500] Kenneth Geers, *Strategic Cyber Security* (Estonya: CCDCOE Yayınları, Haziran 2011), 96, E.T.: 28 Haziran 2018, url: https://ccdcoe.org/publications/books/Strategic_Cyber_Security_K_Geers.PDF.
[501] Tzu, *Savaş Sanatı,* 1-43.
[502] Singer ve Friedman, *Siber Güvenlik ve Siber Savaş,*192.
[503] Keleştemur, *Siber İstihbarat*, 186.

Cumhuriyeti'nin iletişim ve ses ağları güvenliğinden sorumlu başka bir birim vardır.[504] Genelkurmay 4. Dairesi'nde; elektronik istihbarat çalışmaları yapılmaktadır. Teknik keşif büroları şeklinde söz edilen, sinyal istihbaratı yaparak stratejik, taktik hedeflerle görevlerini gerçekleştiren bürolar şeklindedir.[505]

Çin Halk Cumhuriyeti bünyesinde 'Mavi Ordu' isimli siber savaş birimi bulunduğunu 2011 yılında kabul edilmiştir. Çin Ordusu Bilgi Harbi Milis Üniteleri, 2002 yılı itibariyle, ticari ve akademik çevreden oluşan personellerle, ordu ve sivil güvenlik faaliyetleri arasında koordinatörlük görevi yapmaktadır.[506] Kamu Güvenliği Bakanlığı; siber suçlar üzerine araştırma, geliştirme, kritik altyapıları koruma ve sağlama görevleri yapmaktadır. Ayrıca Great Firewall of China buraya bağlıdır.[507]

Çin Halk Cumhuriyeti; birçok alt birimi, kurum ve kuruluş içerisinde belirli yapılara ayrılmıştır. Çin Halk Cumhuriyeti, strateji ve kurumların çalışmalarıyla, günümüzde, siber anlamda belirli politikalar izlemektedir. Çalışmalarında Çin Halk Cumhuriyeti, diğer devletlere göre farklı bir sistemle ilerlemiştir. Özellikle savunmada, askeri bir sistem benimsemiştir. Bu çalışmalar, siber alandan gelecek tehditler üzerine ciddi çalışmalardır. Ancak, Çin Halk Cumhuriyeti, günümüzde dışarıya gösterilmeden, daha detaylı ve farklı birimler üzerinden yeni çalışmalara devam ediyor olabilir.

Dışarıya kapalı olan Çin Halk Cumhuriyeti, sınırlı kaynaklar bulunmasına rağmen, siber anlamda pek çok çalışma yaptığı bilinmektedir. Ekonomik olarak gelişmeler gösteren Çin Halk Cumhuriyeti, yatırımını teknolojik anlamda siber alan üzerinden yapmıştır. Teknolojinin ekonomiyle bağlantısının farkında olmaları, bu yönde çalışmalar yapmalarında etkili olmuştur. Gelişmelerini sürdüren Çin Halk Cumhuriyeti, hedef ülkelerden biridir. Siber alan tehditlerinin farkında olarak yapılan çalışmalar, iç ve dış tehditlerin ortaya çıkmasının önüne geçmek amaçlı yapılmıştır. Çin Halk Cumhuriyeti, yaşadığı saldırılar sonucunda belirli politikalar ve savunma yöntemleri geliştirmiştir. Ayrıca, ileride oluşabilecek tehditlere karşı, önlem amaçlı çalışmalar yapmıştır. Özellikle kendi sistemlerinde, askeri yapının önemli olması, bu alandaki çalışmalara daha çok eğilmelerine sebep olmuştur. Bu alanı koruyabilmek için, bilgisayar sistemlerine

[504] Çiftçi, *Her Yönüyle Siber Savaş*, 46.
[505] Keleştemur, *Siber İstihbarat*, 186.
[506] Çiftçi, *Her Yönüyle Siber Savaş*, 46-48.
[507] Raud, "China and Cyber: Attitudes, Strategies, Organisation," 17.

kadar önlem alma ihtiyacı duyulmuştur. Özellikle askeri alana gelebilecek bir siber tehdit karşısında Çin Halk Cumhuriyeti, saldırıya göre, daha sert cevap verebilecek bir yapıdadır. Ancak, sonucunun sıcak bir savaşa dönme ihtimalini taşımaktadır. Bu ihtimal, uluslararası sistemde tehlike oluşturabilecek güçlerden biri olmasından dolayı problem oluşturacaktır. Bu sebeple; günümüzde daha dikkatli saldırılar yapıldığı bilinmektedir. Ancak, bu saldırılar hep aynı şekilde kalmayacaktır. Ekonomi, teknoloji gibi güç olarak önemli faktörlere erişimle, ilerleyen süreçlerde dengelerin değişmesi farklı sonuçlara yol açabilir. Siber alandaki saldırılarsa biriken süreçle, ayrı bir tetikleyici etken olabilir. Çin Halk Cumhuriyeti gibi tehdit altında olan başka devletler vardır. O devletlerin belirlemiş oldukları politikalar ve politika çalışmaları vardır. Bunlardan biri; özellikle Soğuk Savaş sonrası dönemde ilgiyi üzerine çeken, günümüz ismiyle Rusya Federasyonu'dur. Rusya Federasyonu siber anlamda önemli, kendini geliştiren ülkelerden biridir. Rusya Federasyonu'nun yapmış olduğu çalışmaları ayrıca incelemek gerekir.

2.1.3. Rusya Federasyonu

Rusya Federasyonu, siber alanda, Çin Halk Cumhuriyeti ve ABD'yle beraber en güçlü devletlerden biri olup, bu nedenle çalışmalarına ayrı bir önem vermektedir.[508] Eski bir tarihi olmasına rağmen birçok dönüşüm geçirmiş, günümüzdeki ismiyle Rusya Federasyonu olmuştur. Resmi belgelerde kuruluş tarihi; 25 Aralık 1991'dir. Mihail Gorbaçov'un istifası sonrası, Boris Yeltsin'in gelişiyle, günümüz sistemine başlamıştır.[509] Kuruluş yılına bakıldığında yeni bir devlet gibi görünmektedir. Ancak, Rusya Federasyonu'nun temelleri çok eski ve köklü bir geçmişe dayanır. Günümüzdeki adıyla Rusya Federasyonu, yeni bir sistemle varlığını sürdürmekte, geçmişin birikimiyle pek çok konuda çalışmalar yapmaktadır.

Rusya Federasyonu, kuruluş yılı itibariyle, siber alanın gelişmelerin arttığı döneme denk gelmiştir. Siber olayların dikkat çekmeye, gelişmeye başladığı dönemlerde, Rusya Federasyonu belirli olaylar içerisinde bulunmuştur. Kendi güvenliğiyle savunmasını; belirli stratejiler, uluslararası alandaki olaylar ve kendi

[508] Çıtak, *Güvenlik ve İstihbarat*, 247.

[509] Remzi Bulut, "SSCB'nin Dağılması ve Rusya Federasyonu'nun Serbest Piyasaya Geçişi," *Mehmet Akif Ersoy Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi* Cilt: 1-Sayı: 2 (2014): 13, E.T.: 30 Eylül 2018, url: http://dergipark.gov.tr/download/article-file/231924.

yaşadığı problemler üzerinden oluşturmuştur. Rusya Federasyonu'nda yaşanan önemli bazı olay ve politikalardan, siber alandaki gelişmelerin anlaşılması için bahsetmek gerekir.

Siber olaylardan önemli bir tanesi 1994 yılında yaşanmıştır. 11 Aralık 1994 yılında, Rus birlikleri, hava ve karadan saldırılara başlamış, Çeçenistan'ın başkentine girmiştir. Direnişin kısa süreceği düşünülmüştür. Ancak tam tersi olunca, Soğuk Savaş sonrası dönemde ilk askeri anlamda çatışma yaşanmıştır.[510] Askeri çatışmanın beraberinde, Çeçenler medyayı kullanarak, bilgi savaşının ilk örneklerini, propaganda ve bilgi üzerinden yapmışlardır. Bu da çatışmanın siber alan için önemini göstermektedir. Çünkü çatışma internet ortamına yansımıştır.[511] Soğuk Savaş sonrası dönemde bu olay, teknolojik olarak değişimleri göstermektedir. Aynı zamanda olayın internet ortamına taşınması, medyanın yardımıyla savaşın farklı bir boyuta geçmesini sağlamıştır. Siber alan üzerinden, bilgi kullanılarak yapılan savaşlardan söz edildiğinde ilk akla gelen bu olaydır. Propaganda yönteminden yararlanılarak yapılmıştır.

Siber alandaki tehditlerin görülmesiyle Rusya Federasyonu belirli düzenlemelere gitmiştir. 5 Haziran 1996 yılında, Rusya Federasyonu Ceza Kanunu- 28. Bölümde[512], bilgi teknolojileri üzerinden işlenen suçlara düzenlemeler yapılmıştır. Bilişim suçları üzerine yasal düzenlemeyle, siber alandaki suçların takibi amaçlı çalışmalar yapan öncü devletlerden biri Rusya Federasyonu'dur.[513] Siber alan çalışmalarına verdiği önemle Rusya Federasyonu, diğer aktörlerin dikkatini çekmiştir.

Kanun çalışmaları dışında, alanla alakalı birimler kurulmuştur. 1996 yılı sonrası düzenlemeler yapılmış, Rusya Federasyonu'nda "R" bölümü açılmıştır. Ancak 7 Ocak 1998 yılında bölümün adı değiştirilerek "İleri Teknoloji ile Mücadele Bölümü" olmuştur. 1999 yılında, bölgesel birimler tamamlanmıştır. 2002 yılındaysa bu bölüme son verilmesi kararlaştırılmıştır. Bu bölümündeki her şey İçişleri Bakanlığı Özel Teknik Birimine geçmiş, 2009 yılında "K" birimi olarak adlandırılmıştır.[514] Birimler, 1991 sonrası devletin kuruluşuyla hızlı bir

[510] John Russell, *Chechnya – Russia's 'War on Terror'* (New York: Routledge, 2007), 62-63.
[511] Bıçakçı, *21. Yüzyılda Siber Güvenlik*, 30.
[512] "The Criminal Code of The Russian Federation," World Intellectual Property Organization, E.T.: 18 Ağustos 2019, url: https://www.wipo.int/edocs/lexdocs/laws/en/ru/ru006en.pdf.
[513] Çakmak ve Altunok, *Suç, Terör ve Savaş Üçgeninde Siber Dünya*, 118.
[514] Çakmak ve Altunok, *Suç, Terör ve Savaş Üçgeninde Siber Dünya*, 119.

biçimde oluşturulmuştur. Yeni kurulan birimler, işlevlerine ve ihtiyaca göre değişimler göstermiştir. İlerleyen dönemlerde, bazı düzenlemelerde değişiklikler yapılmıştır. Siber alanla alakalı çalışmalaraysa devam edilmiştir.

2000'li yıllarda daha kapsamlı çalışmalar yapılmıştır. 10 Ocak 2000 yılında, "Ulusal Güvenlik Strateji Belgesi/Güvenlik Konsepti (National Security Concept of Russian Federation)[515]" ile Rusya Federasyonu kendi ulusuna gelebilecek tehditleri güvenlik kapsamında tek tek ele almıştır. Güvenlik kapsamlarını; uluslararası, iç siyasi, askeri, sınır, çevre ve haberleşme olmak üzere altı ana alana bölmüştür.[516] Resmi belgede ilk defa bilgi güvenliği kavramı kullanılmıştır. Genel anlamda; bilgi güvenliği, tehditlerin varlığı, bunlara karşı tedbirlerin alınması gerektiğinden bahsedilmiştir.[517] Savunma Bakanlığı'nın Elektronik Harp Birliğinde, bilgi harekâtı üzerine savunma ve saldırıya yönelik çalışmalar yapılmıştır. 2001 yılı ve sonrasında siber alan üzerinde eğitim veren enstitü ve üniversiteler açılmıştır.[518] Rusya Federasyonu'nun siber anlamda önemli olmasının sebeplerinden biri; kendi içerisinde, 2003 yılında kurulmuş olan, Özel İletişim ve Bilişim Servisi'ne bağlı dünyanın en büyük hacker okuludur.[519] Siber alanda eğitime erken dönemlerde önem verilmesi, Rusya Federasyonu'nun, bu alan çalışmalarını daha ciddi derecede yürüttüğünü göstermektedir. Aynı tarihlerde, resmi belgeler ve savunmaya da ayrı bir önem verilmiştir. Eğitim açısından, üniversitelerde eğitim ve bir hacker okulunun bulunması, Rusya Federasyonu'nun siber alandaki çalışmalarında, bazı konularda, farklı bir yol izlediğini gösterir. Günümüzde, siber alan üzerine üniversite eğitimi birçok ülkede vardır. Rusya Federasyonu'nun farkı; kendi içerisinde bir hacker okulu bulundurmasıdır. Bazı devletler, yakın dönemlerde siber alanı eğitim kurumlarına eklemiştir, ancak Rusya Federasyonu, daha erken dönemlerde bunu yapmıştır.

Siber alanda çalışmaların devam ettiği süreçte, Rusya Federasyonu ve Estonya Cumhuriyeti arasında önemli bir olay yaşanmıştır. 27 Nisan 2007 yılında,

---

[515] The Ministry of Foreign Affairs of the Russian Federation, *National Security Concept of the Russian Federation* (Rusya: Ocak 2000), E.T.: 30 Eylül 2018, url: http://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/589768.

[516] Yalçın, *Ulusal Güvenlik Stratejisi*, 170.

[517] Darıcılı, *Siber Uzay ve Siber Güvenlik*, 144.

[518] Çiftçi, *Her Yönüyle Siber Savaş*, 50.

[519] KURGAN, *Siber Mücadeleye Giriş*, 154.

Estonya'da, Kızıl Ordu Anıtı'nın bronz olması sebebiyle adını buradan alan, Bronz Gecesi (Bronze Night) olayı patlak vermiştir.[520] Estonya Cumhuriyeti, Tallinn'in merkezinde bulunan Kızıl Ordu Anıtı'nı, mezarlığa taşımak istemesi sonucu ayaklanmalar yaşanmıştır. Şiddetli tepkiler beraberinde Estonya hükümeti ve altyapıları ciddi bir internet saldırısına maruz kalmıştır.[521] Rusya Federasyonu ve Estonya Cumhuriyeti arasındaki bu anlaşmazlık, siber alanda önemli bir yer tutmaktadır. Olayın siber alandaki önemiyse; ilk defa bir devlete üç hafta boyunca, çok taraflı, sistemli siber saldırılar gerçekleşmiştir.[522] Aradan uzun süre geçmeden, başka bir olay yaşanmıştır.

2008 yılı Temmuz ayında, Güney Osetya'da asiler, Gürcistan'a bağlı köylere saldırmıştır. Gürcistan buna karşılık vermiş, Ağustos ayında Rus ordusu harekete geçmiştir.[523] 8 Ağustos'ta, Rus savaş uçağının, Güney Osetya'dan Gürcistan hava sahasına girmesiyle Rusya Federasyonu ve Gürcistan Cumhuriyeti arasında yaşanan anlaşmazlıklar artmıştır. Aynı gün, Gürcistan hükümeti resmi sayfalarına, siber saldırı yapılarak zarar verilmesi şeklinde ilerlemiştir.[524] Gürcistan Cumhuriyeti'nin kendi içerisindeki hackerlar, Rusya Federasyonu ve Güney Osetya hükümet sitelerini hedef almakla suçlanmıştır.[525] Ayrılıkçı gruplar yüzünden, Gürcistan kuvvetleri, olayın sıcak çatışmaya dönüşmesine sebep olmuştur. Rus güçlerin karşılık vermesi, hem siber hem sıcak çatışmaya, yani; hibrit bir savaşa dönüştürmüştür.[526] Savaş, fiziksel ve siber bir savaşın aynı anda görüldüğü biçimi almıştır. Siber savaş ve fiziksel savaşın beraber yürütüldüğü, günümüze yakın önemli örneklerden biri olmuştur.

18 Ocak 2009 tarihinde, Kırgızistan Cumhuriyeti'ne yapılan saldırılarla tüm internet siteleri, internet üzerinden yapılabilecek haberleşmeler kesilmiştir. Saldırıyı yapan Rusya Federasyonu; Manas'taki ABD askeri üssünün kapatılmasını hedeflemiştir.[527] Aynı yıl Haziran ayında Rusya Federasyonu strateji belgesi yayımlamıştır. Belge; "2020'ye Doğru Rus Ulusal Güvenlik

[520] Clarke ve Knake, *Siber Savaş,* 13.
[521] Ehala, "The Bronze Soldier: Identity Threat and Maintenance in Estonia," 143.
[522] Bayraktar, *Siber Savaş*, 156.
[523] Clarke ve Knake, *Siber Savaş,* 17.
[524] Johanna Popjanevski, "From Sukhumi to Tskhinvali: The Path to War in Georgia," içinde *The Guns of August 2008, ed.* Svante E. Cornell ve S. Frederick Starr (New York: M.E. Sharpe, 2009), 152.
[525] Çakmak ve Altunok, *Suç, Terör ve Savaş Üçgeninde Siber Dünya*, 47.
[526] KURGAN, *Siber Mücadeleye Giriş*, 184.
[527] Darıcılı, *Siber Uzay ve Siber Güvenlik*, 215.

Stratejisi (Russia's National Security Strategy to 2020) Belgesi"'dir.[528] Burada Rusya Federasyonu; büyüme ve istikrardan söz edip, tehdidi istikrarsızlık şeklinde tanımlamıştır. Dokuz ana başlık içeren belgede; devlet ve kamunun güvenliği, ulusal savunma, Rus halkının kaliteli yaşamalarını sağlamak, stratejik istikrar, çevre ve ekoloji, bilim, eğitim ve teknoloji, ekonomik büyüme, sağlık hizmetleri, kültür üzerine odaklanılmıştır.[529] Bu yıl içerisinde, 149 sayılı Federal Kanun üzerinde değişiklikler yapılmıştır. Bu değişiklikler, internete kayıt yapılırken kimlik numarası kullanımı, bir soruşturma ihtimalinde her türlü verinin yetkililere teslim edilmesi şeklinde olmuştur.[530] Bu belgede; siber anlamda tehditler, gelişmelerin kültürel, ekonomik, toplumsal yansımaları, yapılması gereken atılımlar gibi konulara yer verilmiştir.[531] Belgeye bakıldığında; internet kullanımının özgür, ancak şartların neredeyse Çin Halk Cumhuriyeti'ndeki gibi, hükümetin elinde olduğunu göstermektedir. Belgede, siber anlamda bazı konularda yapılması gerekenleri ayrıca açıklamışlardır.

2011 yılında yayımlanan "Bilgi Çağında Rus Silahlı Kuvvetleri'nin Faaliyetlerine İlişkin Kavramsal Görüşler (Conceptual Views Regarding the Activities of the Armed Forces of the Russian Federation in the Information Space)"[532]adlı belge, siber uzay üzerine, Rusya Federasyonu'nda yayımlanmış açıklayıcı ilk belgedir. Bilgi merkezli siber faaliyetler, daha çok operasyonel mantık içerisinde, çatışma üzerinden değerlendirilmiştir. Bir diğer önemli nokta; siber uzay üzerine, uluslararası iş birliğinin geliştirilmesine vurgu yapılmıştır.[533] Belge; siber uzay üzerine, Rusya Federasyonu'nun yayımlamış olduğu ilk açıklayıcı belge olma özelliğini taşır. Ayrıca, belgede, yapılabilecek faaliyetler için iş birliği önerisinde bulunmuştur. Uluslararası alanda bu özellikleri sebebiyle önemlidir.

2013 yılı Haziran ayında yapılan G-8 toplantısı sırasında; Rusya Federasyonu ve ABD, siber anlamda güven kurmak amaçlı antlaşma

[528] Keir Giles, "Russia's National Security Strategy to 2020," *Zürih Federal Teknoloji Enstitüsü* (2009) E.T.: 17 Ağustos 2019, url: https://www.files.ethz.ch/isn/154909/RusNatSecStrategyto2020.pdf.
[529] Yalçın, *Ulusal Güvenlik Stratejisi*, 175-296.
[530] Çiftçi, *Her Yönüyle Siber Savaş*, 98.
[531] Darıcılı, *Siber Uzay ve Siber Güvenlik*, 147-148.
[532] CCDCOE, *Conceptual Views Regarding the Activities of the Armed Forces of the Russian Federation in the Information Space* (Rusya: 2011), E.T.: 30 Eylül 2018, url: http://www.ccdcoe.org/strategies/Russian_Federation_unofficial_translation.pdf.
[533] Darıcılı, *Siber Uzay ve Siber Güvenlik*, 149-150.

imzaladıklarını duyurmuştur. Bu antlaşmada; iki devlet arasında, tehditler üzerine birlikte çalışma grubu kurulması, iş birliği gibi konulardan bahsedilmiştir.[534] 2011 yılında yayımlanan belgede hedeflenen siber anlamda uluslararası iş birliğini, Rusya Federasyonu, 2013 yılındaki G-8 toplantısında gerçekleştirdiğini göstermiştir.

2014 yılında, Rusya Federasyonu ve Ukrayna arasında, askeri ve politik gerginlikler yaşanmıştır.[535] Gerginlikler aynı zamanda, siber uzayda da kendini göstermiştir. Kiev'deki açık hava reklamlarında; dijital saldırılarla, Rusya lehine yayınlar yapılmış, Kievlilere psikolojik saldırı uygulanarak, silah olarak siber alan kullanılmıştır.[536] Siber alan farklı amaçlarla, çeşitli şekillerde kullanılmaya başlanmıştır. Ukrayna ile yaşanan olaylar, siber alan için ayrı bir öneme sahiptir. Ancak, siber saldırılar ve gerginlikler sadece Ukrayna'yla sınırlı kalmamıştır. Gerginlikler, Rusya Federasyonu'nun yeni çalışmalar yapmasını gerektirmiştir. 2015 yılında, farklı devletlerle antlaşmalar yapmaya devam etmiştir.

30 Nisan 2015 yılında, Çin Halk Cumhuriyeti ve Rusya Federasyonu "Siber Pakt" isimli bir antlaşma yapmıştır. İki ülke, siber tehditlerin tanımlamasını yapmış, bilgi paylaşımıyla iş birliğinden söz etmiştir. Uluslararası platformlarda, norm ve yasalarla, belirli ölçüde anlaşılmıştır.[537] Rusya Federasyonu; ABD ve Çin Halk Cumhuriyeti ile siber alan üzerine iş birliği hakkında görüşüp, belirli çalışmalar için adımlar atmıştır. Siber alanda önemli tehditlerden görülen üç devletin yapmış olduğu çalışmalar dışında, iş birliği için adımlar attığı görülmektedir. Ancak, iş birliği çalışmaları yapılırken, birbirlerine karşı ayrı çalışmalar yürüttükleri bilinmektedir. Diğer devletlerle siber alanda adımlar atılırken, Ukrayna ile yaşanan olaylar durulmamıştır. Aynı yılın Aralık ayında, Rus saldırı gruplarından biri olan Sandworm, Ukrayna'ya saldırmıştır. Elektrik şebekesine yapılan saldırılarla elektrik kesintisine yol açmıştır.[538] 23 Aralık 2015'de yaşanan bu olay, elektrik dağıtım merkezinin hacklenmesi sonucu ortaya çıkmıştır. Elektrik dağıtım biriminin kapatılması sonrasında 250.000 civarı

[534] "G8 Summit," President of Russia, E.T.: 17 Ağustos 2019, url: http://en.kremlin.ru/events/president/news/18358.
[535] "Russian 'Invasion' of Crimea Fuels Fear of Ukraine Conflict," *The Guardian*, 28.02.2014, E.T.: 17 Ağustos 2019, url: https://www.theguardian.com/world/2014/feb/28/russia-crimea-white-house.
[536] KURGAN, *Siber Mücadeleye Giriş*, 164.
[537] Çiftçi, *Her Yönüyle Siber Savaş*, 137.
[538] Huzeyfe Önal, " Siber Savaşlarda En Kritik Bileşen Siber İstihbarat," *Uluslararası Siber Güvenlik Federasyonu* 2 (2017): 44.

Ukraynalının elektriği kesilmiştir.[539] Olay, bir siber saldırının ciddi boyutlarda kesinti ve etki bıraktığının en büyük göstergesidir. Günümüzde bir elektrik kesintisi, birçok alanda problemler oluşturmaktadır. Özellikle, uzun süreli kesintiler, devletin işleyişinde aksamalara sebep olacak boyuta kadar gelebilmektedir. Ciddi sayıda Ukraynalının elektriksiz kalmasıysa dikkat çekicidir. Olaylarla beraber Rusya Federasyonu, güvenlik amaçlı bir doktrin hazırlamıştır. 6 Aralık 2016 yılında, "Rusya Federasyonu Enformasyon Güvenliği Doktrini (Doctrine of Information Security of the Russian Federation)"[540] ile bilgi güvenliği, siber savunma üzerine ulusal çıkarlar belirlenmiş, oluşabilecek siber tehditlerden söz edilmiştir.[541]

2019 yılı Haziran ayında Rusya Federasyonu, ekonomisindeki önemli noktaların siber saldırıya uğradığından söz etmiş, ABD içerisinde saldırı yapanların, başkandan habersiz saldırı düzenliyor olması dahi, siber savaş için bir işaret olduğundan da bahsetmiştir.[542] Aynı süreçte, başka çıkan bir haberde; Rusya Federasyonu'na yapılan saldırıların çoğu, AB ve ABD sunucularından çıktığı belirtilmiştir. Yapılan saldırıların amacınınsa; savunma ve enerji sanayinde, nükleer ve roket üretimi bilgilerinin ele geçirilmesi olduğu ortaya çıkmıştır.[543]

Rusya Federasyonu 2000 ve 2009 yılında yayımlamış olduğu önemli iki belgede; siyasi, ekonomik, sistemik düzensizlikleri tehdit olarak görmüştür. Buna karşın, gücü merkezileştirme, biriktirme ve önleyici tedbirler almayı önermiştir. 2000 ve 2009 yılındaki belgelerde; Rusya Federasyonu, kendi kontrolü dışında oluşabilecekler dönüşümlerden endişe duymuş, istikrar için belirli yöntemler önemiştir. İçerik açısından; her alanı güvenliğin alanına dâhil eden, birbirine çok yakın olan iki belge, devlet otoritesini niteleyen bir yapıdadır.[544] 2010 yılı sonrasındaysa işbirliklerine yönelik çalışmalar yapmış, ancak siber alanda farklı adımlar atmıştır. Hem ABD hem Çin Halk Cumhuriyeti ile belirli konularda

[539] Başaran, *Siber Kıyamet*, 17.
[540] The Ministry of Foreign Affairs of the Russian Federation, *Doctrine of Information Security of the Russian Federation* (Rusya: Aralık 2016), E.T.: 30 Eylül 2018, url: http://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/2563163.
[541] Darıcılı, *Siber Uzay ve Siber Güvenlik*, 161-162.
[542] "Rusya'dan ABD'ye Siber Savaş Uyarısı," *Hürriyet Haber,* 17.06.2019, E.T.: 17 Ağustos 2019, url: http://www.hurriyet.com.tr/dunya/rusyadan-abdye-siber-savas-uyarisi-41246672.
[543] "Rusya'ya Yönelik Siber Saldırılar ABD ve Avrupa'dan Yayılıyor," *Hürriyet Haber,* 28.06.2019, E.T.: 17 Ağustos 2019, url: http://www.hurriyet.com.tr/teknoloji/rusyaya-yonelik-siber-saldirilar-abd-ve-avrupadan-yayiliyor-41257587.
[544] Yalçın, *Ulusal Güvenlik Stratejisi*, 17-99.

anlaşan Rusya Federasyonu, özellikle ABD ile bu alanda karşılıklı saldırılar içerisindedir. Saldırıların amaçları hem politik hem de devlet düzenini bozabilecek nitelikte büyük olmuştur. Sonuçları henüz ortaya çıkmamış olsa da, tehditler gün geçtikçe daha artmaktadır.

Tehdit ve saldırıların artmasıyla Rusya Federasyonu çeşitli belgeler oluşturmuştur. Belgelerle iş birliği taraftarı olan Rusya Federasyonu, amacının; gücünü korum, istikrarı sağlama isteği olduğunu göstermiştir. İstikrar ve gücü korumak için, bunu sağlaması gereken kurum ve kuruluşlara ihtiyaç duyulur. Siber alanda görev yapan resmi kurum ve kuruluşların önemli olanlarından söz etmek gerekir.

Federal Güvenlik Servisi; kritik altyapıların güvenliğinden sorumludur. Aynı zamanda ulusal güvenlik, terörle mücadele, devlet sınırlarının korunması, bilgi güvenliği bu birim tarafından sağlanır.[545] Federal Güvenlik Teşkilatı; devlet birimleri içerisinde hem iletişimin güvenliğini hem devlet yapılarını, dışarıdan gelebilecek zararlara karşı korumakla görevlidir. İnternet üzerinden gelebilecek tehditler için, Federal Güvenlik Servisine bağlı; Bilgi Güvenliği Merkezi SORM adlı bir internet izleme sistemiyle faaliyet yürütülür. İletişim Elektronik Gözleme Merkezi sayesinde; elektronik ortamdaki iletişimin, deşifre ve dinlenmesi yapılır. Bu birim; SSCB döneminde var olan KGB (Devlet Güvenlik Komitesi)'nin devamıdır.[546]

İçişleri Bakanlığı içerisindeki Siber Suçlar İdaresi; suçlarla mücadeleden sorumludur.[547] 5. Boyut Siber Ordu; Rusya Federasyonu Savunma Bakanlığı altındaki, Elektronik Harp Birlikleri ve eğitim almış siber korsanların, profesyonel şekilde yetiştirilerek bir araya getirilmesiyle oluşturulur. [548] Siber çalışmaların yapıldığı birimdir. Çalışmalar gelişerek devam etmektedir. Birimler, Rusya Federasyonu'nun siber alan çalışmalarını daha açık bir biçimde ortaya koymaktadır. Rusya Federasyonu planlı bir ilerleme göstermeye çalışmaktadır. Ancak, siber alanın kendi yapısı değişken bir yapıdadır. Diğer devletlerin

[545] "Federal Security Service," The Russian Government, E.T.: 17 Ağustos 2019, url: http://government.ru/en/department/113/.
[546] Hasan Çiftçi, *Her Yönüyle Siber Savaş* (Ankara: TÜBİTAK Popüler Bilim Kitapları, Temmuz 2017), 50-98.
[547] Hasan Çiftçi, *Her Yönüyle Siber Savaş* (Ankara: TÜBİTAK Popüler Bilim Kitapları, Temmuz 2017), 51.
[548] Atalay Keleştemur, *Siber İstihbarat* (İstanbul: Level Kitap, Ağustos 2015), 188.

politikalarındaki değişkenlik de etkili olmakta, yapılan politika ve çalışmaları kısa sürede daha az etkili kılmaktadır.

Genel anlamda; Rusya Federasyonu, kurulduğu yıldan itibaren, siber anlamda önemli çalışmalar içerisinde bulunmuştur. Yapılan çalışmalar, yaşanan çatışmalarla teknolojinin ilerlemesi, stratejilerde dönüşüme sebep olmuştur. Rusya Federasyonu, siber alanda ciddi tehditlerden biridir. İzlenen yöntemler ve politikalarla, siber alanda güçlü ülkelerden biri olan Rusya Federasyonu, bazı ülkeler için iyi bir müttefik, bazıları için önemli ölçüde tehdit olarak görülmüştür. Hem çatışmacı hem işbirlikçi bir yol izleyen Rusya Federasyonu, kendine özel stratejiler yürütmüştür. Ancak, özellikle ABD ile siber alanda da sürekli karşı karşıya gelmeye başlamıştır. İki devlet siber alanda birbirlerine tehdit oluşturmakta, siber alanla beraber belirli dönemlerde politik gerginliği arttırmaktadır. Gerginliklerin, siber alandan farklı boyutlara geçme ihtimali, Soğuk Savaş Dönemine benzer görünmektedir. Ancak, sonuçlarının günümüz imkânlarıyla ne kadar ileri gidebileceği henüz öngörülememektedir. Siber alanda ABD, Çin Halk Cumhuriyeti ve Rusya Federasyonu gibi başka devletler, olası bir çatışma ya da güvenlik için ayrıca çalışmalar yürütmüştür. Teknolojik çalışmalardan söz edildiğinde, ilk akla gelen ülkelerden biri tanesi; Federal Almanya Cumhuriyeti'dir. Almanya birçok alanda kendini gösteren ülkelerden biri olarak; siber alanda belirli çalışmalarda bulunmuştur. Çalışmaların amaçlarını anlamak içinse, izlediği bazı yöntem ve olaylardan söz etmek gerekir.

2.1.4. Federal Almanya Cumhuriyeti

Rusya Federasyonu, ABD ve Çin Halk Cumhuriyeti gibi, Federal Almanya Cumhuriyeti siber alanda önemli çalışmalarda bulunan devletlerdendir. Federal Almanya Cumhuriyeti, çeşitli alanlarda, önemli çalışmalar yaptığı bilinen devletlerdendir. Siber alanda da benzer çalışmalar yapmıştır. Siber güvenlik alanında tehlikelere karşı önlemler alan devletlerden biri; Federal Almanya Cumhuriyetidir. Siber anlamda atılan adımlar Birinci Dünya Savaşına kadar gitmektedir. Federal Almanya Cumhuriyeti de, Rusya Federasyonu gibi uzun bir geçmişe sahip devletlerdendir. Eski devletlerden biri olmakla beraber, son haliyle 3 Ekim 1990 tarihi itibariyle Federal Almanya Cumhuriyeti şeklinde kurulmuş, resmi olarak bu adı almıştır. Ancak, Rusya Federasyonu'ndan daha farklı bir yapıda olduğu bilinmektedir. Birinci Dünya Savaşı döneminde Federal Almanya

Cumhuriyetine dönüşmemiş ancak, günümüzdeki çalışmalar o dönemde başlamıştır.

Birinci Dünya Savaşı döneminde, Almanların yaptığı çalışmalardan söz etmek, günümüz için açıklayıcı olacaktır. Birinci Dünya Savaşı döneminde, Almanlar için önemli zaferlerden biri; Tanenberg Zaferidir. Bu zafer, haberleşme istihbaratıyla, Rus haberleşmesini dinleyerek, verileri yetkililere anında aktarmayla kazanılmıştır.[549] Aynı zamanda, bu dönemde Alman mühendis olan Arthur Scherbius tarafından, Enigma makinesi üretilmiştir. Enigma isimli makine, şifreleme üzerine en önemli makinelerden biri olmuş, şifreli haberleşmede büyük rol oynamıştır.[550] Ayrıca yapmış oldukları çalışmalar, günümüzde siber istihbarat adına kullanılan sistemlerde, kendi ülkesi içerisinde önemli bir noktadadır.

İkinci Dünya Savaşı döneminde, Almanlar ve İngilizler arasında pek çok elektronik yöntem kullanılmıştır. Uçak sistemlerinin aldatılması, ilk kez elektronik karıştırma kullanılması, elektronik karıştırmaya tedbir olarak ilk defa bahsedilen "Channel Dash olayı (Unternehmen Zerberus/Operation Zerberus)" yine bu dönemde yaşanmıştır.[551] 1942 yılındaki olayda; üç Alman savaş gemisi hasar görmüş biçimde limana sığınmıştır. İngiliz Hava Kuvvetleri tarafından bu öğrenilmiş, bulundukları liman bombalanmıştır. Gemileri kaçırmak için harekete geçen Almanlar, İngilizlerin radarlarını karıştırmış, havadan destekle gemilerini kaçırmıştır. İngilizlerin karıştırmayı, hava olayından kaynaklandığını düşünmeleri sağlanmıştır. Radar olarak güçlü sistemler kullanılmış, ancak Almanlar, gemileri kaçırmayı başarmıştır.[552] Olaylar; İngilizler ve Almanlar açısından önemlidir. Karşılıklı olarak tehditler söz konusudur. Ayrıca iki ülkenin teknolojik bir çekişmede olduğu görülür.

1944 yılında, Almanlar için ayrı önemli bir olay yaşanmıştır. 1944 yılında yaşanan Normandiya Çıkartmasında, ilk defa elektronik savaş, bir hareket planına eklenmiştir. Elektronik anlamda kullanılan sistemlerle sahte hedef gösterilmiş, Almanlar sahte olan hedefe yöneldiği sırada karıştırma sistemi kullanılarak, Almanların atış kontrol sistemlerinde problem oluşmuştur. Bu sayede Almanların yedek kuvvetlerine erişmesi engellenerek, elektronik sistemler bir taktik

[549] Ünal, *Siber Güvenlik ve Elektronik Bileşenleri*, 9.
[550] James Graham, Richard Howard ve Ryan Olson, *Cyber Security Essentials* (Amerika: CRC Press, 2011), 10.
[551] Ünal, *Siber Güvenlik ve Elektronik Bileşenleri*, 12.
[552] Ken Ford, *Run the Gauntlet: The Channel Dash 1942* (ABD: Osprey Publishing, 2012), 29-70.

biçiminde kullanılmıştır.[553] Almanlar için olumsuz sonuçlar ortaya çıkartan bir olay olması, kendilerini belirli alanlarda geliştirmeleri gerektiğini görmelerini sağlamıştır. Bu dönemden itibaren, harekât planlarında, elektronik yöntemlerin kullanıldığı görülmüştür.

Yaşanan pek çok siber olayla belirli çalışmalarda bulunan Almanlar, 1986 yılının 15 Mayıs tarihinde, "2. Ekonomik Suçlarla Mücadele Kanununu[554]" yayımlamıştır. Siber suçlar hakkında uygulamaların belirlenmesi amaçlı Alman Ceza Kanunu'nda değişiklikler yapılmıştır. Siber alan kanunlar içerisine girmeye başlamış, çalışmalar bu çerçevede gelişmiştir. Siber çalışmalar devam ederken, 1997 yılında, internet ortamı üzerine suçlar, sorumlu tutulacak kişiler üzerine ilk çalışmalar; Kıta Avrupa'sında Federal Almanya Cumhuriyeti tarafından yapılmıştır.[555] "Tele Servisler Yasası[556]" adı altında açıklamalar getirilmiştir. Çalışma Almanlar ve pek çok aktör için ayrı bir önem taşımaktadır. O dönem yapılan çalışmalar için yeterlidir. Ancak ilerleyen dönem ve teknoloji, zamanla yetersiz kalmasına sebep olmuştur.

2009 yılı 14 Ağustos tarihinde yayımlanan, "Federal Bilgi Güvenliği Dairesi Yasası" ile bilgi güvenliğine gelebilecek tehlikelere karşı önlem alınmasından bahsedilmiştir. Ayrıca bir güvenlik geliştirilmesi, siber alanda güvenliğin test edilmesi, değerlendirilmesi, tehditlere karşı önlemler, bilgi ve iletişim teknolojisine karşı saldırıları değerlendirme, güvenliğini sağlamadan söz edilmiştir.[557] Üç yıl sonra Almanlar için önemli bir ulusal siber güvenlik stratejisi yayımlanmıştır. 2011 yılında, "Alman Ulusal Siber Güvenlik" stratejisi yayımlanmıştır. İçerik olarak; siber güvenliğin sağlanması, kritik altyapıların ulusal, uluslararası iş birliğiyle korunması, hakların uygulanmasını kapsamaktadır. Aynı zamanda, Ulusal Siber Mücadele Merkezi (NCRC) kurulması

[553] Ünal, *Siber Güvenlik ve Elektronik Bileşenleri*, 16.
[554] "Zweites Gesetz zur Bekämpfung der Wirtschaftskriminalität," Alman Federal Resmi Gazetesi, E.T.: 2 Ekim 2018, url: https://www.bgbl.de/xaver/bgbl/text.xav?SID=&tf=xaver.component.Text_0&tocf=&qmf=&hlf=xaver.component.Hitlist_0&bk=bgbl&start=%2F%2F*%5B%40node_id%3D%27288748%27%5D&skin=pdf&tlevel=-2&nohist=1.
[555] Ergün, *Siber Suçların Cezalandırılması ve Türkiye'de Durum*, 67.
[556] "Teledienstegesetz," E.T.: 2 Ekim 2018, url: https://dejure.org/gesetze/TDG.
[557] "Act on the Federal Office for Information Security," Alman Federal Adalet ve Tüketici Koruma Bakanlığı, E.T.: 2 Ekim 2018, url: http://www.gesetze-im-internet.de/englisch_bsig/englisch_bsig.html.

planlanmıştır.[558] 2016 yılında yayımlanan, "Almanya için Siber Güvenlik Stratejisi (Cyber-Sicherheitsstrategie für Deutschland 2016)" adlı çalışmada, siber çalışmalar üzerine bilgiler verilmiştir. Siber saldırılara karşı önlemler alınması, tespiti, savunması amaçlanmış, bunun için iş birliği ve kendi belirlediği eylemler üzerinden hareket edileceğini belirtmiştir.[559] 2018 yılında, "Dijital Konsey (Der Digitalrat)" ile Federal Almanya Cumhuriyeti, hükümete bağlı şekilde, yapılmak istenen projeleri hayata geçirmek ve bu alanda belirli uzmanlarla ilerlemek amaçlı, bu yapıyı oluşturmuştur.[560] Aynı yıl "Dijital Strateji"lerini duyurmuşlardır. Stratejide hedefler beş alan üzerindendir. Daha çok önlemler paketi şeklindedir. Hedeflenen; dijital alanların ekonomi, eğitim, sosyal alan ve altyapılarda etkilerini kapsamaktadır. Dijital beceri, altyapı ve ekipmanlar, yenilik ve dijital dönüşüm, dijital değişimde toplum, modern devlet konuları üzerine, 2025 yılına kadar beş ana hedef belirlenmiştir.[561] Yapılan çalışmalar ve stratejiler uygulamaya devam edilirken, 2019 yılında Federal Almanya Cumhuriyeti'ne siber saldırı düzenlenmiştir. Ocak aynıda yapılan saldırıda, Cumhurbaşkanı ve Başbakanın da aralarında bulunduğu pek çok siyasetçi, gazeteci, sanatçının kredi kartı bilgileri, adresleri ve telefon numaraları internete sızmıştır. Yapılan saldırılar sadece kişisel veriler üzerinden olduğundan, çok fazla üzerinde durulmamıştır.[562] Ancak, çeşitli konularda dikkat edilmesi gerektiğini gösteren bir olay olmuştur.

Olaylar ve stratejilerde siber alan artık ayrı bir yere gelmiştir. Ancak, stratejilerde Federal Almanya Cumhuriyeti iş birliğinden söz etmiş, yine kendi yöntemlerini takip edeceklerinden bahsetmişlerdir. Ulus ön planda tutulmuş, uluslararası anlamda oluşabilecek iş birliğinde, önce kendilerine uygun gördüklerini alıp, uygun görmediklerinde kendi fikirlerinde devam

[558] Maria Leitner, Timea Pahi, ve Florian Skopik, "Situational Awareness for Strategic Decision Making on a National Level," içinde *Collaborative Cyber Threat Intelligence,* ed. Florian Skopik (Amerika: CRC Press, 2018), 235.

[559] "Cyber-Sicherheitsstrategie für Deutschland 2016," Alman Federal İçişleri Bakanlığı, E.T.: 2 Ekim 2018, url: https://www.bmi.bund.de/cybersicherheitsstrategie/BMI_CyberSicherheitsStrategie.pdf.

[560] "Der Digitalrat - Experten, Die Uns Antreiben," Federal Alman Hükümeti, E.T.: 18 Ağustos 2019, url: https://www.bundesregierung.de/breg-de/themen/digitalisierung/der-digitalrat-experten-die-uns-antreiben-1504866.

[561] "The Digital Strategy of the German Government," Federal Alman Hükümeti, E.T.: 18 Ağustos 2019, url: https://www.bundesregierung.de/breg-en/search/the-digital-strategy-of-the-german-government-1550216.

[562] "Almanya'da Yüzlerce Siyasetçiye Siber Saldırı," *NTV Haber,* 04.01.2019, E.T.: 18 Ağustos 2019, url: https://www.ntv.com.tr/dunya/almanyada-yuzlerce-siyasetciye-siber-saldiri,tW74mFffvkm8o1g1h7FAsw?_ref=infinite.

edebileceklerini göstermişlerdir. Günümüzde siber alandaki tedbirlerle önemli çalışmalar devam etmekte, bu konuda hükümet tarafından oluşturulmuş birimler olduğundan söz edilmektedir.

Birimler, Federal Almanya Cumhuriyeti döneminde kurulmuştur. Siber suçlara karşı Federal Almanya Cumhuriyeti kendi İçişleri Bakanlığı içerisinde "Ulusal Siber Güvenlik Konseyi (National Cyber Security Council)"ni kurmuştur. Konseyde on maddelik bir strateji planı oluşturmuştur. Amaçlar; kritik bilgilerin bulunduğu altyapıların korunması, bilgi sistemlerin güvenliğini sağlamak, Ulusal Siber Suçlarla Mücadele Merkezi kurmak, bilgi teknolojisini güvenilir hale getirmek, eğitim, siber suçlara karşı önlem gibi hedefler belirlenmiştir.[563] Alman Federal Ordusu içerisinde; Stratejileri Aydınlatma Komandosu (Kommando Strategische Aufklarung- KSA), 2002 yılından beri hizmet veren, gözlem, keşif, sinyal, görüntü istihbaratı, elektronik mücadele çalışmalar üzerinden bir birim bulunmaktadır.[564] Ayrıca, Federal İstihbarat Servisi (Bundesnachrichtendienst-BND); istihbarat biriminde, uluslararası iletişimin izlenmesini sağlamıştır. Ticari anlamda bilgilere erişim sağlanmıştır. 1990'ların başında başlamış, özellikle, ticari anlamda bilgi ve teknolojik veriye erişilmiştir.[565] Bilgi Güvenliği Federal Ofisi (Bundesamt für Sicherheit und Informationstechnik- BSI) altında; siber güvenlik üzerine birkaç birim kurulmuştur. Bilgi Teknolojileri Durum ve Analiz Merkezi (IT-Lage und Analysezentrum) siber güvenlik stratejilerine dayandırılmış, günlük olarak internette zayıf noktaların bulunması, potansiyel tehditler gibi raporlama ve mevcut durumu bildirmekle görevlendirilmiştir. IT Kriz ve Müdahale Merkezi (IT-Krisenreaktionszentrum) bir olay karşısında hızlı müdahale, analiz ve önlem amacı gütmektedir. Ulusal Siber Savunma Merkezi (Nationales Cyber-Abwehrzentrum) kamuda operasyonel iş birliğini ayarlama, siber olaylar karşısında savunma ve koruma amaçlı önlemlerin koordinasyonundan sorumlu birimdir.[566] Siber alanla alakalı pek çok çalışma yürütmüş olan Federal Almanya Cumhuriyeti, günümüzde çalışmalarına devam etmektedir. Siber alanda önemli adımlar atmıştır. Birinci Dünya Savaşı'ndan itibaren yürütülen pek çok çalışma ve

[563] Mehmet Ünal ve Murat Gözübenli, "İnternet ve Kolluk," içinde *Siber Suçlar: Tehditler, Farkındalık ve Mücadele,* ed. Fatih Tombul, Murat Güneştaş ve Oğuzhan Başıbüyük (Ankara: Global Politika ve Strateji Yayınları, Ocak 2015), 232.
[564] Çıtak, *Güvenlik ve İstihbarat*, 240.
[565] Ira Winkler, *Spies Among Us* (Kanada: Wiley Yayıncılık, 2005), 94-95.
[566] Maria Leitner vd., "Situational Awareness for Strategic Decision Making on a National Level," 243.

strateji olmuştur. Ancak her çalışma siber alanın kendini yenilemesiyle yetersiz kalmıştır.

Geçmişten beri teknolojiye ağırlık vermiş olan Federal Almanya Cumhuriyeti, siber anlamda gelişip, değişimler ortaya çıkartmaya devam etmektedir. Olası bir saldırı anında, sağlam çıkabilmek için çalışmalara ayrı bir önem gösteren Federal Almanya Cumhuriyeti, şartlara göre iş birliğine sıcak bakmaktadır. İşbirliği dışında, belirli durumlarda kendi düşüncelerinin önemli olduğundan da söz edilmiştir. Olası bir siber tehdit ve saldırı anında izleyecekleri politikalar, saldırının çeşidine göre değişiklik gösterebilecek bir biçimdedir. Ancak, Federal Almanya Cumhuriyeti de diğer devletler gibi siber alanda tehdit altındaki devletlerdendir. Kendisi gibi geçmişte ve günümüzde çalışmalarına devam eden başka devletler de vardır. İkinci Dünya Savaşı Döneminde özellikle, çekişmeli rakiplerinden bir tanesi olan İngiltere, siber alanda çalışmalar yapmıştır. Özellikle geçmişinde, siber alanda çalışmaların temellerini atan ülkelerden biri olan İngiltere, günümüzde farklı çalışmalarıyla dikkat çekmiştir. Çalışmaların önemini daha iyi anlamak için İngiltere üzerine eğilmek gerekir.

2.1.5. İngiltere

Uluslararası alanda siber çalışma yapan devletler içerisinde önemli olanlardan biri İngiltere'dir. Gelişen teknoloji ve internetin her alanda yaygınlaşması, İngiltere üzerinde de bir etki yaratmıştır. Geçmişten günümüze, siber alanda yaşanabilecek ya da yaşanmış bazı olaylar üzerinden getirilen düzenlemeler, uluslararası alanda önemlidir.

Siber alanda İngiltere, çalışmalarına internetin temelleri atılmadan önce başlamıştır. İnternetin temelleri ilk, bilinen tarihinin öncesine gitmektedir. Ancak internetin başlangıcı olarak saymak da sayılmaz. İnternetin öncesinde, iletişim amaçlı yapılmış çalışmalar vardır. İnternetin ortaya çıkışı iletişim temellidir. 1851 yılında, uluslararası denizaltı kablosuyla, günümüzde İngiltere ve ABD olarak geçen iki ülke, iletişim amaçlı ilk çalışmalarla devletlerarasında bağlantıyı sağlamıştır.[567] Bu bağlantı, internet çalışmaları için önemli adımlardan biri olmuş, zamanla yapılan farklı çalışmalarla ve geliştirilen teknolojiyle internet bugünkü

[567] Johnny Ryan, *A History of the Internet and The Digital Future* (Londra: Reaktion Books, 2010), 95.

halini almıştır. Ancak, günümüz siber alanına ulaşmak için İngiltere, başka çalışmalarda bulunmuştur.

Elektronik Harp olarak geçen, savaş dönemlerinde kullanılan elektronik cihazlarla, siber alanın, İngiltere üzerinde gelişmelerde önemi vardır. Olaylardan biri; İkinci Dünya Savaşı döneminde, Almanlar ve İngilizler arasında yaşanan uçak seferlerinde aldatma yöntemi olmuştur. Almanlar önce belirli yerleri bombalamaya yönelmiştir. Yer tespiti için telsiz vericileri kullanıp, radyo frekansları gibi yer tespit etmek amaçlı uygulamalarda bulunmuştur. Ancak, İngilizler bunun farkına varıp, her denemede yerlerini farklı yerde göstererek aldatmaca yöntemini kullanmıştır.[568] Almanlar ve İngilizler arasında, savaş boyunca, elektronik gelişmelerle çekişmeler devam etmiştir. Savaş anında yaşanan çekişmelerle, iki devlet kendini diğerine göre geliştirmek amaçlı çalışmalarına önem vermiştir.

1982 yılında, Arjantin ve İngiltere arasında, Arjantin askerlerinin, İngiliz adalarından biri olan Falkland adasına (Falkland Islands/Islas Malvinas) çıkartma yapmasıyla başlamıştır. İngiltere, aldığı yardımlar sayesinde savaşı kazanmıştır. Elektronik anlamda savaşa önemli örneklerden biridir. Ancak, bu olay İngilizlerin, elektronik anlamda belirli eksikleri olduğunu görmelerini sağlamış, gelişmelerinde yardımcı olmuştur.[569] Eksikleri tamamlamak için belirli çalışmalara gidilmiş, aynı zamanda belirli düzenlemeler yapılmıştır.

İngiltere'de, siber alan üzerine belirli düzenlemelerin önemlilerinden biri, 1990'lı yıllarda yapılmıştır. 29 Temmuz 1990 yılında, bilişim suçları üzerine, "Bilgisayarların Kötüye Kullanılması Yasası[570]", yetkisiz veri ve programlara giriş, suç amaçlı bilişim cihazlarına girme, veri ve programların izinsiz değiştirilmesi üzerine yasa çıkarılmıştır.[571] 1996 yılı sonrasında, İngiltere, Güvenlik Ağı isimli bir oluşum kurmuştur. İçerisinde; servis sağlayıcılar, polis, Londra İnternet Değişim Grubu ve Servis Sağlayıcılar Birliği bulunmaktadır.[572] 1990'lı yıllardan itibaren yasa ve alanla alakalı çalışmalar yapacak birlikler ortaya çıkmaya başlamıştır.

---

[568] Ünal, *Siber Güvenlik ve Elektronik Bileşenleri*, 10-11.
[569] Ünal, *Siber Güvenlik ve Elektronik Bileşenleri*, 22.
[570] "Computer Misuse Act 1990," Birleşik Krallık Ulusal Arşiv, E.T.: 1 Ekim 2018, url: https://www.legislation.gov.uk/ukpga/1990/18/contents.
[571] Ergün, *Siber Suçların Cezalandırılması ve Türkiye'de Durum*, 65.
[572] Çakmak ve Altunok, *Suç, Terör ve Savaş Üçgeninde Siber Dünya*, 150.

1990'lı yıllarda yapılan çalışmaların zamanla yenilenmesine ihtiyaç duyulmuştur. Siber alan, 1990'lı yıllardan itibaren hızlı bir gelişme sürecine girmiştir. Gelişmelerse yeni tehditler getirmiş, yapılan çalışma ve yasaların yetersizleşmesine sebep olmuştur. 2000'li yıllarda, detaylı çalışmalar yapılmıştır. 2008 yılı Mart ayında, "İngiltere'nin Ulusal Güvenlik Stratejisi (The National Security Strategy of the United Kingdom) ulusal belgesi yayımlanmıştır.[573] 2008 yılında yayımlanan ulusal belgede; istikrarsızlık ve çatışma tehdit olarak görülmektedir. Çözüm olarak; iş birliği, önleme, erken harekete geçme, veri toplama, bütçe gibi tedbirler önerilmiştir. Belgedeki tehdit; bir istikrarsızlık, beraberinde ortaya çıkabilecek bir çatışmadır. Çözüm önerisi olarak; ihtiyaca göre iş birliği, önleme beraberinde, veri toplama gibi siber alandan yararlanılarak yapılabilecek tedbirler ortaya atılmıştır. Tony Blair döneminde hazırlanan belge, liberal bir içerik taşır. Ancak belge, güvenliği geniş bir biçimde tanımlar. Bu belgede; güvenlik kavramsallaştırması teorik arka planla oluşturulmuş, ciddi bir biçimde ele alınmıştır. Belgede, ulusal güvenlik hükümetin sorumluluğundadır. Tehdit kavramıysa değişmiş, yeni tehditler olarak; terörizm, sınır ötesi suçlar, çatışmalar, kitle imha silahları, başarısız devletler, salgın hastalıklardan söz edilmiştir.[574] Belgede bazı zamanlarda ittifak yapılabileceğinden bahsedilirken, bazı zamanlarda kendini geliştirme, kendini koruma yöntemine işaret etmektedir. Bu belgenin önem verdiği nokta; güvenlik tehdidi olarak; küresel istikrarsızlığa dikkat etmektir.[575] Genel anlamda; yeni, kapsamlı bir güvenlik tanımlaması yapılmıştır. Tanımlamayla beraber, karşılığında yapılabilecek önlemlerden söz edilmiştir. Ayrıca, küresel istikrarsızlıktan söz edilmiştir. Küresel istikrarsızlık; küresel yapının bozulmasına işaret etmektedir. Küresel yapının bozulması, özellikle uluslararası alanda, tehditlere açık bir yapı ortaya çıkmasına sebep olur. Bir istikrarsızlık oluşmaması için farklı çalışmalara yönelme ihtiyacı duyulmaktadır. Ulusal belgenin yayımlanmasından bir sene sonra, milli güvenlik adına stratejiler belirlenmiştir. 2009 yılı Haziran ayında, "Milli Güvenlik Stratejisi (The National Security Strategy of the United Kingdom: Update 2009 Security for

[573] Kabine Ofisi, *The National Security Strategy of the United Kingdom* (İngiltere: Mart 2008), E.T.: 19 Ağustos 2019, url: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/228539/7291.pdf.

[574] Yalçın, *Ulusal Güvenlik Stratejisi*, 41-82.

[575] Yalçın, *Ulusal Güvenlik Stratejisi*, 58-139.

the Next Generation)"[576] ortaya çıkmıştır.[577] İlk defa siber güvenlikten söz edilmiş bir strateji belgesi (Cyber Security Strategy of the United Kingdom)[578] yayınlanmış, bu konu üzerine önemli adımlar atılmıştır.[579] Belgenin en büyük özelliği ilk defa siber güvenlikten bahsedilmiş olmasıdır. Siber alanla alakalı önemli adımlar atılmasına sebep olmuştur.

2010 yılında yayımlanan "Stratejik Savunma ve Güvenlik Değerlendirmesi (Strategic Defence and Security Review)[580] (SDSR)" ulusal belgesinde; istikrarsızlık, siber saldırı, uluslararası terörizm, askeri krizler şeklinde birçok tehdit öne çıkmıştır. Mücadele amaçlı istihbarat, çıkarların korunması, uluslararası operasyonlar gibi birçok yöntemden de söz edilmiştir. Reel politik biçimde hazırlanan belgeyle, güvenliği önceleyerek politikalar yapılmıştır. Bu belgede tehditlerin yoğun ve çok olduğundan söz edilmiş, dikkat edilmesi gerekenlerin iki ana kriterle belirlenebileceğinden söz edilmiştir. Ana iki kriter; ortaya çıkma ihtimali ve ortaya çıkacak olursa gelişebilecek sonuçlar şeklinde ayrılmıştır.[581]

Siber alandan gelebilecek tehditlere önem verilmeye başlanmıştır. Önceki zamanlara göreyse detaylı çalışmalar yapılmıştır. 2011 yılında, 2009 yılının siber strateji belgesinin yenilenip güncellenmiş biçimi olan; "The UK Cyber Security Strategy: Protecting and Promoting the UK in a Digital World[582]" yayımlanmıştır.[583] Stratejide genel olarak; hükümetin gelişimi, siber anlamda saldırılar için hükümetle özel sektörün beraber hareket etmesi, ekonomik sıkıntıların azaltılması, siber alanda güvenlik üzerine belirli planlardan söz

[576] Kabine Ofisi, *The National Security Strategy of the United Kingdom: Update 2009 Security for the Next Generation* (İngiltere: Haziran 2009), E.T.: 1 Ekim 2018, url: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/229001/7590.pdf.
[577] Keleştemur, *Siber İstihbarat*, 188.
[578] Kabine Ofisi, *Cyber Security Strategy of the United Kingdom* (İngiltere: Haziran 2009), E.T.: 1 Ekim 2018, url: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/228841/7642.pdf.
[579] Keleştemur, *Siber İstihbarat*, 188.
[580] "Strategic Defence and Security Review," Kraliyet Parlamentosu, E.T.: 1 Ekim 2018, url: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/62482/strategic-defence-security-review.pdf.
[581] Yalçın, *Ulusal Güvenlik Stratejisi*, 41-136.
[582] Kabine Ofisi, *The UK Cyber Security Strategy: Protecting and Promoting the UK in a Digital World* (İngiltere: 2011), E.T.: 1 Ekim 2018, url: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf.
[583] Çiftçi, *Her Yönüyle Siber Savaş*, 51.

edilmiştir.[584] Siber alan güvenliği için belirlenen plan; devlet içerisinde bir bütünlük oluşturulması, dışarıya güçlü görünmeyi sağlayacak olmasıdır.

2015 yılında, "Ulusal Güvenlik Stratejisi, Stratejik Savunma ve Güvenlik İncelemesi 2015: Güvenli ve Başarılı Bir Birleşik Krallık (National Security Strategy and Strategic Defence and Security Review 2015: A Secure and Prosperous United Kingdom)" isimli ulusal güvenlik stratejisi yayımlanmıştır. Hedefleri; istihbarat ve güvenliği güçlendirmek, terörizme karşı mücadeleyle siber güvenlikte gelişmelere devam edilmesidir. Siber anlamda; suçlar ve terör kullanımına karşı ayrıca bir tedbir ve güvenlik önlemi alınması gerektiğinden bahsedilmiştir. Bunun sebebi; teknolojik gelişmelerin belirli alanlarda yetersiz kalmasıdır.[585] Güvenlik amaçlı siber alanın korunması için bu alanın gelişmesi gerekir.

2016 yılında yayımlanan "Ulusal Siber Güvenlik Stratejisi 2016-2021 (National Cyber Security Strategy 2016 to 2021)" belgede; dijital anlamda gelişmekte olan devlet için dijital toplum oluşturma hedefi vardır. 2021 yılına kadar, dijital ortamda siber tehdide karşı hazırlıklı olmak, siber anlamda korunma, saldırma, gelişmeye önem vermek, iş birliği içerisinde çalışmak önemlidir. Ayrıca, siber savunma alanında silahlı kuvvetlerde gelişmelerin sağlanması, ihtiyaç olunan araçlara sahip olmak, okullar dâhil pek çok alanda bilinçlendirilmeye devam etmek amaçlanmaktadır.[586] İleriye dönük, sistemli, siber alana dair stratejik çalışmalar yapılıyor olması; alanın korunması, üzerinde çalışılması gerektiğini gösterir. Ayrıca geliştirilmesi, tedbirli olunması gereken tehlikeleri barındıran bir alandır.

2017 yılında; "Geçici Siber Güvenlik, Bilim ve Teknoloji Stratejisi (Interim Cyber Security Science And Technology Strategy)" yayımlanmıştır.

[584] "Protecting and Promoting the UK in a Digital World," Birleşik Krallık Hükümet Sitesi, E.T.: 1 Ekim 2018, url: https://www.gov.uk/government/news/protecting-and-promoting-the-uk-in-a-digital-world--3

[585] "National Security Strategy and Strategic Defence and Security Review 2015 A Secure and Prosperous United Kingdom," Birleşik Krallık Hükümeti Sitesi, E.T.: 1 Ekim 2018, url: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/555607/2015_Strategic_Defence_and_Security_Review.pdf.

[586] "National Cyber Security Strategy 2016 to 2021," Birleşik Krallık Hükümet Sitesi, E.T.: 1 Ekim 2018, url: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf.

Risklerin önüne geçmek, ekonomik alandaki gelişmelerde siber alanı kullanmak, siber araştırma ve geliştirmelerde bulunmak, stratejiler yürütülmek amaçlıdır.[587]

Mart 2018'de; "İngiltere Ulusal Güvenlik Kabiliyeti İncelemesi (National Security Capability Review)" yayımlamıştır. Burada; "Füzyon Doktrini (Fusion Doctirne)" isimli doktrinin ulusal güvenlik amacıyla kullanımından söz edilmiştir. Ekonomik gelişim, silahlı kuvvetler, savunmada modernizasyon ve güçlenme, terörle mücadele stratejisinden söz edilmiştir. Ayrıca, Ulusal Siber Güvenlik Stratejisinin uygulanmaya devam edilmesi, tehditlere göre geliştirilmesi, bunların, yumuşak güç kullanarak yapılmasından bahsetmiştir.[588] İngiltere yeni milli güvenlik stratejisiyle, olası tehditlere karşı, hükümetin tüm unsurlarını koordineli harekete geçirme amacında olduğundan söz etmiştir.[589] İngiltere, yayımladığı belgelerde, siber alana ayrı bir önem vermiştir. Ülke içerisinde iş birliği ve yumuşak güç kullanımından bahsetmiştir. Kendini geliştirme ve savunma amaçlı, araştırma ve eğitime yönelmiştir. Üretilen politikalar dışında kurum ve kuruluşlar üzerinden çalışmalar yapılmıştır.

Belgeler beraberinde kurumsal çalışmalara ayrı önem verilmiştir. İngiltere, geçmişinde bir imparatorluktur. O dönemlerden kalan geniş bir istihbarat mirasına sahiptir. 11 Eylül ve Soğuk Savaş sonrasında, istihbarat alanını güçlendirme çalışmalarına devam etmiştir. Gelişen yeni güvenlik anlayışları üzerine, özellikle, terör ve siber alan gibi sahalarda çalışmalar yapmıştır.[590] Kendini istihbarat alanında geliştirmiş olan İngiltere, güvenlik üzerine kuruluşlar ve çalışmalar yürütmüştür.

Siber güvenlik üzerine İngiltere'de en yetkili birim; Kabine Ofisi (Cabinet Office)'dir.[591] Siber güvenlik, milli istihbarat ve güvenlik üzerine koordinasyon

[587] Kabine Ofisi, *Interim Cyber Security Science And Technology Strategy* (İngiltere: Kasım 2017), E.T.: 1 Ekim 2018, url: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/663181/Embargoed_National_Cyber_Science_and_Technology_Strategy_FINALpdf.pdf.

[588] "National Security Capability Review," Birleşik Krallık Hükümet Sitesi, E.T.: 1 Ekim 2018, url: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/705347/6.4391_CO_National-Security-Review_web.pdf.

[589] "İngiltere'den Yeni Milli Güvenlik Yaklaşımı," *HaberTürk*, 28.03.2018, E.T.: 1 Ekim 2018, url: https://www.haberturk.com/ingiltere-den-yeni-milli-guvenlik-yaklasimi-1894107.

[590] Çıtak, *Güvenlik ve İstihbarat*, 237.

[591] Hasan Çiftçi, *Her Yönüyle Siber Savaş* (Ankara: TÜBİTAK Popüler Bilim Kitapları, Temmuz 2017), 51.

bu birimde kurulur.[592] Devlet İletişim Karargâhı (Government Communications Headquarters- GCHQ); İngiltere'nin kendi iç ve dış güvenlik servislerinden sorumludur.[593] İngiltere'nin milli güvenlikten sorumlu üç birimlerinden biridir. Daha çok siber güvenlik üzerine görev yapar.[594] Ulusal Siber Güvenlik Merkezi (National Cyber Security Center- NCSC), Devlet İletişim Karargâhı'nın (GCHQ) bir parçasıdır. 2016 yılında kurulmuş, siber saldırılardan korunmak, devletin temel internet güvenliğini sağlamak, teknolojinin gelişimine yardımcı olmak amacıyla hizmet etmektedir.[595] Siber Güvenlik ve Bilgi Güvencesi Ofisi (Office of Cyber Security & Information Assurance- OCSIA); siber uzayın ve bilginin güvenliği, stratejik yönlendirmelerle koordinasyon bu kuruma bağlıdır. Siber Güvenlik Harekât Merkezi (Cyber Security Operations Center- CSOC); 2010 yılında kurulmuştur. Siber uzay üzerine yapılan gelişmeler, müdahale işlemleri için koordinasyon gibi görevlerden sorumu olan kurumdur. Milli Altyapıları Koruma Merkezi (Centre for the Protection of National Infrastructure- CPNI); altyapıyı, casusluk ve terörizm gibi tehditlerden korumak amaçlı, herhangi bir zafiyetin giderilmesinde söz sahibi olan kurumdur. Kamu Bilgisayar Olaylarına Acil Müdahale Ekibi (GovCertUK); devlete ait bilgisayarlarda oluşabilecek bir olaya karşı müdahale amaçlı kurulmuştur. Tehditlerin azaltılması amacıyla tavsiye veren kurumdur.[596] Küresel Harekât ve Güvenlik Kontrol Merkezi (Global Operations and Security Control Center); İngiliz Ordu ve Savunma Bakanlığı, siber savunmayla iletişim ağlarının yönetiminde görevli birimdir.[597] Emniyet Merkezi e-Suç Birimi (Police Central e-Crime Unit- PCeU); emniyete bağlı siber suç birimidir.[598] 77. Tugay (77th Brigade); sosyal medyada yaşanabilecek olay ve siber savaş üzerine 2015 yılında kurulmuş birimdir.[599] Siber alan üzerine pek çok birim ortaya çıkarmış olan İngiltere, detaylı çalışmalar yaparak kendini göstermiştir. İngiltere günümüzde çalışmalarına devam etmekte, yeni çalışmalar ortaya

[592] "About Us," Kabine Ofisi, E.T.: 19 Ağustos 2019, url: https://www.gov.uk/government/organisations/cabinet-office/about#responsibilities.
[593] Keleştemur, *Siber İstihbarat*, 189.
[594] Çiftçi, *Her Yönüyle Siber Savaş*, 52.
[595] "About the NCSC," Ulusal Siber Güvenlik Merkezi, E.T.: 1 Ekim 2018, url: https://www.ncsc.gov.uk/information/about-ncsc.
[596] Keleştemur, *Siber İstihbarat*, 189-190.
[597] Hasan Çiftçi, *Her Yönüyle Siber Savaş* (Ankara: TÜBİTAK Popüler Bilim Kitapları, Temmuz 2017), 54.
[598] Atalay Keleştemur, *Siber İstihbarat* (İstanbul: Level Kitap, Ağustos 2015), 190.
[599] Hasan Çiftçi, *Her Yönüyle Siber Savaş* (Ankara: TÜBİTAK Popüler Bilim Kitapları, Temmuz 2017), 54.

çıkarbilecek ülkelerden biri olmaktadır. Yaptığı çalışmalar ve kurduğu birimler çeşitlilik göstermektedir. Siber alanda yapmış olduğu çalışmalar, yeni tehditler çıkana kadar yeterli kalacaktır. Ancak, önemli olan, siber bir saldırı karşısında yeterli savunmayı sağlayabilmektir. Aksi bir durumda, günümüzde siber saldırıların çeşitleri çoğalmakta, zararları artmaktadır. Savunma yeterli olmadığında, devletin alacağı hasar artmaktadır. Hasara sebep olan devletle diğer devlet arasında, günümüzde var olan gerginliklerin artacağıysa daha açık görülmektedir.

Genel anlamda; siber güvenlik çalışmalarına devam eden İngiltere, belirli olaylar üzerinden hareket etmektedir. Olası bir saldırı karşısında hazırlıklı olma amacıyla, ulusal belgelerinde sık sık siber güvenliğe yer vermiştir. Siber güvenliği en iyi seviyeye getirmeye çalışmaktadır. Genel olarak, yaşanabilecek bir siber savaş için hazırlıklı olmaktadır. Hazırlıklı olmak için; hem araştırmalara hem teknolojik çalışmalara devam etmektedir. İngiltere çalışmalarını, kendi içerisinde bir iş birliği üzerinden yapma düşüncesindedir. Birim üzerinden, ilerleyen dönemlerde, önemli çalışmalar ortaya koyabilecektir. Uluslararası alanda, gelişen teknolojiyle, her geçen gün siber çalışmalarına önem vererek kendinden söz ettiren devletler vardır. Bu devletler içerisinde olan İngiltere dışında, incelenmesi gereken başka bir tanesi Türkiye Cumhuriyeti'dir. Belirli çalışmalarda bulunan devletlerden biri olan Türkiye Cumhuriyeti, siber alanda, diğer devletlere göre biraz daha geri konumdadır. Ancak, belirli konularda, alanda adından bahsedilebilen devletlerden biridir. Yapılan çalışmaların daha açık anlaşılması için Türkiye Cumhuriyeti'nden söz etmek gerekir.

2.1.6. Türkiye Cumhuriyeti

Siber çatışmalar uluslararası alanda çoğunlukla iki devlet arasında görülmektedir. Küresellikle beraber, siber çatışmalar iki devlet arasında olsa dahi, her aktörü ilgilendiren bir hâle dönüşmüştür. Hem kendi üzerinden, hem diğer devletler üzerinden çatışmalarla etkilenen devletler de bulunmaktadır. Siber saldırılarda adından söz edilen ve en çok etkilenen devletlerden biri Türkiye Cumhuriyetidir. Gelişen teknolojiyle, stratejilerini buna göre düzenlemiştir. Stratejik konumu itibariyle hâlâ önemli bir noktada bulunan Türkiye Cumhuriyeti, altyapıların elektronik ortama taşınmasıyla, alanla alakalı çalışmalarda bulunmuştur.

Türkiye Cumhuriyeti'nde, siber alanla ilgili teknolojik çalışmalar, yakın zamanlı gibi görünse de, 1960'lı yıllara kadar gitmektedir. Türkiye Cumhuriyeti'nde teknoloji üzerine önemli kurumlardan biri olan, 1968 yılında, Orta Doğu Teknik Üniversitesi'nde, sivil araştırma amaçlı kriptoloji ve elektronik araştırmalar yapılmıştır. Elektronik Araştırma Ünitesi'nin bugünkü hali olarak, Türkiye Bilimsel ve Teknolojik Araştırma Kurumu (TÜBİTAK) kurulmuştur. Hem teknolojik, hem siber alanda araştırmalarla önemli çalışmalar bu kurum içerisinde sağlanmıştır.[600] Günümüzde çalışmalarına devam eden kurum, bu alanda önemli birçok adım atmıştır.

TÜBİTAK dışında, önemli başka kurumlar 2000'li yıllarda, internetin ve siber alanın yaygınlaştığı dönemde ortaya çıkmıştır. Telekomünikasyon İletişim Başkanlığı (TİB); Ocak 2000 yılında kurulmuş, Kasım 2008 yılında Bilgi Teknolojileri ve İletişim Kurumu (BTK) adını almıştır. Telekomünikasyon sektöründe düzenleme ve bilgi teknolojilerinden sorumlu olan kurum, internet üzerine düzenleme, güvenlik, emniyet sağlama amaçlı görevleri de vardır.[601]

Kurum ve kuruluşların geliştirilmesi beraberinde kanun çalışmaları yapılmıştır. Türk Ceza Kanunu (TCK), siber güvenlik üzerine, dünya çapında belirlenmiş birçok ihlale düzenleme getirmiştir. 2004 yılında, TCK 1. Kitap (5237 Sayılı Türk Ceza Kanunu) 3. Kısım'da, Topluma Karşı Suçlar isimli Onuncu Bölümde[602], ihlallere düzenleme getirilmiştir. 243. Maddeyle, bilişim sistemlerinde yetkisiz girişle cezaya tabi tutulması hakkında kararlar belirlenmiştir.[603]

2007 yılı 4 Mayıs tarihinde, 5651 sayılı yasa "İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun[604]" yapılmıştır. 23 Mayıs 2007'de, Resmi Gazetenin 26530 sayılı yayınında uygulamaya koyulmuştur. İnternet ortamının kullanım esasları, yükümlülükler, sorumluluklar, cezai durumlar, kanunen aykırı

[600] Mitat Çelikpala, Salih Bıçakçı ve F. Doruk Ergun, "Türkiye'de Siber Güvenlik," *Ekonomi ve Dış Politika Araştırma Derneği* (2016): 33-35, E.T.: 30 Eylül 2018, url: http://edam.org.tr/document/CyberNuclear/SiberKitapTR/edam_siber_guvenlik_b2.pdf.

[601] Çelikpala vd., "Türkiye'de Siber Güvenlik," 33.

[602] "5237 Sayılı Türk Ceza Kanunu," Mevzuat Bilgi Sistemi, E.T.: 20 Ağustos 2019, url: http://www.mevzuat.gov.tr/Metin.Aspx?MevzuatKod=1.5.5237&MevzuatIliski=0&sourceXmlSearch=

[603] Çakmak ve Altunok, *Suç, Terör ve Savaş Üçgeninde Siber Dünya*, 184-185.

[604] "İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun," Mevzuat Bilgi Sistemi, E.T.: 20 Ağustos 2019, url: https://www.mevzuat.gov.tr/MevzuatMetin/1.5.5651.pdf.

zamanlarda internet ortamında bulunan yayının kaldırılması şeklinde hükümler içermektedir.[605] 24 Temmuz 2004'te 5070 sayılı kanunla[606], Elektronik İmza kullanımının hukuki boyutu belirlenmiştir. 5809 sayılı kanunla[607] 10 Kasım 2008'de Elektronik Haberleşme üzerine siber alanda düzenleme ve haklar tanımlanmıştır.[608] 2007 yılı 1 Kasım tarihinde, Resmi Gazetenin 26687 sayılı basımında, "İnternetin Toplu Kullanım Sağlayıcıları Hakkında Yönetmelik" yayımlanmıştır. 5651 sayılı kanuna göre hazırlanmış, düzenlemelerde siber anlamda tehditlerle mücadele ele alınmıştır.[609] Kanunlar çerçevesinde çalışmalar; devlet içerisinde, vatandaşların ihlalleri üzerine yapılmış yasalardır. Düzenlemelerin kanun içerisinde yapılması, devlet politikalarında siber alanın önemini göstermektedir. Ancak, yeni çalışmalara ihtiyaç duyulmuştur.

2009 yılı Ocak ayında, siber alanda ilk resmi belge olan; "Ulusal Sanal Ortam Güvenlik Politikası" yayımlanmıştır.[610] Mayıs ayındaysa, Bilgi Teknolojileri ve İletişim Kurumu "Siber Güvenliğin Sağlanması: Türkiye'deki Mevcut Durum ve Alınması Gereken Tedbirler" adlı belgeyi yayımlamıştır. Belgede; siber güvenlik, altyapı ve kritik bilgilerin tanımlanması, korunması ve yapılabileceklerden söz edilmiştir.[611] Aynı yıl siber olaylar yaşanmıştır. 9 Temmuz 2009 yılında, Sinbo isimli bir kullanıcının gönderisinde; Türk Ayyıldız Hack Takımı, Çin Halk Cumhuriyeti'nin 2000'den fazla internet sayfasına saldırmıştır. Aynı grup, Temmuz 2008 tarihinde, Alman Focus dergisinin belirttiği üzere; Avrupa Birliği sistemlerine girmiş, hassas bilgileri çalmaya çalıştığı makalede yer almıştır.[612] Türkiye Cumhuriyeti'nde, ülke saldırısı dışında, sivil saldırılar yapan hackerlar çoğunluktadır. Ancak bunları yapan; yine Türkiye Cumhuriyeti vatandaşıdır.

---

[605] Çakmak ve Altunok, *Suç, Terör ve Savaş Üçgeninde Siber Dünya*, 186-187.
[606] "Elektronik İmza Kanunu," Mevzuat Bilgi Sistemi, E.T.: 20 Ağustos 2019, url: http://www.mevzuat.gov.tr/MevzuatMetin/1.5.5070.pdf.
[607] "Elektronik Haberleşme Kanunu," Mevzuat Bilgi Sistemi, E.T.: 20 Ağustos 2019, url: http://www.mevzuat.gov.tr/MevzuatMetin/1.5.5809.pdf.
[608] Keleştemur, *Siber İstihbarat*, 423-430.
[609] Çakmak ve Altunok, *Suç, Terör ve Savaş Üçgeninde Siber Dünya*, 188-189.
[610] Keleştemur, *Siber İstihbarat*, 172.
[611] Bilgi Teknolojileri ve İletişim Kurumu, *Siber Güvenliğin Sağlanması: Türkiye'deki Mevcut Durum ve Alınması Gereken Tedbirler* (Türkiye: 2009), E.T.: 20 Ağustos 2019, url: https://www.btk.gov.tr/uploads/undefined/sg.pdf.
[612] Daniel Ventre, "Riots in Xinjiang and Chinese Information Warfare," içinde *Cyberwar and Information Warfare,* edit.: Daniel Ventre (Amerika: Wiley-ISTE, 2011), 306-307.

Siber alanda sadece saldırılar yapılmamış, aynı zamanda saldırılara maruz kalınmıştır. 13 Temmuz 2009'da; Türkiye Cumhuriyeti Başbakanı Recep Tayyip Erdoğan, soykırım olayların söz etmiştir. Bu olay üzerine; Çin Halk Cumhuriyeti yanlısı hackerlar, Pekin'deki Türkiye Büyükelçiliği'ne siber saldırı yapmıştır. Amaçları; Türkiye Cumhuriyeti hükümetinin, Çin Halk Cumhuriyeti iç işlerini açığa çıkartacağı, Sincan olaylarına müdahale edilmemesi için durdurulmasıdır.[613] Bunlar sonucunda devlet, siber alanda belirli çalışmalar yapmıştır.

2010 yılı 27 Ekim tarihinde, siber tehditler tartışılmıştır. Milli Güvenlik Kurulu içerisinde yapılan görüşmeler sonucu; siber tehditlerin "Milli Güvenlik Siyaset Belgesi"'ne dâhil edilmesi kararı verilmiştir.[614] Aynı yıl TÜBİTAK, kendi içerisinde Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi(BİLGEM)'ni kurmuştur. Haberleşme, bilgi güvenliği, kriptoloji üzerine çalışmalar burada yapılmıştır.[615] Aynı zamanda TÜBİTAK, kendi içerisinde TR-CERT isimli birimi oluşturmuştur. Ağ güvenliği sağlanması, risklerin tespiti çalışmaları yapılmıştır.[616] Çalışmalar bu kadarla kalmamış, ilerleyen yıllarda, öncekilere göre daha kapsamlı olmuştur.

2012 yılı 20 Ekim tarihinde, "Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyona İlişkin Karar", Bakanlar Kurulu tarafından onaylanmıştır. [617] 11 Haziran 2012 yılında, siber güvenlikle alakalı stratejiler, önlem ve planların onaylanması, koordinasyonunu sağlamak üzere Siber Güvenlik Kurulu oluşturulmuştur. Ulaştırma, Denizcilik ve Haberleşme Bakanlığı tarafından belirlenen stratejilerin onaylanmasıyla faaliyetlerin uygulanmasına karar verilmiştir.[618] Siber alan, güvenlik anlamında önemli bir yere gelmiştir.

20 Haziran 2013 tarihinde, "Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı[619]" yayımlanmıştır.[620] Eylem Planı'nda; kurumlardaki bilgi

[613] Ventre, "Riots in Xinjiang and Chinese Information Warfare," 307.
[614] Bıçakçı, *21. Yüzyılda Siber Güvenlik*, 45.
[615] "Siber Güvenlik ve Kritik Altyapı Güvenliği Çalışma Grubu Nihai Rapor Sürüm 1.0," Türkiye Bilişim Derneği, 10, E.T.: 30 Eylül 2018, url: http://www.kamu-bib.org.tr/kamubib-17/wp-content/uploads/2015/10/Kamu-BIB-CG1-Siber-Guvenlik-ve-Kritik-Altyapilar.pdf.
[616] Çakmak ve Altunok, *Suç, Terör ve Savaş Üçgeninde Siber Dünya*, 115.
[617] Bıçakçı, *21. Yüzyılda Siber Güvenlik*, 46.
[618] "Siber Güvenlik ve Kritik Altyapı Güvenliği Çalışma Grubu Nihai Rapor Sürüm 1.0,", 1-2.
[619] Bilgi Teknolojileri ve İletişim Kurumu, *Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı* (Türkiye: 2013), E.T.: 20 Ağustos 2019, url: https://www.btk.gov.tr/uploads/pages/2-1-strateji-eylem-plani-2013-2014-5a3412cf8f45a.pdf.
[620] Ünal, *Siber Güvenlik ve Elektronik Bileşenleri*, 126.

teknolojileri ve verilerin güvenliğinin sağlanmasından söz edilmiştir. Aynı zamanda, kritik altyapıların sistem güvenliğinin sağlanması, siber güvenlik sağlanarak, olası saldırılarda etkiyi en aza indirip, olayı tespit ederek, en kısa zamanda normale dönme hedeflerinden bahsedilmiştir.[621] 27 Mayıs 2013 tarihinde faaliyete geçen, Eylem Planı sonrası kurulan Ulusal Siber Olaylara Müdahale Ekibi (USOM); koordinasyon ve iş birliği amaçlı kurulmuştur. Kurumsal anlamda, Siber Olaylara Müdahale Ekipleri (SOME)[622], kurum ve kuruluşlar için 11 Kasım 2013 tarihinde Resmi Gazetede usul ve esasları yayımlanmıştır.[623] Genel olarak SOME; gelişebilecek bir siber tehditten, en asgari hasarla, olayın yayılmasının önüne geçmek için araştırma ve mücadeleyle kurtulma görevini üstlenmiştir.[624] Kurum ve kuruluşların çalışmaları devam etmektedir. 2013-2014 Eylem Planı süreci tamamladıktan sonra, yeni bir eylem planına ihtiyaç duyulmuştur. Aynı dönemde, siber alandaki ilerlemeler göz önüne alınarak, yeni eylem planı gündeme gelmiştir.

6 Mart 2015 tarihinde, "Bilgi Toplumu Stratejisi ve Eylem Planı 2015-2018" yayımlanmıştır. Bu planda; bilgi teknoloji ve güvenliği üzerine izlenecek eylemlerden söz edilmiştir. Siber Güvenlik Kanunu, kişisel verilerin korunması amaçlı mevzuatlar, güvenli internet kullanımında farkındalık oluşturma gibi; internet, bilişim ve teknoloji üzerine eylem planı olmuştur.[625] Strateji ve planlar, bir siber tehdit karşısında yapılacaklar üzerinedir. Planlar oluşturulurken; yaşanan olaylar dikkate alınır. Dikkate alınacak olayların sonuçlarıysa, savunma ve ileriye dönük çalışmalarda etkilidir. Söz edilen yılda eylem planı yayımlanmış, kısa sürede etkisiz kalarak, siber alanda bazı olaylar meydana gelmiştir.

2015 yılı 24 Kasım tarihinde; Türkiye Cumhuriyeti ve Rusya Federasyonu arasında siyasi gerginlik yaşanmıştır. Olayın başlangıcı; Türk F-16'sının, Rus Su-24 uçağını hava sahası ihlali sebebiyle düşürmesi olmuştur. 14 Aralık 2015 tarihinde, Türkiye Cumhuriyeti'ne siber saldırılar yapılmış, kritik alt yapılar hedeflenerek yapılan saldırılar Anonymus hacker grubu tarafından üstlenilmiştir.

---

[621] "Siber Güvenlik Stratejisi ve Eylem Planı," Bilgi Teknolojileri ve İletişim Kurumu, E.T.: 20 Ağustos 2019, url: https://www.btk.gov.tr/siber-guvenlik-stratejisi-ve-eylem-plani.

[622] "Kurumsal SOME Kurulum ve Yönetim Rehberi," T.C. Ulaştırma, Denizcilik ve Haberleşme Bakanlığı, E.T.: 30 Eylül 2018, url: http://www.udhb.gov.tr/doc/siberg/Kurumsal_SOME_Reh_V1.pdf.

[623] "Siber Güvenlik ve Kritik Altyapı Güvenliği Çalışma Grubu Nihai Rapor Sürüm 1.0," 6.

[624] Başaran, *Siber Savaş Cephesinden Notlar*, 215.

[625] Çiftçi, *Her Yönüyle Siber Savaş*, 418.

Resmi bir açıklama yapılmaması, saldırının Rusya Federasyonu operasyonlarından biri olması düşüncesini getirmiştir.[626] Bu olay yeni bir eylem planının ihtiyacını ortaya çıkartmıştır.

Teknolojinin ilerlemesiyle, güvenlik amaçlı, Ulaştırma, Denizcilik ve Haberleşme bakanlığı, ulusal siber güvenlik stratejisini güncelleme ve 2016-2019 eylem planlamasını yapmak için çalışmalara başlamıştır. 2015 yılında yapılan plan, "2016-2019 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı" adıyla ortaya çıkmıştır.[627] Yapılan eylem planının hedeflenen son dönemleri olan 2019 yılındaysa yeni bir plan hazırlanmıştır. Hazırlanan yeni strateji planı "2019-2023 Strateji Planı"dır. Plandaki hedefler; bilgi toplumu olmak için dijital dönüşüm sürecini hızlandırmaktır. Mobil olarak yerli haberleşme teknolojisini üretmek ve geliştirmek, kritik altyapıları korumak amaçlı elektronik haberleşme ve ulusal siber güvenliği sağlamaktır. Aynı zamanda güvenli, bilinçli ve etkin internet kullanımını arttırmayı kapsamaktadır.[628] Yapılan bu stratejilerle belirlenen sistemler dışında, belirli kurumlar siber güvenlik amaçlı çalışmalar yürütmüştür. Türkiye Cumhuriyeti'nde siber güvenlik amaçlı en önemli kuruluşlar; Silahlı Kuvvetler, Emniyet Genel Müdürlüğü, Milli İstihbarat Teşkilatı'dır.

Milli Güvenlik Kurulu; siber saldırılar sonrasında, tehditlerin ciddiyetini görerek, güvenlik tanımlamalarını 'Kırmızı Kitap' isimli askeri strateji belgesine eklemiştir. 2010 yılında, Siber Savunma Komutanlığı; siber ordu kurulması kararı almış, 2013 yılında, kuruluşu ilan edilmiştir.[629] 21 Ocak 2013 tarihinde, Türk Silahlı Kuvvetleri, Siber Savunma Merkezi Başkanlığı'nı oluşturmuş, bunun koordineli biçimde, Ulaştırma, Denizcilik ve Haberleşme Bakanlığı'yla yapacağını duyurmuştur.[630] 2013 yılında, kurulmuş olan Türk Silahlı Kuvvetleri Siber Savunma Merkezi Başkanlığı, 30 Ağustos 2013 yılında Türk Silahlı Kuvvetleri Siber Savunma Komutanlığına dönüşmüştür.[631] Güvenlik konusunda

[626] Darıcılı, *Siber Uzay ve Siber Güvenlik*, 223-225.
[627] "2016-2019 Ulusal Siber Güvenlik Stratejisi," T.C. Ulaştırma, Denizcilik ve Haberleşme Bakanlığı, 6, E.T.: 20 Haziran 2018, url: http://www.udhb.gov.tr/doc/siberg/2016-2019guvenlik.pdf.
[628] Bilgi Teknolojileri ve İletişim Kurumu, *2019-2023 Stratejik Planı* (Türkiye: 2019), E.T.: 20 Ağustos 2019, url: https://www.btk.gov.tr/uploads/pages/yayinlar-stratejik-planlar/btk-2019-2023-stratejik-plani.pdf.
[629] Çelikpala vd., "Türkiye'de Siber Güvenlik," 44.
[630] Bıçakçı, *21. Yüzyılda Siber Güvenlik*, 45-47.
[631] "Türk Ordusunun Yeni Kuvveti Siber Savunma," *Hürriyet Haber,* 06.06.2016, E.T.: 20 Ağustos 2019, url: http://www.hurriyet.com.tr/teknoloji/turk-ordusunun-yeni-kuvveti-siber-savunma-40113652.

siber alan artık belirli bir yapı içerisine oturmaya başlamıştır. Çalışmaların belirli bir kurum içerisinden yürütülmesi, yapılacak savunma ve saldırı anlarında düzen beraberinde başarı sağlayacağı bilinmektedir.

1998 yılı Nisan aynıda, Emniyet Genel Müdürlüğü içerisinde, Bilgisayar Suçları ve Güvenlik Kurulu oluşturulmuştur. Kuruluşun amaçları kapsamında; bilişim suçları, mevzuatların incelenmesi, bir bilişim teknolojisiyle işlenecek suçta, araçlar ve çeşitlerinin farklarının belirlenmesi vardır. 2011 yılında; Bilişim Suçlarıyla Mücadele Daire Başkanlığı hayata geçirilmiş, 2013 yılında, Siber Suçlarla Mücadele Daire Başkanlığı'na dönüşmüştür. Ayrıca, siber güvenlik amaçlı, bir tehdidin önüne geçmek için, istihbarat toplama görevi Milli İstihbarat Teşkilatı'na verilmiştir.[632]

15 Mart 2017 yılında; derneklerle faaliyette bulunup, sonradan bir araya gelen, devlet üzerinden eğitimle bağlı, Uluslararası Siber Güvenlik Federasyonu kurulmuştur. Siber alanda pek çok derneğin bağlı olduğu federasyon, çalışmalar yapıp, siber güvenlik alanında eğitim vererek, ülke içerisinde, siber alanda eğitimli kişiler yetiştirmeyi hedeflemiştir.[633] Aynı yıl, Savunma Sanayi Başkanlığı'nın desteğiyle, Türkiye Siber Güvenlik Kümelenmesi kurulmuştur. Tüm kamu, akademik ve özel sektör temsilcilerinin katılımlarıyla ortaya çıkmıştır. Siber güvenlik üzerine çalışmalar yapılması amaçlı bir proje şeklindedir.[634] Yapılan proje ve çalışmalar devam etmektedir. Siber alanın aynı hızda ilerlemesi çalışmalara da yansımıştır.

Genel olarak; Türkiye Cumhuriyeti siber alan için çalışmalarda bulunmuştur. ABD, Çin Halk Cumhuriyeti ve Rusya Federasyonu kadar güçlü değildir. Ancak, yapılmış ve yapılacak çalışmalarla, büyük gelişmeler gösterecek kapasitededir. Kurumsal ya da hükümet açısından büyük çalışmalar, uzun süreçlerde yapılmaktadır. Bireysel siber çalışmalardaysa, kişilerin kendilerini geliştirip, önemli ölçüde kendini gösterdiği bilinmektedir. Özellikle hacker grupları içerisinde; Türk hackerların önemli bir yeri vardır. Ancak devlet, bu gruplara göre, yakın dönemde alana daha çok eğilmeye başlamıştır. Türkiye Cumhuriyeti eylem planları ve stratejilerini, önceki yıllara göre geliştirmesi, bir

[632] Çelikpala vd., "Türkiye'de Siber Güvenlik," 46-47.
[633] "Uluslararası Siber Güvenlik Federasyonu," *Uluslararası Siber Güvenlik Federasyonu* 2 (2017): 25.
[634] "Hakkında," Türkiye Siber Güvenlik Kümelenmesi, E.T.: 20 Ağustos 2019, url: https://siberkume.org.tr/hakkinda/.

siber savaş halinde güçlenmesini sağlar. Ancak, çalışmalar asgari düzeyde kaldığı sürece, bir siber savaş karşısında problemler çıkacaktır. Siber alana, günümüzde biraz daha önem verilmesi, siber saldırılar karşısında daha güçlü olunmasını sağlayacaktır.

Uluslararası alanda, iş birliği çalışmalarında bulunanlar sadece devletler değildir. Siber alanda çalışma yapan belirli örgütler vardır. Bu örgütler siber anlamda çalışmalar yaparken, kendi içerisinde bazı ülkelerin iş birliğinde olduğundan da söz edilir. Uluslararası yapıların siber çalışmalarından söz etmek, ülkelerin kendileri dışında, ortak yaptıkları çalışmaları anlamada yardımcı olacaktır. Uluslararası alanda çalışmalarda bulunan örgütler, genelde üye ülkeleri kapsayıp, sadece belirli ölçüde etkili olmaktadır. Önemli bazı örgütlerin, siber alanda izledikleri politika ve antlaşmaları belirli örnekler üzerinden açıklamak gerekir.

2.2. BAZI ÖRGÜTLERİN SİBER ORTAMDA OLUŞABİLECEK TEHDİTLER ÜZERİNE BELİRLEDİKLERİ POLİTİKALAR VE ANTLAŞMALAR

Siber çalışmalar ülkeler düzeyinde gelişip ilerlemektedir. Günümüzde ülkeler kendi amaçları doğrultusunda çalışmalar yaparlar. Ancak, siber alan sadece ülkelerle sınırlı değildir. Siber alan ülkeleri aşan bir yapıdadır. Ancak, küresellikle benzerlikler gösterebilir. Küreselleşme içerisinde karşılıklı bağımlılık barındırırken, bu siber alanda yoktur. Siber alanın sınırlarının bilinmezliğiyse devletlerin önlem almalarına sebep olmuştur. Siber alanın yine de belirli ölçüde bağlayıcı bir yapısı vardır. Fakat küreselleşmenin getirdiği kadar ciddi boyutta değildir.

Devletler yaptığı çalışmalarında, her biri kendi amaç ve çıkarları doğrultusunda hareket etmektedir. Uluslararası kuruluşlarsa, devletlerden daha farklı amaçlara sahiptir. Uluslararası kuruluşlarda genel amaç; devletlerarasında uzlaşmayı sağlamaktır. Uluslararası yapılar, kendi içerisindeki üye devletlerin çıkarlarını gözetecek bir sistemdedir. Ancak siber tehditler daha karmaşık bir yapıya sahiptir. Siber tehditler, sadece bir devlete yapılmamaktadır. Aynı zamanda tek taraflı değildir.

Siber saldırılar sadece devletlerle sınırlı değildir. Terör örgüleri gibi farklı aktörler arasında da görülmektedir. Teknolojik olarak gelişmiş her grup, siber

alanı rahatlıkla kullanabilmektedir. Gelişen teknolojiyle, belirli dönemlerde, tek bir kişi dahi bir devlete tehdit oluşturabilmektedir.

Siber alan her birey, devlet ya da uluslararası sisteme açıktır. Bu sebeple; önemli birçok uluslararası örgüt, belirli düzenlemeler yapmıştır. Günümüzde bir siber savaş yaşanmaktadır. Ancak günümüzde devam eden siber savaş, siber alanda devletler düzeyindedir. Karmaşık bir yapıda olan siber alanın, uluslararası ilişkilerde problem oluşturacak önemli tehditlerinden biri; devletlerin kendi arasında oluşan ve oluşabilecek anlaşmazlıklardır. Bu nedenle önlemler alınarak, ciddi çalışmalar yapılmaktadır. Uluslararası örgütler içerisinde önemli olan örneklerden söz ederek, çalışmalarından bahsedilmelidir. Bunun için ilk olarak; Avrupa Birliği'nden söz etmek gerekir.

2.2.1. Avrupa Birliği

Siber alanda, uluslararası çalışmalarda bulunan önemli yapılanmalardan biri; Avrupa Birliği'dir. Üye devletler siber alanda çalışmalar yapmaktadır. Ancak, uluslararası bir yapı olarak Avrupa Birliği, siber alanda farklı ve önemli çalışmalar yapmıştır.

Siber alan üzerine çalışmalarda; kritik altyapıları korumak, tehditlere karşı güvenlik sağlamak önemlidir. Avrupa Birliği, kritik altyapıları tanımlamıştır. Tanımlamaya göre; Kritik altyapılar, toplumsal işleyişin sürdürülmesi için en gerekli sistemlerdir. Kritik altyapılara gelecek bir zarar, vatandaşların, toplumun, üye devletlerin, ciddi derecede olumsuz etkilenmesine sebep olur.[635] Avrupa Birliği'nin tanımladığı önemli altyapılar; su, sağlık, enerji iletişim, bilgi teknolojileri, kamu-hukuk düzeni, finans, uzay ve araştırma, sivil yönetim, nükleer, kimyasal sanayi ve taşımacılığı kapsar.[636] Günümüzde kritik altyapılar, siber alanla bağlantılı konuma gelmiştir. Bu sebeple; kritik altyapılara gelecek bir zarar için önemli politikalar oluşturulup, çalışmalar yapılmalıdır.

1995 yılında, "Avrupa Birliği Kişisel Verilerin Korunması ve Gizlilik Direktifi" yayımlanmıştır. Bu direktifle kişilerin siber alandaki verilerinin korunması çalışmaları yapılmıştır. Direktifte; veri ve bilginin özgürce dolaşmasını sağlamak, kişinin mahremiyetini korumak, bunu devletler üzerinden dengelemek

[635] "Critical Infrastructure," European Union, E.T.: 21 Ağustos 2019, url: https://ec.europa.eu/home-affairs/what-we-do/policies/crisis-and-terrorism/critical-infrastructure_en.
[636] Ünal, *Siber Güvenlik ve Elektronik Bileşenleri*, 109.

gerektiğinden bahsedilir.[637] Üye devletlerin uyum çalışmasına yarayan bu belge, veri koruma amaçlı, ekonomik problemler çıkmasını önlemek adına, birbirine yakın bir koruma düzeyi geliştirilmesini amaçlamıştır.[638] Yapılan çalışmada, hem veri hem kişilerin korunması amacı vardır. Verilerin özgürce dolaşması için uyumun öneminden bahsedilir. Direktifte söz edilen ekonomik eşitsizliğinin çıkaracağı problemi engellemek bir amaçtır. Bunun için dengeli bir koruma sisteminden bahsedilmiştir. Bu sistem; devletlerarasında dengeyi sağlayarak, birlik içerisinde hareket etmelerini kolaylaştırmıştır. 1995 yılında yapılmış bu çalışma, daha çok başlangıç niteliğinde olmuştur.

31 Temmuz 2002'de, "Elektronik Haberleşme Sektöründe Gizliliğin Korunması Direktifi[639]" yayımlanmıştır. Bu direktif, 1995 yılındaki direktifin tamamlayıcı niteliğindedir. Elektronik haberleşme üzerine temel özgürlük ve haklara saygı, kişisel verilerin korunması, özel yaşamın gizliliğinden söz edilmiştir. Teknolojik gelişmeler buna dâhil edilmiş, istenmeyen e-posta, ticari elektronik iletiler üzerine düzenlemeler değerlendirilmiştir.[640]

5 Haziran 2003 tarihinde, Avrupa Birliği Ağ ve Bilgi Güvenliği Ajansı (European Union Agency for Network and Information Security- ENISA) kurulması kararı alınmıştır. 14 Mart 2004'te kuruluşu fiilen tamamlanmıştır. ENISA'nın amacı; Avrupa Birliğinde siber güvenlik sağlanması için, koordinasyonla tüm Avrupa'da bilgi ve ağ güvenliğini sağlamaktır.[641] ENISA, bazı olaylarda operasyonel ekiplerle iş birliğinde bulunup, politika oluşturarak çalışmaları destekler, ayrıca, siber güvenlik stratejileri geliştirir.[642] 2012 yılında, siber olaylara müdahale amaçlı CERT-EU (Computer Emergency Response Team-EU- Avrupa Birliği Bilgisayar Acil Müdahale Ekibi) kurulmuştur.[643] 2013 yılında, enerji ve ulaşım altyapısı gibi endüstriyel kontrol sistemlerinde, siber anlamda ulusal direncin gelişimini sağlamak için; ENISA, kendi içerisinde

[637] "European Directive on Protection of Personal Data and Privacy-Directive 95/46/E.C," Avrupa Parlamentosu ve Konseyi, E.T.: 3 Ekim 2018, url: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:31995L0046&from=en.
[638] Ergün, *Siber Suçların Cezalandırılması ve Türkiye'de Durum*, 64.
[639] "Privacy and Electronic Communications Directive 2002-Directive 2002/58/EC," Avrupa Parlamentosu ve Konseyi, E.T.: 3 Ekim 2018, url: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32002L0058&from=EN.
[640] Eren, *Avrupa Birliği'nin Siber Güvenlik Politikası*, 76.
[641] Eren, *Avrupa Birliği'nin Siber Güvenlik Politikası*, 73.
[642] Leitner vd., "Situational Awareness for Strategic Decision Making on a National Level," 230.
[643] Çiftçi, *Her Yönüyle Siber Savaş*, 58.

Endüstriyel Kontrol Sistemi- Bilgisayar Güvenliği Olaylarına Müdahale Ekibi (ICS-CSIRTs)'ni kurmuştur.[644]

15 Mart 2006 yılında, "Verilerin Saklanması Direktifi (European Directive on Data Retention)"[645] yayımlanmıştır. İçeriği; siber tehditlere karşı mücadele için yapılması gereken hükümlerdir.[646] Direktif, üye devletlerin belirledikleri yasal çerçevelerde uyum sağlanmasını amaçlar.[647] Direktifte, üye devletlerin yasalarının uyumlaştırılması, bir tehdit anında karışıklık çıkmadan karar alınmasını sağlar. 7 Şubat 2013 tarihinde, "Avrupa Birliği Siber Güvenlik Stratejisi: Açık, Güvenilir ve Güvenli Bir Siber Alan (Cybersecurity Strategy of the European Union: an Open, Safe, and Secure Cyberspace)"[648] isimli belge yayımlanmıştır. Burada; siber güvenliğin önemi, güvenliğin sağlanabilmesi için iş birliği, ayrıca, ENISA'nın geliştirilip modernleştirilmesi gerektiğinden bahsedilmiştir. Siber tehditler üzerine yeni gelişmelerin takip edilmesi, buna göre çalışmalar yapılmasından söz edilmiştir.[649] Gelişmelerin takip edilmesi, savunma ve güvenlik açısından önemli aşamalardandır. İşbirliği düşüncesi üzerinden güvenliği sağlamak, üye devletlerin arasında oluşabilecek olumsuzlukların önüne geçmek için bir çalışmadır.

Güvenlik stratejileri oluşturulduğu dönemde, politikalar da üretilmeye başlanmıştır. 18 Kasım 2014 tarihinde, "Avrupa Birliği Siber Savunma Politikası Çerçevesi (EU Cyber Defense Policy Framework)"[650] ile üye devletlere siber savunmanın gelişimi için destek olunması hedeflenmiştir. Aynı zamanda; iletişim ağlarının güvenliklerini arttırmak, asker ve sivil arasında iş birliğini genişletmek, tatbikat ve eğitimler geliştirilmesine yardımcı olmak, uluslararası kurumlar arasında iş birliği sağlamak amacı gütmüştür. Tamamen siber savunma üzerine bir faaliyet içermektedir. Bilgi ve ağ güvenliğinin sağlanması, uluslararası aktörlerle

[644] Eren, *Avrupa Birliği'nin Siber Güvenlik Politikası*, 74.
[645] "European Directive on Data Retention," Avrupa Parlamentosu ve Konseyi, E.T.: 3 Ekim 2018, url: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32006L0024&from=EN.
[646] Çakmak ve Altunok, *Suç, Terör ve Savaş Üçgeninde Siber Dünya*, 170.
[647] Eren, *Avrupa Birliği'nin Siber Güvenlik Politikası*, 76-77.
[648] "Cybersecurity Strategy of the European Union: an Open, Safe, and Secure Cyberspace," Avrupa Komisyonu, E.T.: 3 Ekim 2018, url: https://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf.
[649] Sandro Bologna, Alessandro Fasani ve Maurizio Martellini, "Cyber Security and Resilience of Industrial Control Systems and Critical Infrastructures," içinde *Cyber Security: Deterrence and IT Protection for Critical Infrastructures,* edit. Maurizio Martellini (Amerika: Springer, 2013), 69-70.
[650] "EU Cyber Defense Policy Framework," Avrupa Parlamentosu, E.T.: 3 Ekim 2018, url: http://www.europarl.europa.eu/meetdocs/2014_2019/documents/sede/dv/sede160315eucyberdefencepolicyframework_/sede160315eucyberdefencepolicyframework_en.pdf.

iş birliği, üye ülkelerde siber altyapıya zarar gelmemesi için uzman desteği verilmesi amaçları benimsenmiştir.[651] Avrupa Birliği içerisinde, Avrupa Savunma Ajansı (European Defence Agency- EDA) bulunmaktadır. Siber güvenlik ve savunmayı öncelikli bir eylem olarak görmektedir. 2014 yılında yayımlanmış olan belgeyle çalışmalarına, siber alanla alakalı yenilerinin eklemiştir. Siber alanda eğitim ve tatbikatlar, farkındalık sağlamak, siber ve askeri alanda teknolojinin geliştirilmesini hedeflerken, kriptografi amaçlı çalışmalar da yürütmektedir.[652] 2014 yılındaki çalışmalarda; eğitim ve iş birliği amacı vardır. Teknoloji ve siber alanın eskisinden hızlı ilerlemesi, yapılan çalışmaların yerine yenilerine ihtiyaç duyulmasına sebeptir.

6 Temmuz 2016 tarihinde, "Ağ ve Bilgi Sistemlerinin Güvenliği Hakkındaki Direktif- NIS Direktifi (The Directive on Security of Network and Information Systems- NIS Directive)"[653] yayımlanmıştır. İlk gerçek siber güvenlik kurallarını belirleyen direktif olmuştur.[654] Siber güvenlik seviyesini arttırmak için yasal önlemleri amaçlamaktadır. Devletlerin siber güvenlik kapasitelerini düzenlemek için çalışmalar, sektörler arası iş birliğiyle önemli altyapıların güvenliği, dijital hizmet veren sağlayıcılar, bu direktifle belirli bir düzene oturtulması hedeflenmiştir. Ayrıca, bildirim ve güvenlik amaçlı şartlara uymaları gerektiğinden söz etmektedir.[655] Direktifle, Avrupa Birliği üyelerinin hepsi, siber güvenlik üzerine iş birliği ve standartları uygulamayı kabul etmişlerdir. Ancak, sadece kendi üyelerini kapsamaktadır. Bu da etkisini sınırlı kılar.[656]

2018 yılında, Avrupa Birliği, ENISA'nın görevlerini güçlendirerek, bir Siber Güvenlik Yasası üzerine anlaşmışlardır. 2017 yılında önerilen bu yasa, 2019 yılında onaylanmıştır. Amacı, üye ülkelere siber güvenlik üzerine, tehdit ve saldırılarda destek vermek ve bu alanda iş birliğine yöneltmektir. ENISA'nın gücünün arttırılmasıysa; bir siber saldırıda, etkin cevap verebilmeyi sağlamak

[651] Çiftçi, *Her Yönüyle Siber Savaş*, 102-103.
[652] Leitner vd., "Situational Awareness for Strategic Decision Making on a National Level," 231.
[653] "The Directive on Security of Network and Information Systems (NIS Directive)," Avrupa Parlamentosu ve Konseyi, E.T.: 3 Ekim 2018, url: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016L1148&from=EN.
[654] Kremling ve Sharp Parker, *Cyberspace, Cybersecurity, and Cybercrime*, 357.
[655] "The Directive on Security of Network and Information Systems (NIS Directive)," Avrupa Komisyonu, E.T.: 3 Ekim 2018, url.: https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive.
[656] Kremling ve Sharp Parker, *Cyberspace, Cybersecurity, and Cybercrime*, 357.

amaçlıdır. Aynı zamanda, kritik altyapıların geliştirilip, üye ülkeleri bu amaçlı bilgilendirmeyi kapsar.[657]

Avrupa Birliği genel olarak; kurulduğu yıldan beri çeşitli direktifler yayımlamıştır. Direktifler içerisinde; siber alanın, uluslararası alanda ciddi bir yer tutmasıyla, üzerine politikalar yapılmasına önem verilmiştir. Çeşitli devletlerin üye olması, problemleri de beraberinde getirmiştir. Siber alandaki gelişmelerden farklı olarak; yayımlanan belgelerin birçoğunda devletlerarası uyum çalışmaları yapılmıştır. Genel olarak; siber alanda, ülkelerin teknolojik olarak gelişmiş olanının, daha güçlü olduğu kanısı vardır. Bu sebeple; yapılabilecek uyum çalışmaları, iş birliği düşüncesiyle belirli bir çözüm getirebilecek olsa bile, tam bir çözüm, olaya göre değişkenlik gösterir. Bir siber savaş ihtimali, savaşın hangi devletlerarasında olacağına bağlı olarak, siber alandaki güç dengesinin önüne geçebilir. Avrupa Birliği, kendi bünyesindeki devletlerarasında problemler çıkmasını engellemek amacıyla çözümler geliştirmektedir. Ayrıca, dışarından gelebilecek tehditlere karşı çözümler bulmaya çalışmıştır. Söz konusu bağlayıcılık, bir devlet kanunları kadar olmadığı için, bir siber savaş ihtimalinde geçerliliği, olayın büyüklüğü ve koşullarına göre değişiklik gösterecektir. Ancak, yeni hazırlanan yasanın getireceği sonuçlar ve bağlayıcılığı henüz bilinememektedir. Bağlayıcı olsa dahi, sadece üyeleri kapsaması, yine yapılan çalışmayı belirli sınırlar içerisinde tutmaktadır. Siber alanda, uluslararası bir yapılanma olarak, Avrupa Birliği dışında çalışma yapan başka kuruluşlar bulunmaktadır. Avrupa Birliği dışında önemli çalışmalar yapan, ilk akla gelenlerden biri NATO'dur. NATO'nun siber alanda yapmış olduğu çalışmaları incelemek, bu alan için önemlidir.

2.2.2. NATO

Avrupa Birliği'nin uluslararası alanda yaptığı çalışmalar gibi, NATO bu alanda önemli çalışmalarda bulunmuştur. Genellikle askeri ve savunma üzerine çalışmalar yapan NATO, siber alan üzerine de çalışmalar yapmıştır. Siber alan, artık savunma ve savaş alanında yeni bir boyut olarak görülmeye başladı. Devletler dışında, uluslararası alanda ayrı ve önemli bir yere sahip olmuştur. NATO, askeri ve siyasi olarak, üyelerinin özgürlük ve güvenliklerini sağlama

[657] "The EU Cybersecurity Act," European Union, E.T.: 21 Ağustos 2019, url: https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-act.

amaçlı ortaya çıkmıştır. Askeri ittifakla savunma, kolektif olarak güvenlik organizasyonu şeklinde geliştirilmiştir.[658] Amaçları doğrultusunda, siber alandaki tehditler için çalışmalarına başlamıştır.

Siber alandaki problemler, sadece devletlerarasında yaşanmamıştır. Artık uluslararası sistemde siber tehditler kendini göstermiştir. Saldırılar artık ulus-devlet düzeyini aşacak konuma gelmiştir. Uluslararası örgütler, bu konuda, hazırlık yapmaya başlamıştır. NATO; 1999 yılında, özellikle internet üzerine yapılan çalışmalarda, üyelerini askeri haberleşme sistemlerine gelecek bir saldırıya karşı uyarmıştır. Üyelerin hazırlıklı olmaları istenmiş ancak, ilk siber saldırılar tahmin edilenden önce gerçekleşmiştir.[659] NATO, 1990'lı yılların sonlarında, siber alanda ortaya çıkabilecek tehditlerin ciddiyetini, çalışmalar yaparak belirlemiştir. Üye devletleriyse hazırlıklı olmalarına karşı uyarmıştır. Siber alan ve teknoloji, beklenenden daha hızlı ilerlemiş, bu hıza yetişmek zor olmuştur. Siber alanın gelişmeleri ve getirdikleri sonucunda saldırılar yaşanmıştır. 1999 yılında, Kosova Krizi'nde, NATO'nun gerçekleştirdiği Kosova operasyonu sürecinde, Brüksel'de bulunan ağ sunucuları, Sırbistan kaynaklı saldırılara uğramıştır. Başka kaynaklar üzerindense, Yugoslavya'nın ana sunucusu, e-posta saldırılarına uğramıştır.[660] Bu olaylar sonucu belirli çalışmalar yapılmaya başlanmıştır. 2002 yılında, NATO Prag Zirvesi[661]'nde Bilgisayar Olaylarına Müdahale Yeteneğinin (NATO Computer Incident Response Capability-NCIRC) ve siber savunmanın geliştirilmesi görüşmeleri yapılmıştır.[662] Çalışmalar bu kadarla kalmamış, birçok zirve yapılarak, konu üzerinde geliştirme ve görüşmeler devam etmiştir.

2008 yılında, NATO Bükreş Zirvesi[663] sonucu; üyelerin sistemlerini siber saldırılara karşı güçlendirmeye devam edip, siber savunma oluşturulacağından söz edilmiştir. NATO'nun amacı; siber savunmadır. Üye devletlerin siber sistemlerini, istedikleri takdirde, güçlendirmeye yardım edilip, devletlerarası ilişkilerin güçlendirilmesinden söz edilmiştir. Zirve sonrasında, Brüksel'de bir NATO Siber

[658] Levent Yiğittepe, *NATO Güvenlik Politikaları ve Terörle Mücadele Stratejileri* (İstanbul: Cinius Yayınları, Şubat 2017), 28.
[659] Bıçakçı, *21. Yüzyılda Siber Güvenlik*, 30.
[660] Çakmak ve Altunok, *Suç, Terör ve Savaş Üçgeninde Siber Dünya*, 47.
[661] "Prague Summit Declaration," North Atlantic Treaty Organization, E.T.: 4 Ekim 2018, url: https://www.nato.int/cps/en/natohq/official_texts_19552.htm.
[662] Keleştemur, *Siber İstihbarat*, 193.
[663] "Bucharest Summit Declaration," North Atlantic Treaty Organization, E.T.: 4 Ekim 2018, url: https://www.nato.int/cps/en/natolive/official_texts_8443.htm?mode=pressrelease.

Savunma Yönetimi Otoritesi (Cyber Defense Management Authority) kurulmuştur. Siber savunma çalışmaları için bir merkez oluşturma ve hareket kabiliyetini güçlendirme hedeflenmiştir.[664] Ayrıca, 14 Mayıs 2008'de, Estonya Tallinn'de, Siber Savunma İşbirliği Mükemmeliyet Merkezi (CCD COE-Cooperative Cyber Defence Center of Excellence) kurulmuştur. 2009'da ilk siber güvenlik konferansını düzenleyerek, siber alanda teknoloji ve çatışma konularında araştırmalara başlamıştır. Görevleri; siber alanda ittifak amaçlı kavram ve doktrinler üretmek, eğitim, araştırma, geliştirmede bulunmak, yaşanmış siber olaylar üzerinde çalışarak, bir saldırıda istendiği takdirde tavsiye verebilmektir.[665] CCD COE; 2013 yılında, siber savaşta uygulanabilecek, uluslararası bir hukuk yasası anlamını taşıyabilecek, siber savaşta kılavuz biçimindeki Tallinn El Kitabı'nı yayımlanmıştır.[666] 2018 yılındaysa, CCD COE, NATO içerisinde siber savunma alanında eğitim ve koordinasyondan sorumludur.[667] Bu çalışmalar, siber alanda atılan önemli adımlardandır. Siber savunma için bir merkez ve kılavuz ortaya çıkması, siber alanda, uluslararası sistem üzerinde büyük bir adım atıldığını gösterir. Ancak, hızla ilerleyen teknoloji, siber alanın tahmin edilemezliği, bazı çalışmaların yetersiz kalmasına sebep olmuştur.

19-20 Kasım 2010 yılında Lizbon Zirvesi[668] yapılmıştır. Yeni stratejik konseptler üretilmiştir. Ulusal bir yasadışı faaliyette, ittifak güvenliği tehdit edileceğinden, siber saldırıların kritik bir altyapıya yapılması, zararın pahalı olacağını gösterir. Ayrıca zirvede; teknolojinin NATO'ya ait operasyonları, askeri planları etkileyebilecek küresel sonuçları olacağından söz edilmiştir.[669] 20-21 Mayıs 2012'de, Şikago Zirvesi[670] yapılmıştır. Lizbon Zirvesinde bahsedilenlerle beraber, yeni birçok stratejik konseptten söz edilmiştir. Diğer konular dışında, siber alanda belirli kararlar alınmıştır. "Siber Savunma Konsepti, Politika ve Eylem Planı (Cyber Defence Concept, Policy, and Action Plan)"'ndan söz edilmiş, kabul edilip, uygulanmaya konmuştur.[671] 4-5 Eylül 2014 yılında, Wales

[664] Bıçakçı, *21. Yüzyılda Siber Güvenlik*, 36-37.
[665] "About Us," CCDCOE, E.T.: 22 Ağustos 2019, url: https://ccdcoe.org/about-us/.
[666] Steed, "The Strategic Implications Of Cyber Warfare," 85.
[667] "About Us," CCDCOE.
[668] "Lisbon Summit Declaration," North Atlantic Treaty Organization, E.T.: 5 Ekim 2018, url.: https://www.nato.int/cps/en/natolive/official_texts_68828.htm
[669] Yiğittepe, *NATO Güvenlik Politikaları ve Terörle Mücadele Stratejileri*, 95-96.
[670] "Chicago Summit Declaration," North Atlantic Treaty Organization, E.T.: 5 Ekim 2018, url.: https://www.nato.int/cps/ra/natohq/official_texts_87593.htm?selectedLocale=en.
[671] Yiğittepe, *NATO Güvenlik Politikaları ve Terörle Mücadele Stratejileri*, 96-98.

(Newport) Zirvesi[672] yapılmıştır. Zirvede; siber alanda yeteneklerin geliştirilmeye devam edileceği, ittifak için ulusal şartlarda, siber güvenliğin arttırılıp, esnek ve korunaklı hale getirileceğinden söz edilmiştir.[673] Siber alan için bir politika ve eylem planı geliştirilmiştir. Siber alanın uluslararası hukuk içerisinde bulunduğu, siber savunmanın, kolektif savunmanın bir parçası olduğundan söz edilmiştir. Ortaklık kurulması ihtimalinde, eğitim ve siber alanda yapılacak çalışmaların öneminden bahsedilmiştir.[674] Yapılan zirvelerde, alanda ciddi çalışmalar yapılması gerekliliği ortaya çıkmıştır. Siber alanda ortaya çıkabilecek bir tehdidin, sadece teknoloji açısından değil, farklı konularda da büyük zararlar verebileceği görülmüştür. Bu zararlar; bazı alanlarda ortaklığı bulunan devletler için kolektif problem yaratacağı, çalışmaların bu yönde olması gerektiğini gösterir. Artık, siber tehditler, uluslararası hukuk üzerinden söz edilecek bir yapıya dönüşmüştür.

8-9 Temmuz 2016'da Varşova Zirvesi[675] yapılmıştır. Bu zirvede; terör örgütleri üzerinden çalışmalar yürütülmesi kararı verilmiştir. Ayrıca, siber eğitim, kapasitelerin geliştirilmesi, elektronik erken uyarı uçakları gibi çalışmalardan söz edilmiştir. Müttefik devletlerle siber savunma üzerine iş birliği, savunmanın güçlendirilmesi, ulusal siber savunmayı güçlendirmek amacıyla savunmaya dahil edilmesinden bahsedilmiştir.[676] Siber alanı, normal şartlarda kara, deniz, havanın savunulduğu gibi, aynı önemle savunulması gereken, operasyonel bir alan olarak tanımlamıştır.[677] 11-12 Temmuz 2018'deki Brüksel Zirvesi (Brussels Summit Declaration), daha çok Rusya Federasyonu ile olan ilişkiler üzerine yapılmıştır. Siber alanda tehditlerin; genel anlamda daha zorlayıcı, yıkıcı, karmaşık hale geldiğinden söz edilmiştir. Savunma amaçlı; hibrid, tehditlere karşı; caydırıcılık, savunma, mücadele yöntemleri geliştirileceğinden bahsedilmiştir. Zirvede, siber alanda, uluslararası güven ve barışın sağlanmasıyla, istikrar için siber çalışmalara devam edileceğinden söz edilmiştir.[678] Siber alanın, kontrol edilemeyecek gelişmeler ortaya çıkarması, kullanım alanlarının yayılması, yapılan çalışmaların

[672] "Wales Summit Declaration," North Atlantic Treaty Organization, E.T.: 5 Ekim 2018, url.: https://www.nato.int/cps/ic/natohq/official_texts_112964.htm.
[673] Yiğittepe, *NATO Güvenlik Politikaları ve Terörle Mücadele Stratejileri,* 100-101.
[674] Leitner vd., "Situational Awareness for Strategic Decision Making on a National Level," 232.
[675] "Warsaw Summit Communiqué," North Atlantic Treaty Organization, E.T.: 5 Ekim 2018, url.: https://www.nato.int/cps/su/natohq/official_texts_133169.htm.
[676] Yiğittepe, *NATO Güvenlik Politikaları ve Terörle Mücadele Stratejileri*, 101-103.
[677] Leitner vd., "Situational Awareness for Strategic Decision Making on a National Level," 233.
[678] "Brussels Summit Declaration," North Atlantic Treaty Organization, E.T.: 6 Ekim 2018, url: https://www.nato.int/cps/ic/natohq/official_texts_156624.htm.

sonuçlarının problem çıkarabileceği bir sisteme dönüştüğünü gösterir. NATO'nun bu çalışmaları; siber tehditlerin en az zararla atlatılması, NATO üyeleri için fiziksel bir savaştan farklı görülmemeye başlamasından dolayı yapılmıştır. Siber alanın özellikleri sebebiyle; NATO'nun alan içeriği, kendi üyelerini kapsayacak biçimde hareket etmesi, bazı konularda sorunlar ortaya çıkartacaktır. Eğitimler ve çalışmalar, kendi üyeleri içerisinde sınırlı kalacağından, olumlu ve olumsuz yansımaları da sadece kendi içerisinde kalacaktır. Aynı zamanda, NATO'nun kurulma amacından dolayı çalıştığı alan bellidir. Bu sebeple, siber alanda yapılan çalışmalar genellikle bu yönde olmaktadır.

NATO'nun çalışmaları sadece zirvelerle sınırlı kalmamıştır. NATO, kuruluşunda savunmayı amaç edinmiş bir yapıdır. Siber alan için ayrıca birimler oluşturarak, savunma ve koruma amaçlı çalışmalar yürütmüştür. NATO Siber Savunma Komitesi (NATO Cyber Defense Committee-CDC), siber savunmayla alakalı en üst seviyedeki teşkilattır. NATO Yeni Gelişen Güvenlik Sorunları Bölümü (NATO Emerging Security Challenges Division-ESCD); 1 Ağustos 2010 yılında kurulmuştur. Yeni oluşan güvenlik tehdit ve sorunları karşısında, NATO karargâhlarının yeteneklerini birleştirmeyi amaçlamıştır. NATO Siber Savunma Yönetim Kurulu (NATO Cyber Defence Management Board-CDMB); NATO Siber Savunma Politikasının uygulanması, üyelerden herhangi birine gelecek siber saldırıda en uygun önlemin alınmasında görevlidir. NATO Bilgisayar Olaylarına Müdahale Yeteneği (NATO Computer Incident Response Capability-NCIRC); 2012 yılında kurulmuştur. NATO Muharebe ve Bilgi Teşkilatı (NATO Communications and Information Agency-NCIA) altında görev yapmakta olup, siber saldırılara karşı savunma ve korumadan sorumlu birimdir.[679] Aynı zamanda, bir toplu savunmada cevap verecek önemli birimlerdendir.[680]

İtalya'da bulunan Latina kentinde, NATO İletişim ve Bilgi Sistemleri Okulu (NATO Communications and Information Systems School-NCISS) bulunmaktadır. Bu okulda; NATO bilgi ve iletişim sistemleri üzerine, üyelik fark etmeksizin, personellere eğitim vermektedir. Almanya'nın Oberammergau'da bulunan NATO Okulu; strateji, operasyon, politika, prosedürleri destek amaçlı siber savunma eğitimi vermektedir. İtalya'nın Roma şehrinde; NATO Savunma

[679] Çiftçi, *Her Yönüyle Siber Savaş*, 61.
[680] Leitner vd., "Situational Awareness for Strategic Decision Making on a National Level," 233.

Koleji; siyasi ve askeri konular üzerine, stratejik eğitimler vermektedir.[681] Bu çalışmalar; uluslararası alanda bilinçlenme ve güvenlik amaçlıdır. NATO, üye devletleri savunma ve koruma çalışmalar yapmıştır. Eğitim olaraksa, uluslararası çalışmalara açık olduğunu göstermiştir. Ancak yeterli değildir. İleride ortaya çıkabilecek olaylar, devlet kapasiteleri, devletlerin kendi aralarındaki ilişki; siber yeteneklerine göre tartışılabilecek bir konumdadır. NATO altında bir iş birliği düşüncesi vardır. Ancak, uluslararası alanda tüm devletleri bağlayacak bir siber kural henüz tam olarak ortaya çıkmamıştır. Siber alanın günümüzde değişkenler barındırması, yapılan çalışmaların gün geçtikçe eski kalmasına sebep olmaktadır.

Genel anlamda NATO; siber alanda çeşitli çalışmalar yapmıştır. Özellikle devletlerin savunmalarına odaklı yürütülen çalışmalara daha çok dikkat edilmesi sağlamıştır. NATO'nun yürüttüğü çalışmalar; siber bir savaşın önüne geçilmesi, ortaya çıkmasındaysa; savunmada birlik olmayı hedeflemiştir. Ancak devletler belirli konularda söylenenlere uymak zorunda değildir. NATO, üye devletleri, kendi içlerinde, bazı olaylar karşısında birbirlerine bağlı hareket etmelerini sağlamıştır. Ancak, her devlet için aynı bağlılık geçerli değildir. Uluslararası sistem, bazı konularda, değişkenlik göstermektedir. Siber alan, hem ani hem hızlı gelişip değişen bir yapıdadır. Alanda ortaya çıkan tehditlerin sonuçları çok ciddiye alınmıyor gibi görünse bile, bu her dönem, her olayda aynı şekilde gitmeyecektir. Bu sebeple; bazı devlet ve uluslararası örgütler, siber alanı ciddi bir biçimde politika ve çalışmalarına dâhil etmiştir. Benzer çalışmalar yapan başka örgütler de vardır. Bu örgütlerden önemli bir tanesi; Birleşmiş Milletlerdir. Siber alandaki yeri ve önemini anlamak için, Birleşmiş Milletler'in siber alan için yaptığı çalışmalarından söz etmek gerekir.

2.2.3. Birleşmiş Milletler

Uluslararası alanda örgütler çeşitli amaçlarla çalışmalar yapmıştır. Günümüzde evrensel güvenlik üzerine pek çok konuda, birçok devletin katılımıyla, etkinliği tartışmalı olmasına rağmen, bu konuda en önemli faaliyetleri gösteren tek yapılanma Birleşmiş Milletler'dir.[682] Uluslararası güvenlik ve barış amacıyla kurulan Birleşmiş Milletler, siber alanda aynı biçimde çalışmalar

[681] Leitner vd., "Situational Awareness for Strategic Decision Making on a National Level," 233.
[682] Dedeoğlu, *Uluslararası Güvenlik ve Strateji*, 307.

yapmaktadır.[683] Saldırgan bir yöntemdense, barışçıl bir güvenlik yöntemi izlenmesi taraftarı olmuştur. Devletlerarası saldırı ihtimalinde, dünya üzerinde başvurulacak esas kurum; Birleşmiş Milletlerdir. Ancak, uluslararası düzeyde ilk çalışmalardan birini yapan; NATO Siber Savunma Mülkiyet Merkezi olmuştur. Tallinn El Kitabı'yla olabilecek siber savaş üzerine, belirlenmiş hukuki sistemlerden söz edilmiştir.[684] Ancak yapılan bu çalışmalar tek bir sistemin elinden çıkmıştır. Fakat pek çok yapılanma, siber alanda farklı çalışmalar yürütmüştür.

Birleşmiş Milletler, siber alanla ilgili çalışmalarına 1980'li yıllarda başlamıştır. 1985 yılında, Birleşmiş Milletler ilk defa, bilgisayar suçları üzerine çalışma yapmıştır. "7. Suçtan Korunma ve Suçluların Rehabilitasyonu Kongresi[685]" isimli kongre, sonrasında "Milan Eylem Planı (E/AC.57/1988/16)" ile bilgisayar suçlarından söz etmiştir.[686] Bu kongrenin 12.'si 1990 yılında düzenlenmiştir. Bilgisayar suçları üzerine çözüm taslakları sunulmuştur. Bu taslaklar 13. Toplantıda kabul edilmiştir. Bu sayede, Birleşmiş Milletler, kendi içerisinde, bilişim suçları üzerine çalışmalar yapmaya başlamıştır.[687] Siber alanda ilk yapılan çalışmalar; bilgisayar ve bilişim üzerine olmuştur. 1980'li yıllarda çalışmalara başlanmış olması, kendi gibi birçok uluslararası örgütten, bazı konularda ileride hareket ettiğini göstermiştir.

2000 yılında, "10. Birleşmiş Milletler Suçları Önleme ve Suçlulara Muamele Kongresi (the Tenth United Nations Congress on Crime Prevention and the Treatment of Offenders)[688]", Avusturya'nın Viyana kentinde yapılmıştır. Siber güvenlik, bilgi sistemlerine karşı gelebilecek tehditlerin önlenmesi, karşılık verilmesi, uluslararası koordinasyonun öneminden söz edilmiştir. Ayrıca, suçluların etkili ve hızlı bir biçimde soruşturularak, ulusal kanun uygulayıcıların aralarında adli ve teknik olarak anlaşmalarının öneminden bahsedilmiştir. Aynı

[683] Keleştemur, *Siber İstihbarat*, 436.
[684] Ünal, *Siber Güvenlik ve Elektronik Bileşenleri*, 123-124.
[685] United Nations Digital Library, *Seventh United Nations Congress on the Prevention of Crime and the Treatment of Offenders* (Milan: 1985), E.T.: 23 Ağustos 2019, url: https://digitallibrary.un.org/record/114498?ln=en.
[686] Çakmak ve Altunok, *Suç, Terör ve Savaş Üçgeninde Siber Dünya*, 177.
[687] Keleştemur, *Siber İstihbarat*, 437.
[688] "Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders," Birleşmiş Milletler, E.T.: 10 Ekim 2018, url: https://digitallibrary.un.org/record/432663/files/A_CONF.187_15-EN.pdf.

zamanda, siber terörizmin önüne geçmek için eğitim programları önerilmiştir.[689] Siber alan bu dönemde güçlenmeye başlamıştır. Bu sebeple; alanla ilgili eğitim ve yaptırımlar için çalışmalar önemlidir. Siber suçlar için yaptırımlarda, uluslararası alan ve devletlerin kendi sistemlerinde problemler oluşabileceği için, buna bir çözüm bulunabilmesi amaçlı bir adımlar atılmıştır.

2008 yılında, Dünya Siber Güvenlik Zirvesi, sonrasında, Siber Tehditlere Karşı Uluslararası Çok Uluslu Ortaklık (International Multiliteral Partnership Against Cyber Threats-IMPACT) isimli pakt yapılmıştır. İnternetin faydaları beraberinde getirdiği tehditlere karşı küresel bir çözüm bulmak için International Telecommunications Union (ITU) tarafından hazırlanmıştır. 2009 yılında faaliyete geçmiştir.[690] Amacı; siber tehditler karşısında pek çok devletin mücadele yeteneklerini geliştirmesi için bir araya getirmektir. Merkez yeri Malezya olan kurumun, siber alanda tehditlere karşı ilk özel-kamu iş birliği olduğu bilinmektedir.[691] Yapılan bu iş birliği, siber alan için önemli bir adımdır. Aynı zamanda, yetenek geliştirme, tehditlere karşı hazırlıklı olma amacı taşır.

29 Haziran 2012'de, Birleşmiş Milletler İnsan Hakları Komisyonu (United Nations Human Rights Council); insanların temel haklarının birebir siber alanda da geçerli olduğunu kabul edilmiştir.[692] Bir kişinin temel hakları her alanda geçerli olmalıdır. Yapılan bu çalışma, siber alanda temel hakların geçerli olduğunu ve buna göre bir yol izlenmesi gerektiğini göstermiştir. 2013 yılında, "Siber Suçlar ve Siber Güvenlik Eylemi (Action On Cybercrime And Cyber Security)" raporu hazırlanmıştır. Yapılan görüşmede, siber suç ve güvenliğinin Birleşmiş Milletler üzerindeki etkileri tartışılarak, bu konudaki teknoloji ve politikalar ele alınmıştır. Burada; BM Siber Suçlar ve Siber Güvenlik Grubu(UN Group on Cybercrime and Cyber Security)'nun kurulması kabul edilmiştir. Aynı zamanda belirlenmesi gereken bir politika ihtiyacından söz edilmiş, ancak bunun insan haklarını koruyacak biçimde olmasından bahsedilmiştir.[693] 2015 yılında "Uluslararası Güvenlik Bağlamında Bilgi ve Telekomünikasyon Alanındaki

[689] Süleyman Özeren, "Cyberterrorism and International Cooperation: General Overview of the Available Mechanisms to Facilitate an Overwhelming Task," içinde *Responses to Cyber Terrorism,* edit. Centre of Excellence Defence Against Terrorism (Ankara: IOS Yayınları, 2008), 81.
[690] "Making an IMPACT on Cybersecurity," International Telecommunications Union, E.T.: 23 Ağustos 2019, url: https://www.itu.int/net/itunews/issues/2009/08/22.aspx.
[691] Çiftçi, *Her Yönüyle Siber Savaş*, 124.
[692] Çiftçi, *Her Yönüyle Siber Savaş*, 123.
[693] "Action on Cybercrime and Cyber Security," United Nations System, E.T.: 23 Ağustos 2019, url: https://www.unsystem.org/content/action-cybercrime-and-cyber-security.

Gelişmelerle İlgili Hükümet Uzmanları Grubu Raporu (Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security)" yayımlanmıştır. Raporda; Bilgi ve iletişim teknolojileri üzerine riskler ve tehditler incelenmiştir. Aynı zamanda, terör ve suç amaçlı kullanımlarda ceza uygulayabilmek için bilgi alışverişi ve yardımlaşma çağrısı yapmıştır.[694]

2019 yılında, Birleşmiş Milletler Silahsızlanma Araştırma Enstitüsü (United Nations Institute for Disarmament Research-UNIDIR), Siber Politika Portal[695]'ını oluşturmuştur. Bir sitede, bütün üyelerin, kısa ve kapsamlı siber güvenlik profil ve kuruluşlarını toplamışlardır.[696] Ancak, portalın bilgi içeriği sınırlı olması sebebiyle, geliştirilmesi gerekmektedir. 2019 yılına kadar, Birleşmiş Milletler, siber alan için önemli adımlar atmış, bunun için uzman grupları belirlemiştir. Ancak, yapılan çalışmaları arttırmak gerektiği görülmüştür. Güvenlik üzerine ayrıca çalışmalar yapan Birleşmiş Milletler, siber alanı kapsayan belirli birlikler oluşturduğu da bilinmektedir.

Birleşmiş Milletler adı altında siber alanla bağlantılı birlikler bulunmaktadır. Uluslararası Telekomünikasyon Birliği (International Telecommunication Union- ITU); ulusal sistemlerin birbiriyle bağlantısını kurmak amaçlı, ağ operatörleri tarafından kurulmuştur. Devletlerarası ara bağlantıların düzenlenmesi, sistemler üzerinden iletişimi sağlama görevleri bulunmaktadır. Sanayi ve hükümetlerin ortak bulunduğu Birleşmiş Milletler organizasyonu, 2008 Nisan ayı sonrasında, Bilgisayar Teknolojileri üzerine iş birliği ve eğitimi teşvik etmiştir.[697] Birliğin en önemli çalışması; siber alanda ciddi bir yeri olan, iletişimin kurulmasındaki problemlerin önüne geçmektir. İletişim, ağlar üzerinden sağlandığı için, siber alan, özellikle üzerinde çalışılıp, eğitiminin sağlanması gereken bir yapıya dönüşmüştür. Bunun için çalışmalar yapılmıştır. İletişim alanındaki suçlar için, çalışmalar içerisine siber alan dâhil edilmiştir.

---

[694] United Nations General Assembly, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security,* United Nations General Assembly (2015), E.T.: 23 Ağustos 2019, url: https://undocs.org/A/70/174.

[695] Cyber Policy Portal, E.T.: 23 Ağustos 2019, url: https://cyberpolicyportal.org/en/.

[696] "UNIDIR Launches Cyber Policy Portal and Announces Date, 6 June 2019, for its Cyber Stability Conference 2019 in New York," United Nations Office for Disarmament Affairs, E.T.: 23 Ağustos 2019, url: https://www.un.org/disarmament/update/unidir-launches-cyber-policy-portal-and-announces-date-6-june-2019-for-its-cyber-stability-conference-2019-in-new-york/.

[697] "International Intergovernmental Organizations," içinde *Global Initiatives to Secure Cyberspace*, ed. Seymour Goodman ve Michael Portnoy (Amerika: Springer, 2009), 11.

Birleşmiş Milletler Uyuşturucu ve Suç Dairesi (United Nations Office on Drugs and Crime- UNODC); 1997 yılında kurulmuştur. Yasadışı uyuşturucu kontrolü, uluslararası terörizm ve suç önleme çalışmalarına yardım amaçlı kurulup, siber alanda suç yasası, eğitim, kolluk kuvvetlerini içermektedir.[698] Siber alan her yapının içerisine dağılmıştır. Bu sebeple; bazı alanlarda çalışmalara faklı bir önem verilmiştir. Aynı zamanda uluslararası alanda yapılan siber suçlara karşı önlem almak için bu birimde çalışmalar yapılmaktadır.

Kurulduğunda farklı bir amacı bulunan Birleşmiş Milletler Silahsızlanma Dairesi (United Nations Office for Disarmament Affairs- UNODA); 1982 yılında, silahsızlanma, nükleer silahların yayılmasına engel olmak amaçlı oluşturulmuştur. Değişen şartlar ve teknolojiyle son yıllarda, bilgi savaşı ve terörizme odaklanmış, siber alandaki tehditleri kabul etmiştir. Siber silah kontrolü ve bilgi boşluğunu doldurmak için halkı bilinçlendirme çalışmaları yapmıştır.[699] Siber alan ilk yıllara göre, daha ciddiye alınmaya başlanmıştır. Ancak yeterli olmamış, daha çok çalışmaya ihtiyaç duymuştur. Yapılan bu çalışmalarda dikkat çeken nokta; bilinçlenmeye önem verilmesidir. Aynı zamanda, siber alandaki tehditler daha tehlikeli boyutlara ulaşmaya başlamıştır. Özellikle uluslararası alanda, devletlerin birbirine karşı kullanacağı önemli bir sistem şekline gelmiştir. Tehditler hızlı bir biçimde artarken, devletler ve örgütlerin aynı şekilde güvenlik çalışmaları devam etmektedir. Ancak, her devlet ya da örgüt kendi çıkarları ölçüsünde çalışmalarını hazırlamaktadır.

Birleşmiş Milletler, devletlerin bir arada bulunduğu bir topluluktur. Ancak, devletleri bağlayıcı bir örgüt değildir. Diğer topluluklar gibi Birleşmiş Milletler, çalışmalarında daha çok öneri düzeyinde kalmaktadır. Birleşmiş Milletlerden bir konu üzerine yardım istendiğinde önemli adımlar atmaktadır. Siber alanda çalışmalarında, daha çok eğitim ve birlikte hareket etme üzerine ilerlemiştir. Kendisi gibi önemli olan ve siber alanda çalışma yapan örgütlerden biriyse; Avrupa Konseyidir. Önemli çalışmalar yürüten bu örgüt, daha iyi anlaşılması için incelenmelidir.

[698] "International Intergovernmental Organizations," 20.
[699] "International Intergovernmental Organizations," 21.

2.2.4. Avrupa Konseyi

Siber alanda çalışmalar yapan örgütlerden biri Avrupa Konseyi'dir. Siber alanda bilinen en kapsamlı belgelerden birini Avrupa Konseyi oluşturmuştur. 1970'lerde, kişilerin özel yaşamına zarar gelmemesi için; elektronik verilerin korunması amacıyla gelişmeler başlamıştır. 28 Ocak 1981 yılında, "Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması[700]" isimli sözleşmeyle önemli bir adım atılmıştır.[701] Bireyler için yapılan bu düzenleme, uluslararası alan ve siber alanda önemli bir adımdır. Avrupa Konseyi, siber alanla alakalı çalışmalarına 1970'li yıllarda başlanmıştır. Teknoloji ve siber alanın değişmeleriyle, Avrupa Konseyi çalışmaları da ilerlemiştir.

23 Kasım 2001'de başlayıp, 1 Temmuz 2004'te yürürlüğe giren "Avrupa Konseyi Sanal Ortamda İşlenen Suçlar Sözleşmesi[702]" Avrupa Konseyi bünyesinde, ilk resmi siber suçlar üzerine hazırlanmış belgedir.[703] Sözleşmenin amacı; toplumları, ortak bir suç politikasıyla, siber suçlardan korumaktır.[704] Bilgisayar ağ ve elektronik bileşenlerinin belirli suçlarda kullanılma, belirli kanıtların bu alanda depolanma ihtimali vardır. Aynı zamanda, siber suçlarla mücadelede, özel sektör ve devlet arasında bilgi teknolojileri, iş birliğinin geliştirilmesinin önemi bu sözleşmede söz edilmiştir.[705] Bu çalışma, siber suç odaklıdır. Toplumları koruma amaçlı adımlar atılması, özel sektörle devletlerin iş birliğinin öneminden söz edilmiştir. Ancak, siber tehditler sadece siber suçlarla kısıtlı değildir.

Terörle Mücadele Uzmanlar Komitesi (Committee of Experts on Terrorism- CODEXTER); uluslararası alanda, terörizm ve hukuk analizi üzerine çalışmalar yapmıştır. Ayrıca, internetin terör amaçlı kullanımı üzerine çalışmalarda bulunmuştur. Avrupa Konseyi, öneri olarak; ulusal hukukların uyumlaştırılması, iş birliği, altyapıların korunması konularının siber alanda

[700] "Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data," Avrupa Konseyi, E.T.: 15 Ekim 2018, url: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680078b37.

[701] Çakmak ve Altunok, *Suç, Terör ve Savaş Üçgeninde Siber Dünya*, 172.

[702] "Convention on Cybercrime," Avrupa Konseyi, E.T.: 15 Ekim 2018, url.: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680081561.

[703] Ünal, *Siber Güvenlik ve Elektronik Bileşenleri*, 125.

[704] Çakmak ve Altunok, *Suç, Terör ve Savaş Üçgeninde Siber Dünya*, 148.

[705] Özeren, "Cyberterrorism and International Cooperation: General Overview of the Available Mechanisms to Facilitate an Overwhelming Task," 78-79.

önleyici bir faktör olabileceğinden söz etmiştir.[706] Çözüm olarak; iş birliğinin faydalı olacağı görüşü vardır. Önemli altyapıların kullanılması, hukuksal uyumlaşma, atılan adımlarda kolaylık sağlamıştır. Ancak, 2003 yılında oluşturulan bu komite, 2017 yılında sona ermiştir. 2018 yılında, Avrupa Konseyi Terörle Mücadele Komitesi (Council of Europe Counter-Terrorism Committee-CDCT)'ne dönüşmüştür.[707] Siber alandaki suç ve tehditler üzerine ayrıca belirli sözleşmeler yapılmıştır.

"Küresel Siber Suç Projesi Aşama I Siber Suçlar Sözleşmesi'nin" uygulanmasında önemli bir rolü vardır. Bu proje, Eylül 2006 yılında başlamıştır. 2009 yılı Şubat ayında tamamlanıp, yasal süreçleri gözden geçirme, eğitim amaçlı çalıştaylar, küresel konferans ve etkinliklerin gerçekleştirilmesinde katkı sağlamıştır. Aynı zamanda, 'Octopus' programının başlangıcı buradan olmuştur.[708] Octopus; Siber Suç Topluluğu, Avrupa Konseyi içerisinde; elektronik kanıtlar, siber suçlarla ilgili bilgi paylaşımı, iş birliğini içeren bir platformdur. Ayrıca, eğitimler, politikalar, siber suçla alakalı mevzuatların burada bir araya getirildiği bilinmektedir.[709] 2007 yılında, Octopus Konferansı ile çalışmalarına başlanmıştır. İşbirliğini güçlendirmek amacıyla, farklı yerlerden, birçok siber suç uzmanını topluluk adı altında bir araya getirmeyi başarmıştır.[710] Bu çalışma, siber suçlar üzerine önemli adımlar atılmasını sağlamıştır. Eğitim ve politikaların belirlenmesi, özellikle günümüzdeki çalışmalarda önemli olmuştur. Günümüzde büyük problemlerden biri; uyumlu çalışma, politikaların belirlenmesidir. Bunun üzerine yapılan çalışmalar, özellikle siber alanda iş birliğini içermektedir.

2011 yılı 8 Kasım tarihinde, Avrupa Birliği ve Avrupa Konseyi siber suçlara karşı bölgesel iş birliği yaparak " Madde 15 Budapeşte Siber Suçlar Konvansiyonu Kapsamındaki Koşullar ve Korunmalar (Article 15 Conditions and Safeguards under the Budapest Convention on Cybercrime)," raporunu

[706] Eneken TIKK ve Reet OORN, "Legal and Policy Evaluation: International Coordination of Prosecution and Prevention of Cyber Terrorism," içinde *Responses to Cyber Terrorism,* edit. Centre of Excellence Defence Against Terrorism (Ankara: IOS Yayınları, 2008), 90-91.
[707] "Commitee of Experts on Terrorism (2003-2017)," Avrupa Konseyi, E.T.: 24 Ağustos 2019, url: https://www.coe.int/en/web/counter-terrorism/codexter.
[708] "Global Project on Cybercrime Phase I," Avrupa Konseyi, E.T.: 16 Ekim 2018, url: https://www.coe.int/en/web/cybercrime/global-project-phase-i.
[709] "Octopus Cybercrime Community," Avrupa Konseyi, E.T.: 16 Ekim 2018, url.: https://www.coe.int/en/web/octopus/home.
[710] Jonathan Clough, "A World Of Difference: The Budapest Convention on Cybercrime and The Challenges Of Harmonisation," *Monash Üniversitesi Hukuk Dergisi* 40-3 (2014): 735-736, E.T.: 16 Ekim 2018, url: https://www.monash.edu/__data/assets/pdf_file/0019/232525/clough.pdf.

hazırlamıştır. Amaç; siber suçların araştırılması ve kanıt toplanması için yetkilendirilmeyi içermektedir. Aynı zamanda, bu yetkiyle insan haklarının korunarak ilerlenmesinden söz edilmiştir. Siber suç konusunda kapasite geliştirilirken, insan haklarına etki edilmeden yapılması için bir ortak çalışma şeklinde hazırlanmıştır. Devletlerin belirledikleri çalışmalara ayrıca ilgi çekmek, uluslararası bir anlaşmanın neden düzenlenemediğine, bunun iç hukuk ve uygulamalara bırakılıp desteklenmesi gerektiğine dikkat çekilmiştir.[711]

2013 yılında Avrupa Birliği ve Avrupa Konseyi ortak projesi olan GLACY + (Siber Suçlarda Küresel Eylem-Global Action on Cybercrime) oluşturulmuştur. Amacı; devletlerin siber suç ve elektronik yasalarını uygularken kapasitelerini güçlendirip, uluslararası işbirliklerini geliştirmektir. Ayrıca, siber suç ve güvenlik üzerine, politika ve stratejiye teşvik etmeyi amaçlar.[712] Ekim 2013 tarihinde, Avrupa Konseyi Bakanlar Komitesi, Avrupa Konseyi Siber Suçlar Program Ofisi'ni (Cybercrime Programme Office of the Council of Europe - C-PROC) kurulmaya karar verilmiş, 2014 yılında yürürlüğe girmiştir. Avrupa Konseyi, burada devletlere, siber tehditlere karşı yasal sistem kapasitelerini güçlendirerek, küresel teknik yardımı vermektedir. Aynı zamanda, iş birliğiyle hukuk kuralları ve insan haklarıyla uyumlu biçimde siber suç mevzuatlarını güçlendirmeye yardım eder.[713]

2016 yılındaysa, "Siber Suçlar Konvansiyon Komitesi (The Cybercrime Convention Committee-T-CY)" kurulmuştur. Budapeşte Siber Suçlar Konvansiyonu taraf devletlerini temsil etmektedir. Sözleşmenin 46. maddesine dayanarak, sözleşmenin etkili bir şekilde kullanılmasını ve uygulanmasını, bilgi alışverişini ve gelecekteki değişikliklerin dikkate alınmasını kolaylaştırmayı amaçlamaktadır.[714] 2019 yılı Kasım ayında, siber suçlar üzerine Octopus Konferansı yapılacaktır. Konferansta; verilerin korunması ve cezai sistemdeki problemler, siber suçlar ve e-kanıtlar üzerine iş birliğiyle kapasite geliştirme ve

[711] Avrupa Konseyi, *Article 15 Conditions and Safeguards under the Budapest Convention on Cybercrime* (Fransa: Kasım 2011), E.T.: 25 Ağustos 2019, url: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802f2464.

[712] "Global Action on Cybercrime Extended (GLACY +)," Avrupa Konseyi, E.T.: 25 Ağustos 2019, url: https://www.coe.int/en/web/cybercrime/glacyplus.

[713] "Cybercrime Programme Office (C-CPOC)," Avrupa Konseyi, E.T.: 25 Ağustos 2019, url: https://www.coe.int/en/web/cybercrime/cybercrime-office-c-proc-.

[714] "Cybercrime Convention Committee," Avrupa Konseyi, E.T.: 25 Ağustos 2019, url: https://www.coe.int/en/web/cybercrime/tcy.

seçim müdahaleleri üzerine konuşulacaktır.[715] Günümüzde, özellikle politik açıdan, seçimlere müdahale tehditleri ortaya çıkmaya başlamıştır. Bir devletin yönetimini belirleyecek seçimlere yapılacak dışarıdan müdahale, devlet yönetiminde ve iç düzende büyük sorunlara sebep olabilmektedir. Aynı zamanda, buna benzer saldırılar, uluslararası alanda problemlere açık olunmasına sebep olur. Siber alan kullanılarak yapılan bu saldırı ve müdahaleler, gün geçtikçe devletlerarası ilişkileri olumsuz etkilemeye devam etmektedir.

Avrupa Konseyi, belirli dönemlerde, bölgesel olmak üzere; çalışmalar, konferanslar, çalıştaylar yapmaktadır. Bu programlar içerisinde; siber alanda, özellikle eğitim amaçlı çalışmalara önem verilmesi gerektiğinden söz edilmiştir. Aynı zamanda, iş birliği ve insan hakları çerçevesinde belirli düzenlemelere yardımı amaçlamışlardır. Burada; bir siber tehdit karşısında hazırlıklı olabilmek, zararı en aza indirmek için çalışmalar, daha çok caydırma amaçlı yapılmaktadır.

Günümüzde, özellikle Avrupa Birliği, Birleşmiş Milletler, NATO ve Avrupa Konseyi gibi örgütlerin yaptığı çalışmalar; bir siber savaşın fiziksel tehditlere dönüşme ihtimalinin önüne geçmeyi deneyebilir, ancak başarısı kesin değildir. Alınan önlemler, tehditlerin gerçekleşmesini önlemeye çalışsa da, yeterli değildir. Devletlerin yaptığı çalışmalar eşit düzeyde görünmektedir. Ancak bir kısmı yetersiz kalmıştır. Örgütlerin çalışmalarıysa yeterince bağlayıcı değildir. Günümüzde, siber savaşın fiziksel bir savaşa dönüşmesi, yakın tarihte olmayacak gibi düşünülmektedir. Ancak, bir anlaşmazlıkta, bunun yakınına yaklaşıldığı, geçmişte yaşanan Stuxnet gibi olaylarda görülmüştür. Bu yapılan çalışmaların, alınabilecek önlemlerin, bir savaş ihtimaline dönüşüp dönüşmemesi, devletlerin maddi güç ve imkânlarına bağlıdır. Siber savaş, istenilen bir politikanın, karşı tarafa kabul ettirilmesinde başvurulabilecek bir yöntemdir. Ancak, siber bir savaş, henüz fiziksel, büyük bir savaşa sebep olmamıştır. Bunun olasılığı bile çok büyük bir tehlike taşımaktadır. Siber alanda olabilecek bir siber savaş ve onun daha ciddi boyutlara tırmanmaması için, bunun önüne geçilmesi amaçlı yeni çalışmalar olmalıdır. Ayrıca, bu olasılığın ortaya çıkmaması için, farklı yöntemler eklenebileceğini yeni bir başlık altında tartışmak gerekir.

[715] Avrupa Konseyi, *Octopus Conference 2019* (Fransa: Mayıs 2019), E.T.: 25 Ağustos 2019, url: https://rm.coe.int/octopus-conference-2019-outline/1680948eba.

2.3. BÖLÜM DEĞERLENDİRMESİ

Siber alanda, ilk bölümde söz etmiş olduğumuz üzere, birçok tehdit bulunmaktadır. Bu tehditlerin uluslararası alanda yansımaları, bireyler ya da toplumlar arasındaki yansımalarından çok farklı bir boyuttadır. Siber alanın tek boyutlu bir yapı olmaması, tehditler ve önlemler için de karmaşıklaşmasına sebep olmaktadır.

Siber alanda ortaya çıkan olayların, uluslararası yansıması daha tehlikelidir. Her dönemde, özellikle; Soğuk Savaş Sonrası Dönemde, bir Üçüncü Dünya Savaşı söylemi bulunmakta, her gerginlikte bunun ortaya çıkması beklenmektedir. Bu savaş, fiziksel olarak klasik bir savaş biçimde beklenmiş, ancak gerçekleşmemiştir. Günümüzde savaşlar ekonomi gibi daha farklı yapılar üzerinden yürütülmeye başlamıştır. Siber savaşlarda yeni savaş yöntemleri içerisine dâhil edilmiştir. Uluslararası alanda siber savaşlar, özellikle güvenlik açısından, normal savaşlar kadar ciddiye alınmaya başlamıştır. Siber alan, güvenlikte daha farklı boyutlara çıkmıştır. Devlet ve örgütlerin bu alanda politika çalışmaları yapmasına sebep olmuştur.

Siber alanda pek çok devlet ve örgüt çalışmalar yürütmektedir. Devletlerin çalışmaları, örgütlere göre daha fazladır. Her devlet kendine özel politikalar belirlemektedir. Siber alan çalışmaları; ekonomik, teknolojik çalışmaların yoğunluğuna etki etmektedir. Genel anlamda ekonomisini doğru şekilde yürüten bir devlet, yeterli bilgiye sahip olduğunda, projelerinde, özellikle teknolojik anlamda sorun yaşamazlar. Ancak, ekonomik olarak yetersiz devlet, bilgiye sahip olsa bile, çalışmalarını dökebileceği bir ortamı olmadığından, daha geride kalmaktadır. Aynı zamanda, bir problemin güvenlik içerisinde değerlendirilmesi, sorunun çözülüp, üzerinde ilerlenmesinde önemlidir. Siber alanı, bir güvenlik alanı konumunda görüp görmemekse alan üzerine çalışmalarda etkili olmaktadır.

Siber alanda yapılan çalışmalar, önemli adımlar atmış bazı devletler olan; ABD, Çin Halk Cumhuriyeti, Rusya Federasyonu, Federal Almanya Cumhuriyeti, İngiltere ve Türkiye Cumhuriyeti üzerinden, örneklerle açıklanmıştır. Günümüzde siber alanda çalışmalarda bulunan farklı devletler de vardır. Ancak özellikle altı ülkeden üçü olan; ABD, Çin Halk Cumhuriyeti ve Rusya Federasyonu, siber alanda en dikkat edilmesi gereken devletlerden biridir. Bu üç devlet, siber alanda yapılan çalışmalarda en üst düzeydedir. Üçünün bu alanda en iyi olmak için birbiriyle rekabette olduğu bilinmekte, birbirlerini tehdit olarak görmektedir.

Federal Almanya Cumhuriyeti, Rusya Federasyonu gibi resmi kuruluşu yakın tarihli görünen, ancak geçmişleri daha eskiye dayanan devletlerdir. Toplumlarında eski bir yapının mirasını devam ettirmektedirler. İngiltere ve Türkiye Cumhuriyeti; siber alanda, çalışmalar yapmış önemli devletlerden ikisidir. Federal Almanya Cumhuriyeti ve İngiltere siber alanda en eski çalışmalarda bulunmuş ülkelerdendir. Türkiye Cumhuriyeti ise; bu alanda kendini göstermeye başlamış ve yapacağı çalışmalarla kendini daha çok gösterebilecek bir ülkedir. Her devletin siber alanda ayrı bir özelliği vardır. Ancak, günümüzde bütün devletlerin dâhil olduğu bir siber savaş vardır. Sadece devletler değil, örgütlerde tehdit altındadır. Devletler, sınırlı biçimde çalışmalarına devam etmektedir. Ancak, siber alan ve tehditleri, devletleri aşan bir konuma gelmiştir. Aynı zamanda, bir devlette oluşan sorun, içinde bulunduğu örgütün diğer üyelerini etkileyecek yapıdadır. Bunun için; uluslararası alanda önemli örgütler çalışmalar yapmıştır. En bilinenleri olan; Avrupa Birliği, NATO, Birleşmiş Milletler ve Avrupa Konseyi önemli çalışmalarda bulunmuştur, ancak, siber alan için yeterli değildir. Uluslararası alanda yapılan çalışmalar, bütün devletler için bağlayıcı değildir. Ayrıca, tehlike boyutu devletten devlete değişim göstermektedir.

Hem devletler hem uluslararası örgütler tarafından, siber alanda güvenlik çalışması yürütülmesine karşın, herkesi kapsayan, tam bir uzlaşı, kurallar konulamamıştır. Bu sebeple; anlaşmazlıklarda, siber alanda, tehditlerin aniden büyüme ihtimali vardır. Ekonomik savaş gibi bir savaşta, siber alanın kullanılması daha büyük tehlikelere yol açabilir. Devletler ve örgütler, politikalar üretmelerine karşın, teknoloji ve siber alanın hızlı ilerlemesi, bu politika ve çalışmaların geride kalmasına sebep olmaktadır. Uluslararası alanda, devletlerarasında bazı bağlılıklar vardır. Ancak, zayıf bir barış hâli bulunmaktadır. Bağlayıcılık olmasıysa; büyük tehditlerin önüne kısmen geçebilmektedir.

Devletlerarasındaki ilişkilerde, ekonomik bağlılık gibi bağlılıkların bulunması, bazı olayların yaşanmasına engeldir. Ekonomisini iyi tutup, dışa bağımlılığını azaltan devlet için bağlayıcı olan sadece; devletlerarası antlaşmalar, uluslararası örgülerin belirlemiş oldukları sınırlamalardır. Siber alanda başka bir boyut hâkimdir. Ekonomide kendini güçlendiren, teknolojisini en yüksek seviyeye getirebilir. Bunlara sahip olan devlet, yeterince bilgiye sahip olduğunda, siber alanda hâkim konuma gelecek, uluslararası alanda sistemin değişmesine sebep olabilecektir.

Günümüzde devletlerin pek çok yapısının siber alana dâhil olması, bu alanda ortaya çıkacak tehditlere açık olmalarını ve çok büyük zararlara yol açacağını göstermektedir. Siber alandan gelebilecek bir tehdit, altyapılarda oluşacak bir aksaklıkla, bir devlet ya da ona bağlı devletlerin işleyişlerini sekteye uğratabilecektir. Aynı zamanda, bununla, kendini koruyamayan bir devletin hükümetinin varlığında önemli olan; güvenin sarsılabileceği bir gerçektir. Bu sebeplerden; siber güvenlik, önem verilmesi gereken bir konudur. Alanın sınır aşan yapısıysa, devletler ve örgütlerin çalışmalarında kendini daha çok göstermektedir.

Siber alanın sınırları aşan bir yapı olması, hiçbir devlet ve yapının kontrolünde olmadan hareket edilmesini sağlamaktadır. Kendi içerisinde barındırdığı tehlikelerin sınırlarının olmamasıysa büyük sorunlar oluşturmaktadır. Siber alanın yapısı ve oluşacak tehditler sebebiyle; yapılan çalışma ve politikaların alanda geçerliliği, yine aktörlerin kendilerine bağlıdır.

Günümüzde devam eden siber savaşın, fiziksel alanda henüz bir yansıması olmasa da, bir savaş olduğu gerçeğini değiştirmez. Fiziksel bir savaşa dönüşmesi pek çok devlet için büyük zararlar oluşturabilecektir. Soğuk Savaş döneminde, silahlanmada yaşanan problemlerin en tehlikeli noktaya geldiğinde durup, sona ermesi, aynı şekilde siber alanda ortaya çıkabilecek bir ihtimaldir. Çünkü siber alanda güçlenen bir aktör karşısında, karşıt aktörler güçlenmeye, kendini geliştirmeye devam etmektedir. Geçmiş dönemlerde siber alan, savaşlarda bir yan unsurdur. Ancak günümüzde tamamen kendi alanı üzerinden yaşanan bir siber savaş vardır.

Siber savaş birçok devletin dâhil olduğu bir savaştır. Sadece devletlerin orduları değil, vatandaşların da dâhil olabildiği bir platformdur. Siber savaş, bu alan üzerinden, aynı şekilde devam ettiği sürece, hiçbir vatandaş fiziksel zarar görmeden, sadece ekonomik zarar alarak savaş seyreder. İnsanların ölmemesi olumlu bir sonuçken, ekonomik olarak; saldırılan devletin başka bir devlete bağımlı kalmasına sebep olacak bir sonuç doğurabilir. Bu da; daha büyük problemlere sebep olabilir. Soğuk Savaş dönemindeki silahlanma yarışında, tehlikeli silahlar ortaya çıkmış, ancak kullanılmamıştır. Fakat bu silahların bir sisteme bağlı olduğu, bu sisteminse siber alana bağlı olduğu unutulmamalıdır. Günümüzde şartlar uygun olduğu anda, bu silahların tetiklenmesine sebep olacak bir savaşın ortaya çıkma ihtimali vardır. Bunun da fiziksel bir savaşa dönüşebilme

ihtimali vardır. Ancak, henüz bu şekilde ortaya çıkmamış, bu da göz ardı edilmesine sebep olmuştur. Günümüzde önlemi alınmazsa, pek çok devlet için büyük zarar ortaya çıkacağı bilinmektedir.

Siber savaşlar çok taraflı ve çok boyutlu bir seyir içerisindedir. Ancak, en büyük tehditlerden biri; devletlerarasında yaşanan saldırıların sonucudur. Fakat siber savaşlar henüz bitmiş savaşlar olmadığından, sonuçlarından tam olarak bahsetmek zordur. Günümüzde siber savaşlar daha çok politik, ekonomik ve sistemler üzerinden ilerlemektedir. Savaşın gelişimiyse, gittikçe ilerleyen ve artan saldırılar şeklindedir. Siber savaşlarda saldırılar, devletlerin işleyiş ve ilerleyişlerine kadar etki edebilecek bir konuma gelmiştir. Aynı zamanda, Soğuk Savaş Dönemine benzer biçimde, siber alandaki sistemleri geliştirmeye ve arttırmaya yönelik çalışmalar vardır. Bu çalışmalar içerisine, sistemlere bağlı tehdit unsuru içeren silahlar da dâhildir. Devletlerin önemli altyapılarına yapılan saldırılarsa yine olası bir savaş ihtimalini tetikleyecek sebeplerdendir. Yapılan saldırılarla, bir devletin önemli belgelerine erişmek, aynı zamanda, istenilen her altyapıya zarar verebilme ihtimali olumsuz sonuçlar ortaya çıkartacaktır. Bir elektrik sistemini bozmak, günlük işleyişte aksama oluşturabilirken, bir nükleer tesisin sistemine girmek daha büyük problemlere sebep olur. Kanıtlanabilir saldırılarsa, saldırıyı yapan devlet için politik gerginliğe sebep olacaktır. Ancak, saldırının sonuçlarının şiddetine göre geri dönüşler yapılacağı bilinmektedir. Bir siber saldırının fiziksel bir savaşa dönüşmesiyse saldırıların ciddi sonuçlarından olacaktır. Uçak düşürme ya da askeri amaçla kullanılan cihazların sistemlerine girip, ateşleme gibi olaylar bir savaş çıkmasına sebep olabilmektedir. Günümüzde henüz buna yakın olaylar yaşansa da, devletler birbirlerinin güçlerini yeterince bilmedikleri için ya da siber alanın gücü günümüzde yeterli olduğu için daha ileri aşama yaşanmamıştır. Ancak, ilerleyen yıllarda, daha farklı tehditler ortaya çıkacağı görülmektedir. Siber alanın büyük sorunlara yol açacak bir yapısı olduğu bilinmektedir. Sonuçları açık ve önüne geçilecek derecede olan bir yapı, uzun süredir yapılan güvenlik çalışmalarına ihtiyaç duymaz. Ancak, siber alanda güvenlik, günümüzdeki gidişatından dolayı, ilerleyen süreçlerde daha çok önem kazanacağı bilinmektedir. Ayrıca, yapılan çalışmalar sadece devlet ya da birey düzeyinde kalmamıştır. Uluslararası düzeni etkileyecek boyuta gelmiştir. Bu, siber alandaki bir tehdidin boyutlarının daha önemli konumlara geleceğinin bir işaretidir. Ayrıca, günümüzde uluslararası alanda, devletlerin kendi arasında

gergin bir yapı bulunmaktadır. Düzenler, savaş yapıları, tehdit algılamaları, güvenlik anlayışları, eski yapıya göre büyük ölçüde değişmiştir. Değişikliklerin getirdikleri, aynı zamanda, devletlerin bazılarının sistem içerisinde güçlenmesi, her zaman bir savaş ihtimalini yanında taşır. Siber alandaki tehditler bir anda savaşa dönüşmeyecektir. Ancak, bir önlem alınmazsa, siber alanın hızlı gelişmesi, yeni tehditlerin hızlı bir biçimde ortaya çıkmasıyla, beklenenden önce bir problemin ortaya çıkması kaçınılmazdır.

Tehlikelerin farkında olan bazı devlet ve örgütler, bunların önüne geçmek için çalışmalar yürütmüştür. Ancak yeterli çalışmalar değildir. Siber alan değişip, kullananlarsa aynı şekilde kendini geliştirmektedir. Alana özel çalışmalar yapılması gerekliliği, gün geçtikçe daha çok artmaktadır. Özellikle, fiziksel savaş ihtimalinin önüne geçmek için, sadece siber alanla alakalı çalışmalar yapılarak, bazı tehditlerin önüne geçilebilecektir.

Siber alanda oluşabilecek tehditler için devletler, kendi iç düzeninde yaşanacak tehditleri çözebilecek çalışmalar yürütmektedir. Uluslararası örgütler; farklı açılardan çalışmalar yapmaktadır. Devletlerin ve örgütlerin kendi içyapıları birbiriyle tamamen uyumlu değildir. Bu sebeple; istenilen ölçüde çalışmalar yürütülememektedir. Devletlerin kendi çalışmaları dışında, uluslararası alanda başka çalışmalar yapılmaktadır. Devletlerin ve örgütlerin çalışmaları dışında, siber savaşın bir fiziksel savaşa dönüşmemesi için, önceden, uygun olan bazı adımlar atılması gerekir. Bunun önüne geçmek için, yapılması uygun olan çalışmaları, üçüncü bölümde, daha geniş açıklamak ve incelemek, doğru ve anlaşılır bir sonuca varmayı sağlayacaktır.

ÜÇÜNCÜ BÖLÜM

SİBER TEHDİTLERİN FİZİKSEL BİR SAVAŞA DÖNÜŞME OLASILIĞINA KARŞI GELİŞTİRİLEBİLECEK ÇALIŞMALAR

Uluslararası ilişkilerde, bireyden uluslararası sistemlere kadar etkide bulunan önemli kavramlardan biri güvenliktir. Güvenlik, en dar anlamda; insanın yaşam mücadelesiyle şekillenen, süreçler içerisinde biçim değiştirerek bazen zorunluluk, bazen amaç, bazen ihtiyaç şeklinde, her dönemde önemli olmuş bir alandır.[716] Asıl olan; bakış açısıdır. İçinde bulunan durumun getireceği yarar ve zararlardır. Güvenliğe tarih içerisinde farklı anlamlar yüklenerek, dönem ve aktöre göre tanımlamalar değişmiştir. Bunun altındaysa; tehditten korunma yatmaktadır.[717] Güvenliğin çeşitli tanımlamaları yapılmıştır. Çeşitli tanımların yapılmasıysa, güvenliğin genel çerçevesini belirleyerek, üzerine çalışma yapmayı sağlamıştır. Tehdidin yapısı ve değişimlerse, güvenliğin yeniden tanımlanmasına sebep olmuştur. Bu; uluslararası alanda tek bir güvenlik tanımlaması yapılmasını zorlaştırmaktadır. Ancak, genel olarak yapılan her tanım altında belirli bir amaç vardır; var olan düzeni devam ettirebilmek.

Güvenlik tanımlaması; izlenecek politikalar ve yapılacak çalışmalar için önemlidir. Güvenlik amaçlı izlenecek yöntemlerse, sorunun tanımlamasıyla oluşmaktadır. Bir sorunun boyutu belirlenmeden çözüm geliştirme, o sorunun çözümü için yetersiz kalacaktır. Bir güvenlik oluşturulması için; özellikle üç ana kavrama dikkat etmek gerekir. Bunlar; risk, tehdit ve tehlikedir. Güvenlikte üç kavram, sırasıyla ayrı önem taşımaktadır. Bir problem henüz bir risk taşıyorsa önüne geçmek daha kolaydır. Riskler, henüz tam olarak ortaya çıkmamış, ancak ortaya çıkabilecek tehdit ve tehlikeleri kapsamaktadır. En büyük özelliği; riskler, üzerinde çalışılabilecek ve yönetilebilecek bir yapıya sahip olmasıdır. Tehlikeler, bazı sorunlarda geç kalınmış ve problemlerin önemli şekillerde ortaya çıkmaya

[716] Çıtak, *Güvenlik ve İstihbarat*, 27.
[717] Yalçın, *Ulusal Güvenlik Stratejisi,* 60-61.

başlamasını kapsamaktadır. Tehditlerse; doğru yöntemlerle önüne geçilebilecek, ancak, ciddi sonuçlar doğurabilecek sorunları kapsar. Genel anlamda; devletin sahip olduğu her yapı ve değerlere gelebilecek, olumsuz sonuçlar barındıran olgu ya da olayların bütünüdür.[718] Bir sistemde, tüm devletlerin ortak tehdit gördüklerini düzenlemesi, uluslararası alanda sistemin bütününe yönelik güvenliktir. Bunun dışında, uluslararası alanda, devletin kendi iktidarı, varlığı, vatandaş refahı için yaptığı geliştirme ve korumayı da içermektedir.[719] Güvenlik her düzeyde ayrı önem taşımaktadır. Önemli olan; ortaya çıkan olaylar, gelişen teknoloji, dönemin politikasının, güvenliğin ne olması gerektiğine dair düşüncenin ortaya çıkmasındaki etkisidir. Ayrıca, neyin tehdit olduğu ve güvenli olması gerekenin ne olduğunu belirlemektir. Bu belirleme; hem güvenlik tanımını, hem güvenlik için izlenecek yola dair çalışmaların kolaylaşmasına yardımcı olmaktadır. Bu sebeple; güvende olması gerekenin, risk, tehdit ve tehlikelerin daha açık şekilde belirlenerek bir yöntem izlenmesi, sorunları çözmekte önemli olacaktır.

Güvenli olması gereken, genel anlamda korumaya ihtiyaç duyulan hassas yapılardır. Özellikle yeni ortaya çıkan yapılar, devletin ihtiyaç duyduğu önemli sistemler, hassas yapılara dâhildir. Kendi içerisinde pek çok çalışma alanı barındıran güvenlik, gelişen sistemlerle yeni çalışma alanları ortaya çıkarmıştır. Özellikle teknolojinin ilerlediği günümüz süreçlerinde, sistemlere ayrı önem verilmektedir. Teknolojinin ilerlemesi, her alanda büyük değişikliklere sebep olmuştur. Özellikle uluslararası sistemde, var olan düzende etki edebilecek yapılar ortaya çıkartmıştır. Bu sebeple; teknoloji, uluslararası düzende, aktörler için önemli güçlerden biri haline gelmiştir. Uluslararası alan ve pek çok düzeyde güç, önemli bir yere sahiptir. Ancak, teknolojiyle beraber gücün anlamında da belirli değişikler olmuştur. Güç; bir aktörün başka bir aktörü etkileyerek, bir şey yapmasını ya da yapmamasını sağlamasıdır. Önemli olan; aktörün, etkileme yeteneği, bunu başarması, aktörün gücünü göstermesidir.[720] Bir aktörün, gücünü doğru kullanıp, başarıya ulaşmasının altında; aktörün bu konudaki yeteneğini ve imkânlarını doğru şekilde kullanması yatmaktadır. Burada, başka bir aktörü, istenilen yönde etkileme vardır. Birçok aktör, gücü doğru kullanmak için

[718] Levent Yiğittepe, *Avrupa Birliği'nde Güvenlik Politikaları ve Arayışları* (İstanbul: Cinius Yayınları, Şubat 2017), 27.
[719] Dedeoğlu, *Uluslararası Güvenlik ve Strateji*, 82-83.
[720] Goldstein ve Pevehouse, *International Relations*, 45.

çalışmalar yapar. 1990lı yıllar öncesinde güç, ağırlık olarak askeri güce yakın bir anlam taşımaktadır. Günümüzdeyse; askeri gücün beraberinde ekonomi, teknoloji gibi güçler vardır. Özellikle ekonomik olarak güçlü olan devletler, teknolojisini en üst seviyeye yükseltmeye odaklanmıştır. Bu yönde yapılan çalışmalarsa; uzun süredir kabul edilmiş olan güçler dengesinde değişikliğe sebep olabileceğini göstermeye başlamıştır. Güçler dengesinin değişmeye başlamasıysa bir güvensizlik ortamına sebep olmaktadır. Güvensizlik, devletlerarasında ciddi sorunlara yol açabilmektedir. Uluslararası sistemde, devletlerarasında fark edilebilecek derecede bir gerginlik bulunmaktadır. Güçler dengesinin değişmeye başlamasıysa, var olan gerginliğin daha çok artmasına sebep olabilecek bir etkiye sahiptir.

Güç, özellikle teknolojik olarak artık farklı bir önem taşımaktadır. Eski dönemlerde dahi önem taşıyan teknolojik güç, günümüzde yeni yapısıyla daha çok dikkat çekmektedir. Teknolojinin hızlı bir biçimde yenilenerek ilerlemesi, teknolojik açıdan gücün de sınırlarının bilinmemesine sebep olmaktadır. Aynı zamanda, var olan güçler dengesini tehdit etmesi, bu gücün dikkat edilmesi gereken bir yapıda olduğunu göstermektedir. Doğru izlenen politikalarla güç, özellikle teknolojik açıdan, politikayı yapanlar için olumlu sonuçlar doğuracaktır. Ancak, sürekli teknolojik bir güce sahip olma çalışması, Soğuk Savaş Dönemi'ndeki silahlanma problemine benzer biçimde dönüşecektir. Bu sebeple; yapılan politika ve çalışmalarda, teknolojik güce dikkat ederek ilerlenmelidir. Özellikle belirli aktörlerin teknolojik güçleri belirlenerek, o düzeyde çalışmalar yapılmalıdır.

Teknolojik değişiklikler; siber alan üzerinden de kendini göstermektedir. Siber alan; tüm teknolojik yapılar, sistemler, bu sistemleri kullanan kullanıcılar, veriler, hatta kullanılan cihazlara kadar hepsini kapsayan bir alandır. Ancak, siber alanın sınırları olmaması, pek çok tehdidi bünyesinde barındırmasına sebep olmuştur. Tehditlerin kendini siber alanla aynı oranda geliştirmesiyse, bir güvenlik ihtiyacı ortaya çıkarmıştır.

Uluslararası ilişkiler disiplini, ulusal anlamda güvenliği; küresel, yerel ve bölgesel olarak incelemektedir. Kendi içerisinde; sosyal, siyasi, askeri, çevresel, ekonomik bileşenleri bulunan bir bütün olarak söz edilebilir. Bunların herhangi birine gelecek tehdit; ulusal güvenlik konusu olmaktadır. Siber alan, bu alanların

içerisine yerleşmiş bir yapı oluşturduğu günümüz koşulunda, siber tehditler bir ulusal güvenlik meselesine gelmektedir.[721]

Günümüzde siber alan, artık ulusal güvenliği aşabilecek bir konuma gelmiştir. Soğuk Savaş dönemine kadar, hükümetlerin, özellikle bilişim sistemlerinde, günümüzdeki gibi bir bağımlılıkları bulunmamaktaydı. Siber güvenliğeyse; 1990'lı yıllara kadar önemli bir konum atfedilmemiştir.[722] 1990'lı yıllardan sonra, internetin yaygınlaşması, önemli bilgilerin, özellikle gizli bilgiler, kitle imha silahları hakkında bilgilerin, bu ortamda saklanması, dikkat edilmesi gereken bir yapıya dönüştürmüştür. Devlet işlerinin çoğunluğunun bilgisayar üzerinden işlem görmesi, internet üzerinde, özellikle siber alanda güvenliğin önemini arttırmıştır.[723] Siber alan, 1990'lardan önce var olmasına rağmen, ulusal güvenlik içerisinde bir yapı altında, tek başına olmayacak biçimde, daha az önem gösterilerek söz edilmiştir. Soğuk Savaş Dönemi sonrasında, teknolojinin önemi, siber alanın ayrıca öne çıkmasına yol açmıştır. Öne çıkan teknolojiyle beraber, hızlı biçimde kullanılmaya başlanmıştır. Hızlıca yayılan siber alan, üzerine çalışmalar yapılması ihtiyacı ortaya çıkarmıştır. Günümüzdeyse daha çok önem kazanmıştır. Önemli adımlar atılmış, ancak, diğer alanlara verilen önem kadar henüz dikkat edilememektedir. Gelişen bir çalışma alanı vardır. Daha geniş çaplı çalışmalar yapılabilmesi, alanda ilerlenmesinde daha yararlı olabilecektir.

Siber alanın kendini yenilemesi, sınır tanımayan bir yapısı olması, küresel olduğu düşüncesini oluşturmuştur. Sınırları olmayan siber alanın en önemli haberleşme sistemlerinden biri; günümüzde en çok kullanılan, ağ yapısı olarak tüm dünyada iletişimde etkili, internet ortamıdır. İnternet, iletişim amaçlı ortaya çıkmıştır. Ancak, en başta, günümüzdeki sonuçların ortaya çıkacağı beklenmemiştir. Küreselleşme ve internet, sürekli gelişen ağ teknolojisiyle; birey, kuruluş, uluslara ciddi derecede güç vermiştir. Herkesin bilgi ve iletişime erişmesi, dijitalleşmeye yol açmıştır. Bu; özellikle siyasi, askeri çatışmada etkili bir siber boyuta sahip olmuş, hatta siber savaşların, klasik savaşlardan önemli hâle gelebileceğinin sinyalini vermiştir.[724] Siber alanın güvenlik tehditlerini içerecek biçime ulaşmasının altında; rahat kullanımı sağlanarak, her türlü siber güce herkesin erişiminin kolay olması yatmaktadır. İletişimin anlık, dünya çapında

[721] Bayraktar, *Siber Savaş ve Ulusal Güvenlik Stratejisi*, 159-160.
[722] Bayraktar, *Siber Savaş ve Ulusal Güvenlik Stratejisi*, 18.
[723] Yiğittepe, *Avrupa Birliği'nde Güvenlik Politikaları ve Arayışları*, 75.
[724] Geers, *Strategic Cyber Security*, 9.

kolaylıkla yapılması, alanın tercih edilmesine sebep olmuştur. Küresel şekilde gerçekleşen internet iletişimi, anında yapılabilmekte, maliyeti, pek çok yöntemden düşük olmaktadır.[725] Kullanımda maliyet düşüklüğü; siber alana yönelmeyi daha çok arttırmıştır. Siber alandaki gelişmeler sayesinde, coğrafi mesafeler kısalmış, iletişim yöntemlerinde değişimler yaşanmıştır. Farklı ülkelerden aynı düşüncelere sahip kişiler bir araya gelebilmiş, bir ülkede yaşanan bir olaydan başka bir ülke hızlıca haberdar olup, etkilenebilmiştir.[726] Bir olay yaşandığında, önceki yıllarda, diğer aktörler uzun sürede haberdar oluyorken, günümüzde, olay anını canlı bir biçimde aktarıp, tepki anında alınmaktadır. Özellikle, anında iletim, müdahale ihtiyacında olumlu bir gelişmedir. Ancak, bir anda kitlelerin ayaklanmasına sebep olacak ihtimallerde olumsuz bir gelişmedir. Herkesin, her an ulaşabileceği, maliyetinin düşük olmasından dolayı, pek çok olayda tercih edilebilecek olması, siber alanda önemli bir noktadır. Büyük bir kitleye ulaşma imkânı sağlan bu alan, olumlu ve olumsuz yanları olduğunu bu şekilde göstermektedir. Ancak, yaşanan olayların, tüm dünyayı etkileyebilme ihtimali, küreselliği akla getirmektedir.

Küreselleşme, günümüzde bazı düşüncelerde; siber alanla ilgili biçimde söz edilmektedir. Küreselliğin özelliği olan sınırların azlığı veya yokluğu, siber alanın sınırlarının olmamasıyla benzemektedir. Ayrıca, küreselleşmeyle gelişen yapılar üzerinde siber alanın gelişmesi ve ilerlemesi önemli ölçüde olmuştur. Ancak, küreselleşme ve siber alan arasında önemli farklar da bulunmaktadır. Bu sebeple; küresellik ve siber alan arasındaki farklılığa değinmek önemlidir. Özellikle yapılacak çalışmalar ve izlenecek yöntemler açısından önem taşımaktadır. Genel anlamda küreselleşme; dünya üzerinde karşılıklı bağımlılığın hızlanması, derinleşmesi, hatta yaygınlaşması biçiminde tanımlanmaktadır.[727] Küreselleşmenin getirdiği karşılıklı bağımlılık, tanımı itibariyle, iki farklı aktör ya da olayın, aynı sistem içerisinde, birbirini etkilemesidir. Ayrıca, karşılıklı bağımlılıkla bazı olaylarda engelleyici bir yapıda olmaktadır.[728] Günümüzde bir ürün üretilirken, her parçası farklı ülkeden gelmektedir. Bir ülkenin ekonomisi için, başka bir ülkeden ürünü, sistemi karşılanmaktadır. Bunlar; belirli bir bağımlılık olduğu ve artma ihtimalinin olduğunu göstermektedir. Devletlerin bağımlılığı karşılıklıdır. Özellikle, uluslararası alanda karşılıklı bağımlılık,

[725] Nye ve Welch, *Küresel Çatışmayı ve İşbirliğini Anlamak*, 2.
[726] Bıçakçı, *21. Yüzyılda Siber Güvenlik*, 1.
[727] Çıtak, *Güvenlik ve İstihbarat*, 162.
[728] Nye ve Welch, *Küresel Çatışmayı ve İşbirliğini Anlamak*, 351.

küreselleşmenin getirdiği yapılardan biridir. Ancak, bağımlılığın iki taraflı olması daha önemlidir. Bir ülkeden temin edilen ürünün, başka bir ülke ekonomisini güçlendirmesi, bağımlılığın tek taraflı olmasına sebep olup, farklı bir yapıya dönüşebilir. Ancak, siber alan bir bağımlılık özelliği taşımamaktadır. Hatta bir sınırının olmaması, önemli bir tehdit oluşturmaktadır. Ülkelerin farklı açılardan bağımlı olması, siber alanın belirli tehditlerini azaltabilse de, geçerli olacağı sürecin belli olmaması bir problem oluşturmaktadır.

Küresel alandaki bağımlılık, daha çok karşılıklıdır. Bir tehditte etkilenen sadece bir ülke değildir. Ülkeyle karşılıklı bağımlılığı olan her aktör tehditten etkilenir. Küreselleşmeyle, kendi içerisinde bu tehdit varken, siber alanda dâhil olmak üzere, güvenlik muğlak bir hal alır. Bu muğlaklık, güvenliği sağlanması gerekenin ne olduğu üzerine tartışmalara sebep olur. Güvenlik üzerine kesin yargıların oluşmaması, uluslararası alanda yapılması uygun olan çalışmalarda sorunlar çıkarmaktadır. Güvenlik dışında, teknolojinin gelişmeleri ve küreselleşmeyle, uluslararası alanda olumlu ve olumsuz olaylar ortaya çıkmasına sebep olur. Küreselleşmeyle, teknolojinin gelişmeleri hızlı bir biçimde yayılabilirken, bilginin aynı hızda yayılıp elde edilmesi, güvenliğin sağlanmasında sorunlar çıkarmaktadır.[729] Bilginin dünya üzerinde hızla dolaşması, bilgi edinme açısından olumludur. Ancak, yanlış bilgilerin, aynı hızda, anlık erişilmesi, bilgi kirliliği ve yanlış davranışlara yol açabilir. Bazı bilgilere kolay erişilmesi, aktörlerin güvenliğini sarsacak niteliktedir. Bilginin hızlı yayılmasında en önemli etkenlerden biri, internetin sağladığı olanaklardır. Alandaki anlık iletişim imkânı, bilgilerin hızlı bir biçimde, doğruluğu bilinmeden dolaşması, belirli zamanlarda, ayrı dikkat edilmesi gereken bir konumdadır. Medya alanını da ilgilendiren bu tehditler için, çalışmalara, alanında uzman kişilerce dikkat edilmelidir. Verilecek bilgilerin doğru kaynaklardan çıktığına emin olarak, belirli bilgilerin dağıtımını sağlamak gerekmektedir. Aynı zamanda, istenmeyen diğer aktörlerin erişebileceği bilgilere, yine uzman kişilerce dikkat edilerek alan üzerinde dolaşımına dikkat edilmelidir.

İnternet, ulusal çalışma, üretim gibi alanlarda etki gösterirken, dünya çapında, insanlarla ülkeleri birbirine bağlama, küresel bilgi ağı oluşturmada önemli yeri olmuştur. Bu gelişmeler, hem olumlu hem olumsuz sonuçlar ortaya

[729] Çıtak, *Güvenlik ve İstihbarat*, 162-173.

çıkarmıştır. Küresel bilgi ağı, özellikle iki önemli sonuç ortaya çıkarmıştır. Birbirine bağımlı iletişim ve bilgi teknolojileri, kazanç sağlayıp, ulusal bir değer sayılabilen bilginin sistemlerine bir saldırı ihtimali vardır. Bunun güvenliğini sağlama gerekliliği, günümüzde önemli bir güvenlik alanı haline gelmesine sebep olmuştur.[730] Alanın çeşitli aktörler tarafından kullanılması, iletişimin bu alan içerisinde olması ayrı önemlidir. Siber alanda güvenli iletişim için önemli üç nokta vardır. Gönderinin sadece alıcı ve gönderici arasında olması; gizlilik, içeriğin değişmeden teslim edilmesi; bütünlük ve ulaşması izin verilen kişilerin bilgiye ulaşabilmesi için erişilebilirlik sağlanmalıdır.[731] İletişim güvenliği bunlar üzerinden sağlanması, siber alanda temel noktalardandır. Siber alan ve bu alanda iletişimin birey düzeyinde olmaması, uluslararası alana yansıyacak kadar geniş bir yapıya dönüşmesi, güvenliğe önem verilmesi gerektiğini göstermiştir. Önemli bir bilginin, iletişim ağına sızan, bunlara ihtiyaç duyan bir grup, kişi, devlet tarafından ele geçirilmesi, iletişimde güvenliğe zarar getirecektir. Ancak, siber güvenlik sadece iletişimle sınırlandırılacak bir yapı değildir. Pek çok alan içerisinde görülen siber alan ayrı önem verilmesi ve üzerinde çalışılması gereken bir yapıdadır.

1990'lı yıllarda, ilk defa, siber güvenlik, bilgisayar mühendisleri tarafından, bir ağa bağlı bulunan bilgisayarlar üzerindeki güvenlik sorunlarından söz edilirken kullanılmıştır.[732] Siber alanın güvenliğe dâhil edilmesi sonrası, bir savaş alanı olma ihtimali ortaya çıkmaya başlamıştır. Siber alanın güvenliğinin sağlanması için çalışmalar yapılmıştır. Ancak henüz bu çalışmalar tamamlanmamıştır.[733] Bir alanda çalışmaların tamamlanması, alanla alakalı sorunların sınırlarının belirlenmesiyle sağlanır. Siber alan tam oturmamış ve sınırları tam belirlenememiştir. Günümüzde, siber güvenlik üzerine çalışmalar devam etmekte, başlangıcı 1990'lı yılların öncesine dayanmaktadır. Ancak, tek başına bir güvenlik alanına dönüşmesi; Soğuk Savaş Sonrası Döneme denk gelmektedir. Günümüzdeyse, siber alan üzerine çalışmalar daha kapsamlı hâle gelmiştir.

Siber güvenlikte, önemli konulardan biri; siber tehditlerdir. Tehditlerin boyutuna göre belirli tedbirler alınmaya çalışılmaktadır. Güvenliğin kendi

[730] Çakmak ve Altunok, *Suç, Terör ve Savaş Üçgeninde Siber Dünya*, 85.
[731] Altınkaynak, *Uygulamalı Siber Güvenlik ve Hacking*, 188-189.
[732] KURGAN, *Siber Mücadeleye Giriş*, 46.
[733] Çakmak ve Altunok, *Suç, Terör ve Savaş Üçgeninde Siber Dünya*, 203.

yapısından kaynaklı olarak, var olan bir tehdidin önüne geçmek için çalışmalar yapılmaktadır. Aynı çalışmalar, siber güvenlik içerisinde de vardır. Siber alanda bulunan tehditler içerisinde dikkat edilmesi gerekenlerden bir tanesi, siber tehditlerin fiziksel bir savaşa dönüşme ihtimalidir. Günümüzde henüz bu tehlike tam olarak ortaya çıkmamış, ancak yakın olaylar yaşanmıştır. Önemli sorunlar, ciddi boyutlara ulaşmadan durdurulmuş ya da kanıtlanamadığı için ilerlememiştir. Ancak sorunlar, günümüz olayları için bir birikim olmuştur. Birikimlerse daha büyük problemlere yol açabilmektedir.

Uluslararası alanda, bir sorunun savaşa dönüşmesi için belirli birikimleri olmalıdır. Birikimler dışında, var olan tehditler, ilişkilerin bozulmasına zemin hazırlamaktadır. Aynı zamanda, uluslararası alanda bir devletin güçlenmesi, diğerlerinin güvensiz hissetmesine sebep olur. Bunun sonucunda; tehdit görülen devlete karşı savunma mekanizması geliştirilmeye başlanır.[734] Olası bir güçlenme karşısında, kendini tehdit altında gören aktör ya da aktörler savunma mekanizması geliştirirler. Bu aktörler, kendilerini daha güçlendirmeye çalışır, saldırgan bir tavır sergileme eğiliminde bulunabilirler. Bunları siber alanla bağdaştırdığımızda; günümüzde önemli yapılardan bir tanesi teknoloji olmaktadır. Bir aktörün teknolojisini, başka bir aktörden daha güçlü hale getirmesi, aktörün güvensiz, tehdit altında hissetmesine sebep olabilir. Güvensizlik ve tehdit duygusu, savaş ihtimalini yanında taşır. Savaş ihtimali, tarih boyunca birçok alanda görülmüştür. Ancak, siber alanda görülen örnekler 1990'lar öncesine dayanabilmektedir.

Siber alanın dikkat çekici biçimde görüldüğü ilk olaylar; I. Dünya Savaş'ına kadar gitmektedir. Ancak, siber alan, daha çok elektronik sistemler içerisinde söz edilmiştir. Savaş sırasında elektronik harp biçiminde söz edilmiş, daha ileri dönemlerde siber alan şekline dönüşmüştür. Siber alan, 1990'lar sonrasında, bilgisayarların artmasıyla, bu ortam üzerinden söz edilmiştir. Özellikle savaş alanı olarak, siber alan farklı bir konumda düşünülmeye başlanmıştır. Siber alanın savaşta, klasik savaşlar gibi başlama, bitme kesinliği yoktur. Savaş alanının bir sınırının olmaması, ilk akla gelen savaş alanından çok, mücadele alanı olarak görülmesine sebep olmuştur.[735] Ancak, elektronik sistemlere saldırılması ve büyük sorunların yaşanmasına sebep olması, mücadele olarak sınırlamayı zorlaştırır. Alan olarak, tehlike barındırıp, yaşanan olayların kendi içerisinde

[734] Nye ve Welch, *Küresel Çatışmayı ve İşbirliğini Anlamak*, 24.
[735] KURGAN, *Siber Mücadeleye Giriş*, 68.

ilerlemesi, önem atfedilmesini sağlamıştır. Aynı zamanda, yaşanan her olay, siber alan üzerinden daha dikkate alınmaya başlamış, bunlar birikim olmasına sebep olmuştur. Günümüzde pek çok devlet arasında, siber alanda saldırılar yaşanmış, ancak, kanıtlanamayan bazı olaylar vardır. Kanıtlanamaması; devletlerde birikimlere ve gerginliklere yol açmıştır. Kanıtlananlarsa, politikalar belirlenmesi ve çalışmalara yardımcı olmuştur.

Siber alanı kapsayan yıkıcı olaylardan biri; Eylül 2001'deki, Washington ve New York terör eylemleridir. Bu terör eylemleri; teknolojinin, hükümetin tekelindeki yıkıcı gücünü, artık devlet dışı aktörlerin kullandığını göstermektedir.[736] Terör olayının getirdiği olumsuzluklar dışında, teröristlerin iletişim yöntemi olarak interneti kullanması, olayı önceden simülasyon programı üzerinde çalışmaları, internetin terörist eylemlere açık olduğunu gösterir niteliktedir. Aynı zamanda, bir siber saldırının ekonomik ve kritik altyapılarda hasarlar oluşturma ihtimali, ulusal güvenlik belgelerinde, siber güvenlik stratejilerinin geçmeye başlamasında önemli bir adım olmuştur.[737] 2001 yılındaki bu olay sonrasında, güvenlik tanımlamaları ve yapılan çalışmalara kadar, uluslararası alanda pek çok değişiklik yaşandığı bilinmektedir. Siber alanın çeşitli şekillerde kullanılabildiği artık daha açık görülmeye başlanmıştır. Birçok olay dışında, devlet ilişkilerini sarsabilecek olayların bir kısmının, bu alan üzerinden yaşandığı bilinmektedir.

4 Ekim 2006'da, WikiLeaks[738] isimli web sitesi, kötüye kullanma, yozlaşmayı ortaya çıkarma amaçlı açılmıştır. Amacı; önemli aktörlerin hatalarını, belgelerle ortaya koyarak, tavırlarını tekrardan şekillendirmelerini sağlamaktı. WikiLeaks, 2010 yılında yayımladığı belgeyle, Pentagon'un 2008 yılında söz ettiği; bu sitenin, ABD'nin, özellikle orduda izlediği harekât güvenliği, kuvvet koruma, karşı istihbarat, bilgi güvenliğini tehdit edebilecek düzeye geldiğidir. Bu düşünce, WikiLeaks'ın amacının tehlikeli boyutlara gelebileceğinin işaretidir. WikiLeaks'in ortaya çıkmasındaki amacı; kötüye kullanımın önüne geçmek için hataları, belgeleri paylaşmaktı. Ancak, paylaşımlar beklenenden çok yankı uyandırmıştır. Belgelerin önemli bilgiler içermesi, internet ortamında herkesin ulaşabileceği bir yerde olması, gelecek her türlü tehlikeye yer hazırlamıştır. 2010

[736] Nye ve Welch, *Küresel Çatışmayı ve İşbirliğini Anlamak*, 2.
[737] Bıçakçı, *21. Yüzyılda Siber Güvenlik*, 32-33.
[738] https://wikileaks.org/-Leaks-.html

yılında gelen açıklamalarla, dünya çapında önemli, gizli belgeler art arda ortaya konulmaya başlanmıştır.[739] 28 Kasım 2010 tarihi sonrasında paylaşılan belgeler, o tarihe kadar sızdırılmış, en fazla miktarda gizli belge olması sebebiyle önemlidir. Gizli belgelerin hızlıca ortaya çıkması, siber alanda güvenliğin önemini göstermiştir. Siber güvenlikte, internet teknolojisiyle gizli bilgilerin kolayca açığa çıkması, uluslararası ilişkilerde ciddi sonuçlar ortaya çıkabileceğini göstermiştir. WikiLeaks, bilginin önemli bir güç olduğunu ortaya koymuştur. Bir devletin bildiği bilgiyi, başkalarının öğrenmesi, devletin gücünde azalmaya sebep olacağı görülmüştür.[740] Günümüzde güç; askeri kapasite dışında bir alanın yükselmesini sağlamıştır. Bilgi, çağlar boyu önemli bir kaynak olmuştur. Günümüzdeyse önemi daha çok artmış, bu, pek çok aktör için sorun oluşturmuştur. Artık herkes, her bilgiye ulaşabildiği için, gizli tutulması gereken önemli bilgiler dahi, ulaşılması kolay bir hal almıştır. Bilginin ve onu uygulayanın güce sahip olduğu siber alan, korunması gereken bir alan olmuştur. Ancak olaylar sadece bu kadarla kalmamıştır. Yakın zamanda, siber alanda önemli, farklı olaylar ortaya çıkmıştır.

20 Mayıs 2013'te, ABD'de, NSA'da görevli Edward Snowden, çalıştığı kurumda elde ettiği pek çok gizli bilgiyi, 'The Guardian' isimli gazeteye sızdırarak, bazı belgelerin yayımlanmasını sağlamıştır. Yaptığı eylemin siber anlamda önem taşımasının sebebi; ABD'nin siber casusluk faaliyetlerini bu şeklinde ortaya çıkartmış olmasıdır. Söz edilen belgelerde ortaya çıkan genel olarak; ABD'nin elindeki siber kapasiteyle, izinsiz pek çok kişi ve devletin iletişim bilgilerini kayıt altına alarak, izlemesidir. Siber güvenlik üzerinden değerlendirildiğinde; ağ teknolojileri, dijital ortamda toplanan, aynı zamanda istihbari bilgi olarak analizi yapılan bilgilerin, günümüzde gizli kalmasının zorluğunu ortaya koymuştur.[741] Bu iki önemli olay; bazı devlet ve aktörler arasında güvensizliğin ortaya çıkmasına sebep olmuştur. İki olay sonrasında önemli olan; siber alanda ilişkilerin bir anda bozulabileceğini göstermesi, aynı zamanda, gizli çalışmalarla bilgilerin kolayca ortaya çıkabileceğidir. Ortaya çıkan bilgiler, hızlı bir biçimde yayılıp, herkesin anında erişebildiği bir hale gelmiş, sonucunda birçok olay yaşanmıştır.

[739] Singer ve Friedman, *Siber Güvenlik ve Siber Savaş*, 79-81.
[740] Darıcılı, *Siber Uzay ve Siber Güvenlik*, 123-127.
[741] Darıcılı, *Siber Uzay ve Siber Güvenlik*, 113-120.

Siber alanda yaşanan bir olayın, fiziksel olarak, ciddi bir savaşa dönüşme ihtimalinin en yüksek olduğu olaylardan biri; 2010 yılında, ABD ile İran arasında yaşanan, Stuxnet olayı olmuştur.[742] Stuxnet isimli bir solucan, İran'da bulunan nükleer tesisleri hedef alarak, saldırı yapmıştır. Sonucunda; İran ve ABD ilişkilerinde gerilim yaşanmıştır. Ayrıca saldırı; bir sistemi hedeflerken, kontrolden çıkıp, başka devletlerin siber sistemlerine saldırmıştır.[743] Asıl önemli olan; iki devlet arasındaki ilişkilerin gerilmesine rağmen, büyük bir sonuç ortaya çıkmamıştır. Bunun sebebi; hiçbir devletin olayı üstlenmemesidir. Ancak, ABD-İsrail yapımı bir solucan olduğu ortaya çıkınca, ABD bunu yalanlamamıştır.[744] Saldırı hedefinin nükleer tesisler oluşu, saldırının kontrolden çıkmış olması, tehdidin büyüklüğünü gösterir. Saldırıyı yapanın kesin olmaması, yine de devletlerarasındaki ilişkilerde gerginlik oluşturmuştur. Hatta fiziksel bir savaşın eşiğinden dönülmüştür. Saldırıyı yapanın siber alanda tespitinin zorluğu, saldıran devletin, kendi avantajına kullanmasını sağlamıştır. Siber alanda olaylar, gün geçtikçe daha farklı biçimlerde kendini göstermektedir.

2014 yılında, siber alan için önemli olan; ilk ilan edilmiş dünya siber savaşı ortaya çıkmıştır. 2014 yılında; I. Dünya Siber Savaşı'nın başladığı duyurulmuştur. ABD ve Çin Halk Cumhuriyeti arasında başlayan siber saldırılar, diğer devletlerin katılmasıyla, siber dünya savaşına dönüştüğünden bahsedilmiştir.[745] Savaşın bittiğine dair bir bilgi yoktur. İnternet üzerinden yapılan saldırıların takip edileceği bir web sitesi[746] bulunmaktadır. Olay sanal ortam üzerinde ilerlerken, henüz fiziksel olacak bir saldırı yapılmamıştır. Ancak, bu olay siber alanda, son dönemdeki en önemli olaylardan biridir. Siber alandaki bu savaş, her zaman beklenen, Üçüncü Dünya Savaşının boyut değiştirmiş hâli olabileceği düşünülebilir. Ancak, henüz büyük zarar oluşmamış, sonuçları ortaya çıkmamıştır. Bu sebeple; siber savaş için yapılan yorumlarda, kesin konuşulması sorunlar oluşturacaktır. Ancak, ortaya bir savaş çıkarma ihtimali olduğu bilinmektedir.

[742] KURGAN, *Siber Mücadeleye Giriş*, 196.
[743] Salma Shaheen, "Offense–Defense Balance in Cyber Warfare," içinde *Cyberspace and International Relations: Theory, Prospects and Challenges*, ed. Jan-Frederik Kremer ve Benedikt Müller (London: Springer Publishing, 2014), 84-85.
[744] "Stuxnet ve Uluslararası Hukuk: Bir siber saldırının anatomisi," *Siber Bülten,* E.T.: 20 Ekim 2018, url: https://siberbulten.com/makale-analiz/stuxnet-ve-uluslararasi-hukuk-bir-siber-saldirinin-anatomisi/.
[745] "1. Siber Dünya Savaşı mı Başladı?," *Hürriyet Haber,* 28.12.2014, E.T.: 24 Ekim 2018, url: http://www.hurriyet.com.tr/avrupa/1-siber-dunya-savasi-mi-basladi-27856461.
[746] https://threatmap.checkpoint.com/ThreatPortal/livemap.html

Günümüzde yaşanan bu saldırılar ve olaylar, olası bir savaşın birikme süreçleri ya da gelişim aşaması olma ihtimali vardır. Devletlerin birbirilerine karşı izledikleri gergin politikalarsa, bu ihtimali daha çok tetikleyebilecek bir yapıdadır.

Başka bir açıdan bakanlarsa; siber savaşta çatışmaların, açık şiddete dönüşmeyeceğinden söz edilir. Bu düşüncede siber savaş; Soğuk Savaş benzeri, daha az resmi görülüp, serin savaş olarak söz edilir. Sınırı olmadan, uzun süre fiziksel bir savaş başlatmadan yürütülebilecek bir biçimde devam edeceği fikri bulunmaktadır.[747] Ancak, siber saldırılar hasarsız olmamıştır. Siber alan, günümüzde fiziksel ciddi sonuçlar ortaya çıkartmamıştır. Fakat ciddi bir saldırıda, beklenenden daha olumsuz sonuçlar ortaya çıkacağı bilinmektedir. Siber savaşlar, geleneksel olarak bilinen savaşlardan farklı görünse bile, aslında düşünülenden daha benzerdirler. Fiziksel biçimde başlayacak bir savaş öncesi, siber alan, istihbarat toplayarak işin içine dâhil olup, savaşta kullanılan silahların bağlı olduğu ortamı kapsadığı bilinir. Siber savaşı istihbarattan ayıran özellik; operasyonların ani bilgi toplama eyleminden, saldırgan eylemlere dönüşmesidir.[748] Siber alanın fiziksel bir savaşa dönüşmeyeceği düşünülmektedir. Ancak, bunun tersini savunanlar da vardır. Siber anlamda birçok devlet, ordusunda siber savaş olasılığı üzerine plan ve kuruluş oluşturmuştur. Plan içerisinde; Beş D+1 (Deny- inkar, Destroy- yok etme, Disrupt- dağıtma, Degrade- indirgeme, Deceive- aldatma + Defending- savunma) bulunmaktadır.[749] Plan; bir saldırı için uygulanabilecek yöntemdir. Tehdit algılanmadığı sürece, devletler plan ve projelere ihtiyaç duymazlar. Günümüzdeyse, siber alan kesin şekilde tahmin edilemeyen bir alan olduğu için, tehditlerin önüne geçmek amaçlı plan ve birimlere ihtiyaç duyulmuştur. Bir saldırı ya da oluşabilecek büyük problemler için savunma planları yapılıp, belirli politikalar üretilmeye çalışılmaktadır.

Günlük hayatta uygulanan işlemler, siber alana taşınmaya başlamıştır. Suçların aynı alan üzerinden uygulanıp yayılmasıysa, hukuki düzenlemelere ihtiyaç duyulduğunu göstermiştir.[750] İnternetin sınır aşan, devletlerin sınırları içerisine hapsedilemeyen, bir bakıma küresel yapısı, devletlerin kendi iç hukuklarının siber suçlar üzerinde uygulanmasında sorunlar çıkarmaktadır. Devletin yargısı, kendi sınırları içerisinde olup, siber alanda ortaya çıkan suçlarda

[747] Singer ve Friedman, *Siber Güvenlik ve Siber Savaş*, 166.
[748] P. W. Singer, "Sıfırla Birlerin Savaşı," *Popular Science* 29 (2014): 39.
[749] Singer ve Friedman, *Siber Güvenlik ve Siber Savaş*, 174.
[750] Çakmak ve Altunok, *Suç, Terör ve Savaş Üçgeninde Siber Dünya*, 168.

sadece belirli çerçevede etkili olmaktadır.[751] Siber alanın yapısı sebebiyle; uluslararası hukuk ve sistemlerin tamamen kapsayacağı bir alan değildir.[752] Siber alan için kesin bir sınırlama yoktur. Günümüzde çalışmalar yapılsa bile, siber suç, saldırı ya da savaş ihtimalinde, birebir bağlayıcı kurallar yoktur. İç hukuk ya da uluslararası hukukla uyumlu, bu tehditlerin önüne geçecek ciddi bir sistem bulunmamaktadır. Kuruluşlar bunun için çalışmalar yapmış, ancak, belirli sınırlar ve düzeylerde kalmıştır. Günümüzde siber alan için, ciddi bir biçimde caydırıcılık tam olarak yoktur.

Küresel dünya düşüncesiyle sınırların kalktığı bir ortamda, siber alan, hassas, güvenliği düşük bir alandır. Hizmetlerin dışarıdan sağlanmasıyla, uluslararası iş birliği zorunlu kılınmıştır. İnternet güvenliğinin, sınırlar içerisinde oluşturulması güçleşmiştir. Siber alanın, sınırlar içerisinde güvenliğinin oluşması, sadece bir ulusa bağlı değildir. Bir sınırı olmaması zorluk çıkarmaktadır. Küresel olarak aktörlerin, bazı hizmetler üzerinden birbirine bağlılığı, belirli ölçüde iş birliğini zorunlu hale getirmiştir. Finansal olarak da benzerinin görülmesi, devletlerarasında küresel bir niteliğin varlığı, saldırı ihtimalinin önüne geçilmesini sağlamaktadır.[753] Bazı aktörler birbirine finansal olarak bağlıdır. Bu bağlılığı bozacak tehditleri engellemek için zorunlu bir iş birliği sağlanması gerekmiştir. Devletlerin, büyük yatırımlar yaparak, kendilerini siber alanda güvenlik ve silah bakımından güçlendirme çalışmaları, siber güvensizliği beraberinde getirmektedir.[754] Siber alan, küresel bir sistemde, sınırları hiç olmamış şekilde varlığını sürdürmektedir. Siber alan, kendi teknik gereksinimlerinden dolayı teknolojiye ihtiyaç duymaktadır. Bu teknolojinin sağlanması için belirli bir düzeyde ekonomi gerekir. Ekonomik gelişimlerle yatırımlar, devletlerarasında zorunlu bağlılık oluşturabilmektedir. Bu bağlılıkla; siber saldırı karşısında, devletlerin vereceği tepkilerin önüne geçilebilmektedir. Ancak, kendi ekonomisini güçlendiren, bir süre sonra bağımlılığını en aza indiren aktör için, bu sınırlamanın geçerliliği bilinemeyecektir. Tehditlerin tehlikeye dönüşebileceği zamanlarda, savaş kendini gösterebilecek bir konumdadır.

---

[751] Çakmak ve Altunok, *Suç, Terör ve Savaş Üçgeninde Siber Dünya*, 145.
[752] Bıçakçı, *21. Yüzyılda Siber Güvenlik*, 49.
[753] Çakmak ve Altunok, *Suç, Terör ve Savaş Üçgeninde Siber Dünya* (Ankara: Barış Platin Yayınevi, Mayıs 2009), 68-133.
[754] Bıçakçı, *21. Yüzyılda Siber Güvenlik*, 51.

Bilinmesi gereken önemli bir nokta; bir savaş ya da saldırıda, P. W. Singer'ın bahsettiği üzere; Clausewitz ve Sun Tzu, her strateji ve taktikte, karşı tarafın da aynı şekilde hazırlık yapan, akıllı bir düşmanın varlığından söz etmiştir.[755] Kendini güvenliğe alan, bir strateji kuran aktör dışında, kendisi gibi, benzer biçimde hazırlık yapan başka aktörler bulunmaktadır. Bunlara en güzel örnekler; ABD, Çin Halk Cumhuriyeti, Rusya Federasyonu gibi ülkelerdir. Bu devletlerin her biri kendisini güçlendirmekte, aynı zamanda, karşı aktörlere hazırlıklı olmak için çalışmalar yapmaktadır. Siber alanda, hem birbirlerine hem diğer devletlere karşı tehdit oluşturmaktadır. Aynı zamanda, siber alanda, kendi aralarında siber bir güç savaşı olduğu görülmektedir. Bu güç savaşıysa; özellikle politik anlamda gerginliklere sebep olmakta, gittikçe tırmanan tehditlere dönüşme ihtimalini barındırmaktadır.

Siber alanda aktörler, sadece devletler değildir. Siber suçlar, tek bir noktada gerçekleşebilir. Bir ülkede suçu işleyen kişi, başka bir ülkede ele geçirdiği bilgisayar üzerinden, tamamen farklı bir bilgisayara saldırı düzenleyebilmektedir. Bunlar yine devletlerarasında sorunlar çıkmasına sebep olabilir. Bu; uluslararası iş birliğinin önemini vurgulamaktadır. Ancak, iş birliğinin başarılı olması için, uluslararası hukuk ve iç hukukta uyum sağlanarak, tanımı ve kapsamların belirlenmesi gerekir. Önemli örneklerden biriyse; "Avrupa Konseyi Sanal Ortamda İşlenen Suçlar Sözleşmesi" (Convention on Cybercrime)'dir.[756] Siber alanda suçun kimden ve nereden geleceğinin belirlenmesi zordur. Gerçekleşebilecek siber olayları engelleyebilmek için, iş birliği ve hukukta uyum önemidir. Bunun için yapılan sözleşme, her problemi çözecek nitelikte olmasa bile, önemli adımlardan biri olmuştur. Olabileceklerin önüne geçme amaçlı yapılan sözleşme; siber alanda, internetin ve bilgisayarın kullanımında işlenecek suçlara karşı ilk uluslararası sözleşmedir. Yerel hukukla uyumlaştırmayla küresel düzeyde etkili olabilecek bir belgedir.[757] Anlaşmalar ve belgeler arasında, ilk uluslararası sözleşme olması; siber alanın artık daha çok dikkate alındığını gösterir. Ancak, geçmişteki olaylara göre, güvenlik adına daha çok yeni çalışmalar olduğu bilinmektedir. Bu sebeple; uluslararası hukuk ve iç

[755]bSinger, "Sıfırla Birlerin Savaşı," 41.
[756] Çakmak ve Altunok, *Suç, Terör ve Savaş Üçgeninde Siber Dünya,* 148.
[757] Türkiye Büyük Millet Meclisi, *Sanal Ortamda İşlenen Suçlar Sözleşmesinin Onaylanmasının Uygun Bulunduğuna Dair Kanun Tasarısı ve Dışişleri Komisyonu Raporu (1/676),* (Ankara: 2012), 4, E.T.: 22 Ekim 2018, url: https://www.tbmm.gov.tr/sirasayi/donem24/yil01/ss380.pdf.

hukukta uyumlaştırmalara daha fazla eğilmek gerekir. Tam uyumlu bir hukuk düzeni, günümüz sisteminde zordur. Ancak, belirli tehditlerin daha açık şekilde ortaya konması, tehdit düzeylerinin belirlenerek politikaların buradan ilerlemesi daha olumlu sonuçlar ortaya çıkartacaktır. Siber alanda belirlsiz kalan noktalar olduğu bilinmektedir. Önemli olan, belirsiz alanların üzerine daha çok gidilerek, politikaların buradan yürütülmesine katkı sağlamaktır.

Önemli çalışma yapmış örgütlerin bir kısmı, siber alanı önemseyerek, çalışmalarda bulunmuştur. Birçok örgütün çalışmaları dışında; Ekonomik İşbirliği ve Kalkınma Örgütü (Organisation for Economic Cooperation and Development-OECD) siber suçlar üzerine hazırlanmış yasaların uyumlaştırılması çalışmalarında bulunmuştur. Bilgisayarlarla İlgili Suç: Yasal Politikanın Analizi (Computer-Related Crime: Analysis of Legal Policy) ile 1983-1986 yılları arasında yapılan çalışmayla, öncelik uzlaşı olmuştur. Üye devletlerin ne zaman yaptırım uygulayabileceğinden söz edilmiştir.[758]

Güvenli olmayan yazılımlar sebebiyle çıkan problemler karşısında, bunları gidermek amaçlı; Açık Web Uygulama Güvenliği Projesi (Open Web Application Security Project- OWASP) yapılmıştır. Bu isim altında kurulmuş olan topluluk; yazılım güvenliği için, ihtiyacı olan kişilere, ücretsiz araç ve dokümanları sağlamıştır.[759] Üç yılda bir, bu topluluk, kritik web uygulama açıklıklarının değerlendirmelerini yapmaktadır. En son 2017 yılında, OWASP Top Ten[760] başlığı altında yayımlamıştır.[761]

Çalışmalar içerisinde en önemli olanı; 3 Eylül 2012'de NATO'nun Siber Savunma İşbirliği Mükemmeliyet Merkezi (CCD COE- Cooperative Cyber Defence Center of Excellence) tarafından yapılmıştır. Yirmi hukuk profesörünü görevlendirerek, savaş kurallarının, siber alanda, ne şekilde uygulanması ve düzenlenmesi gerektiğinden bahsedilmiştir. Ayrıca, incelemesinin yapılması, sonrasında resmi olarak bunu doküman haline getirdikleri "Siber Savaş Araçlarına

[758] Çakmak ve Altunok, *Suç, Terör ve Savaş Üçgeninde Siber Dünya*, 178.
[759] Altınkaynak, *Uygulamalı Siber Güvenlik ve Hacking*, 35.
[760] "OWASP Top 10 – 2017: The Ten Most Critical Web Application Security Risks," The OWASP Foundation, E.T.: 18 Ekim 2018, url: https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf.
[761] Ramazan Terkeşli, "Yetkisiz Erişim ve Web Uygulama Güvenliği," *Siber Suçlar: Tehditler, Farkındalık ve Mücadele*, ed. Fatih Tombul vd. (Ankara: Global Politika ve Strateji Yayınları, Ocak 2015), 119.

Uygulanabilir Uluslararası Hukuk Üzerine Tallinn El Kitapçığı[762]" adlı belgeyi yayımlamıştır. Çeşitli konular üzerinde duran doküman, siber alanda savunmadan, siber savaşta sivillerin kanuni korunmalarını kaybetmesine kadar, geniş bir çerçevede fikirleri ortaya koymuştur.[763] Ancak bağlayıcı bir doküman değildir. Çalışmalar, siber alan için ciddi ve önemli olmalarına karşın, bağlayıcı değillerdir. Kuruluşlar altında hazırlanan çeşitli sözleşmelerse, günümüzde etkisiz kalabilecek yapıdadırlar. Ancak, bazı kuruluşlar, siber güvenlikte belirli standartlar oluşturmuşlardır. Bunlardan önemli birkaç tanesinden kısaca söz etmek gerekir.

Teknik standartlar geliştirmek amaçlı Elektrik ve Elektronik Mühendisleri Enstitüsü (Institute of Electrical and Electronics Engineers- IEEE) kurulmuştur.[764] 1963 yılında kurulan enstitü, elektroteknoloji ve bağlı olan bilimler üzerine, kâr amacı olmadan, uygulama ve teorileri geliştirmiştir. Ayrıca, bilgisayar güvenliği üzerine çalışmalar yapmış, bu amaçla farklı çalışmalar yürüten kuruluşlarla beraber çalışmalar da yürütmüştür.[765]

Teknik anlamda DNS (Domain Name System) yani; Alan Adı Sistemlerinin yönetimini yapan ICANN (Internet Corporation for Assigned Names and Numbers- İnternet Tahsisli Sayılar ve İsimler Kurumu) farklı çalışmalar yürütmüştür.[766] Küresel bir topluluk olan ICANN, internette, kişilerin birbirine ulaşması için, bilgisayarların ihtiyacı olan isim ve numaraların birbirini bulmaları amaçlı tanımlama işlemini sağlamaktadır. Aynı zamanda, koordinasyonu yürütmekte, küresel bir internet yönetimini sağlamakta olan bir kuruluştur.[767] Daha çok, internet yapısının, kendisi üzerinden çalışmalarını yürütmekte, tamamen siber alanı kapsayıcı ve bağlayıcı düzenlemeleri barındırmamaktadır.

ISO/IEC (Uluslararası Standartlar Teşkilâtı / Uluslararası Elektroteknik Komisyonu- International Organization for Standardization / International Electrotechnical Commission); en çok duyulmuş, bilgi güvenliği standartlarını

[762] Michael N. Schmitt, "Tallinn Manual on The International Law Applicable to Cyber Warfare," *NATO* (Amerika: Cambridge University Press, 2013), E.T.: 22 Temmuz 2018, url: http://csef.ru/media/articles/3990/3990.pdf.
[763] Singer ve Friedman, *Siber Güvenlik ve Siber Savaş*, 168.
[764] Çiftçi, *Her Yönüyle Siber Savaş*, 252.
[765] "Private-Public and Non-Governmental Organizations (NGOs)," içinde *Global Initiatives to Secure Cyberspace*, ed. Seymour Goodman ve Michael Portnoy (Amerika: Springer, 2009), 88-89.
[766] Çiftçi, *Her Yönüyle Siber Savaş*, 252.
[767] "About ICANN," ICANN, E.T.: 23 Ekim 2018, url: https://www.icann.org/resources/pages/welcome-2012-02-25-en.

geliştirme amacıyla kurulmuştur.[768] ISO, internette ve genel tüm ağlarda aktif olan cihazların aralarındaki iletişim için referans modelini belirlemiştir.[769] Uluslararası standart olarak, görev açısından; özel şirketlerden, kurum ve kuruluşlara kadar pek çok yerde, internet teknolojisinde güvenlik tehditleri, açıklıklar, gizli bilgilerin paylaşımının nasıl yapılacağına dair kılavuz ve genel ilkeler sunmaktadır.[770] Bilgi teknolojileri güvenliği amacıyla, genel teknik ve yöntemlerin standartlaştırılmasına odaklanarak, güvenlik üzerine çalışmalarda bulunmuştur.[771]

Siber alanda yapılan çalışmalar dışında, kullanıcıların yeterince bilinçlenmemesi, internetin kontrolsüz büyümesi, güvenlik sorunlarının oluşmasında önemli noktalardan biridir.[772] Bunun için eğitimlere önem verilmelidir. Birçok devlet bu konuda çalışmalara başlamıştır. Ancak, günümüzde hâlâ internet ve kullanımı üzerine bilgilendirilmesi gereken kişi, grup ve topluluklar vardır. Siber alan konusunda bilgilendirilmemiş kullanıcılarsa ciddi tehdit altındadırlar.

Bilişim sistemlerinde önemli unsurlar; süreklilik, tutarlılık, gizlilik, doğrulamanın sağlanması, bunların güvenliğinden emin olunmasıdır.[773] Bir bilginin güvende olmasında önemli beş nokta; inkâr edilememe, erişilebilirlik, bütünlük, kimlik doğrulama, gizliliğin sağlanmasıdır.[774] Bunlarda problem çıkmaması; internette bilginin güvenli iletimini sağlar. Bunlardan birinin eksikliği, sorunları ortaya çıkarır.

Siber tehditlerle mücadele etmek için hızlı tepki veren, aynı zamanda asimetrik organizasyonlar geliştirilmelidir. Bunu sağlamak içinse; olayı en derin noktasına kadar anlamak gerekir.[775] Ayrıca, sistemler içerisinde protokoller, sistemin kendisinden kaynaklı ortaya çıkan açıklıkların tespit edilip, ortadan

[768] Çiftçi, *Her Yönüyle Siber Savaş*, 253.
[769] Ünal, "Dağıtık Servis Dışı Bırakma (DDOS) Saldırıları: Güncel Yöntemler ve Mücadele," 14.
[770] Florian Skopik, Giuseppe Settanni, ve Roman Fiedler, "The Importance of Information Sharing and Its Numerous Dimensions to Circumvent Incidents and Mitigate Cyber Threats," içinde *Collaborative Cyber Threat Intelligence,* ed. Florian Skopik (Amerika: CRC Press, 2018), 155.
[771] "Private-Public and Non-Governmental Organizations (NGOs)," içinde *Global Initiatives to Secure Cyberspace*, ed. Seymour Goodman ve Michael Portnoy (Amerika: Springer, 2009), 89.
[772] Keleştemur, *Siber İstihbarat,* 127.
[773] Kamil Yılmaz, Murat Güneştaş ve Oğuzhan Başıbüyük, "Siber Terörizm: Motivasyon ve Yöntem," *Siber Suçlar: Tehditler, Farkındalık ve Mücadele*, ed. Fatih Tombul vd. (Ankara: Global Politika ve Strateji Yayınları, Ocak 2015), 92-93.
[774] Çiftçi, *Her Yönüyle Siber Savaş*, 250.
[775] Bıçakçı, *21. Yüzyılda Siber Güvenlik*, 50.

kaldırılması ya da aza indirgeyecek teknolojilere geçilmesi kolaylık sağlayacaktır.[776] Bilgi ve eğitimli kişilerin sayesinde, oluşabilecek açıklık problemlerini en aza indirgemek gerekir. Teknolojinin hızlı ilerlemesi, eğitimin artışı, problemleri azaltmayı ileri yıllarda daha kolaylaştıracaktır. Günümüzdeyse kullanıcı ve sistemlerin çoğu siber risk altındadır.

Risk, üerine çalışmalar yapılabilecek bir konumdadır. Riski en aza indirmek, risk için önlem almadan çok, riskle yaşamayı öğrenmek, davranışları ona göre şekillendirmeyi içerir. Risk yönetimi; riskin analiziyle başlar, devamında var olan açıklığın tespiti yapılarak, risk analiziyle, oluşabilecek riskin kontrolü yapılıp, riskin boyutuna göre çözümler üretilir.[777] Risk kontrolünü yapacak kişileri yetiştirmek, bu alan için istihdam edilmesi gereken kişiler ve özel çalışma alanına ihtiyaç duyulmaktadır. Benzer ve daha geniş çaplı çalışmalar, siber alan için de geçerlidir. Siber alanda, ulusal birçok farklı kurumun birlikte çalışması önemlidir. Ayrıca, kurum içerisinde istihbari, teknik, operasyonel birimlerin eşgüdümlü hareket etmesinin bir önemi vardır. Alanlarında uzman, teknolojinin hızlı gelişimine ayak uydurabilen personelle çalışmalar yürütülerek, eğitim desteğinin aynı seviyede sağlanması önemli olmaktadır.[778] Siber alan, hızlıca gelişen bir alandır. Eğitim ve gelişmeleri anlık takip etmek, bu alanda hem güvenlik, hem başarı sağlamak için önemlidir. Çalışmalar yapılırken; tehditlere, risk üzerinden dikkat etmek gerekir.

Tehdit sayılabilecek bir nokta; internetin özgür dolaşım hakkının devletlerin belirli olaylarda kontrol sağlayamaması, bunda medyanın etkisi olduğu düşüncesini getirmektedir. Bunun zıt biçiminde davranan devletlerse, bireylerin özgürlüklerini ihlal ediyor görünüp, siber savaş ihtimalini öne çıkarabilmektedir.[779] Durum iki açıdan değerlendirilebilir. İlk bakış açısı olarak; bireylerin haklarına sınırlamalar gelmesi, kişilerin özgürlüklerini, en önemlisi bilgiye erişim hakkının elinden alınması olarak görülebilir. Diğer bir açıdansa; devletin belirli ölçüde sınırlama getirmesi, kendi halkını propaganda ve zararlardan koruyarak, önüne geçilmesini sağlayacak bir yöntem olmaktadır. Devlet bazı konuları, kendi yararı ve bütünlüğü için kontrolünde tutmalıdır. Ancak, her alanda bir kontrol olması problemler yaratır. Siber alanda bir kontrol

[776] Yılmaz ve Salcan *Siber Uzay'da Güvenlik ve Türkiye*, 71.
[777] Yılmaz ve Salcan *Siber Uzay'da Güvenlik ve Türkiye*, 73-77.
[778] Çakmak ve Altunok, *Suç, Terör ve Savaş Üçgeninde Siber Dünya*, 221.
[779] Bıçakçı, *21. Yüzyılda Siber Güvenlik*, 50-51.

oluşturulması, dikkatli çalışılması gereken bir konudur. Ancak, çıkabilecek problemler tehditleri oluşturmaktadır. Problemlerin en büyük yol açabileceği sonuç; siber savaştır.

Siber alanda bir siber savaşın, fiziksel savaşa dönüşmesine engel olabilecek belirli durumlar vardır. Bunlar içerisinde caydırıcılıktan söz edilebilir. Caydırıcılık, teorik olarak 1950'li yıllara dayanmaktadır.[780] Caydırıcılık teorisinde, kişi, yaptığı davranış sonucunda, karşılaşabileceği fayda ve zararları ölçerek, davranışlarına karar vermesini içerir. Caydırıcılık teorisi; cezaların keskinliği ve şiddetliliği üzerinden iki sonucu barındırarak uygulanmaktadır. Ceza olarak riskin artması, suç karşısında alınacak cezanın şiddeti; suçu işleyecek kişi üzerinde bir caydırma unsurudur.[781] Caydırıcılık teorisinde ilk belirlenmesi gereken unsur; kime karşı caydırıcılık yapılacağıdır. Siber alandaysa muhatap bulmak oldukça zordur. Siber alanda, ilk saldıranı ortaya çıkartmak zordur. Belirlenecek olası bir aktör karşısında, sonraki adım, kuvvet kullanımı açısından eşit ya da fazlası yapılarak karşılık verileceğine dair taahhüttü içerir. Ancak, siber alanda, her zaman bir eşit karşılık verilmesi söz konusu değildir. Caydırıcılıkta, Soğuk Savaş dönemine bakıldığında; benzer sonuçların ortaya çıkma ihtimali bulunmaktadır. Savaşın önüne geçmeden çok, Soğuk Savaş Dönemindekine benzer silahlanma yarışına sebep olabileceği düşünülmektedir.[782] Siber caydırıcılıksa; siber bir saldırıda, riskleri makul seviye ve maliyete düşürmeyi sağlamaktır. Kriminal ve nükleer caydırıcılıktan farklı olan siber caydırıcılık; saldırganın silah bırakması, hükümetin düşmesi gibi sonuçları barındırmaz.[783] Caydırıcılık genel olarak; zararların oluşmasını aza indirmek için, aktörü, yapacağı eylemden çeşitli yöntemlerle vazgeçirmeyi kapsar. Siber alanda caydırıcılık biraz daha farklı işlemektedir. Günümüzde, aşırı tehdit içermeyen, cezalandırma gibi sonucu çok sert bulunmayan alanda, caydırılacak aktörün dahi bulunamaması sorunlar oluştuğu için, caydırıcılık problemli olmaktadır. Ancak, caydırma amaçlı çalışmalar, alan için bir ihtiyaçtır. Öncelik olarak, alanın ciddiyeti üzerinde durulmalıdır. Sonrasında, alınabilecek cezalar, ortaya

[780] Singer ve Friedman, *Siber Güvenlik ve Siber Savaş*, 198.
[781] Fatih Tombul, "Kamu Yönetiminde Siber Suçlara Karşı Kullanıcılarda Farkındalık Oluşturulmasının ve Kurumsal Bilişim Güvenlik Politikalarının Oluşturulmasının Önemi," *Siber Suçlar: Tehditler, Farkındalık ve Mücadele*, ed. Fatih Tombul vd. (Ankara: Global Politika ve Strateji Yayınları, Ocak 2015), 143.
[782] Singer ve Friedman, *Siber Güvenlik ve Siber Savaş*, 198-200.
[783] Çiftçi, *Her Yönüyle Siber Savaş*, 345-347.

çıkabilecek tehlikeli sonuçların farkına varılarak, bazı konularda aktörleri durdurucu biçimde olmalıdır. Olayı gerçekleştiren kişi ya da aktörlerin tespiti için farklı çalışmalar yapılıp, etkili olunması, caydırıcılıkta önemlidir. Siber alanda daha birçok çalışma yapılması gerekir. Özellikle uluslararası alanda, siber alan için çalışmalara yenileri eklenmesi gerekir.

Uluslararası alan, siber alanın gelişmesiyle daha anarşik bir görünüm almıştır. Siber alanı düzenleyecek bir uluslararası hukuk olmaması, devletlerarasında rekabetin ön plana çıkması, şiddeti getirmiştir. Uluslararası sistem, eski hâlinden daha güvensiz, belirsiz bir biçime gelmiştir.[784] Uluslararası alanda barışın sağlanmasındaki zorluk; sistemin yapılanma biçiminden kaynaklıdır. Çağdaş siyaset kuramına bakıldığında, barış sağlanması için ortaya atılan sorulara dolaylı yanıtlar verilerek, devletlerarası ilişkilerden çok, devletin ve kendi toplumu içerindeki barışın çözülmesine eğilmişlerdir. Düşüncede, düzenleyici bulunmadığı sürece; kişilerin hak, özgürlük, güvenlik, ahlaklı yaşamak için, beklenen şekilde sürdürülmesini sağlayacak temel yapının devlet olduğundan söz edilmektedir. Klasik siyaset kuramında; egemen devlet anlayışı üzerinden oluşturularak, uluslararası ilişkiler, savaş ve barış için benzer şekilde bahsedilmiştir. Barışın ve düzenin ülke devletlerinin mevcut biçimde devamıyla sağlanabileceğinden söz edilmiştir.[785] Uluslararası anlamda oluşması gereken bir güvenlik için, ulusal düzeyde çözümlerden, geçmişteki gibi ulus üzerinden bir barış söylemi yapılması, günümüzde, uluslararası alanda barışı, yine ulusal bir düzeye indirmektedir. Uluslararası alanda yapılacak bir barış için, daha küresel açıdan bakmak gerekir. Ulusal alanda yapılan çalışmalar genelde yetersiz, uluslararası alan için problem oluşturacak bir şekil alır. Uluslararası alan, ulusların üzerinde bir alan olması sebebiyle, farklı çalışmalara ihtiyaç duyar. Siber alan, uluslararası alan içerisinde düşünülmesi gereken güvenlik konularından biridir. Hem ulusal, hem uluslararası çalışılabilecek alan için belirli koşulları göz önünde bulundurmak gerekir.

Genel anlamda; güvenlik oluşturmak için, belirli koşullar sağlanmalıdır. Zaman açısından öngörülü olmak, ileriye yatırım yapmak, tehdidin belirlenmesinde algılara önem vermek, birey ve toplumu dâhil ederek güvenlik

[784] Darıcılı, *Siber Uzay ve Siber Güvenlik*, 128.
[785] Faruk Yalvaç, "Savaş ve Barış," içinde *Devlet ve Ötesi,* der. Atilla Eralp (İstanbul: İletişim Yayınları, 2014), 251-253.

çalışması yapmak, çift taraflı ilişki içerisinde güvenlikten söz etmek, bir güvenlik oluşturulmasında önemli noktalardır.[786] Söz edilen noktalara dikkat edilerek yapılan güvenlik çalışmaları, uluslararası alanda önemli yer tutar. Güvenliğe uluslararası alanda, özellikle siber alanda ihtiyaç vardır. Çalışmalar birçok ülke ve örgüt tarafından yapılmaktadır. Ancak tamamen yeterli olduğu söylenememektedir. Yeterli olunamadığında, siber savaşın görülme olasılığı vardır.

Tehditler üzerinden incelendiğinde; günümüzde bir siber savaş, fiziksel bir savaşa tam olarak dönüşmemiştir. Ancak, bu ihtimalin oluşması ve kıyısına gelinmesi uluslararası alanda görülmüştür. Bir siber savaşın, fiziksel savaşa dönüşmesi ihtimali için bir değerlendirme yapacak olursak; Stuxnet gibi bir solucan sayesinde, benzer bir biçimde sisteme girilmesi, bir olay tetikleyicisi olabilir. Başka bir açıdan bakarsak; bir virüs, solucan ya da programa tam olarak güvenmek yanlıştır. Programlar üzerinden yazılan, oluşturulan birçok programın hata verme olasılığı yüksektir. Stuxnet gibi bir solucanın, nükleer sistemde, bir hata sonucu sistemi harekete geçirmesi, fiziksel anlamda büyük zararlar oluşturabilme ihtimalini göstermiştir. Böyle bir olay sonrasında, günümüzde durgun olmayan uluslararası ilişkilerde, gerginliğin daha çok artması, fiziksel bir savaşa geçilebileceğinin göstergesidir.

Genel olarak; böyle bir olayın ortaya çıkması; her devlete belirli zararlar vereceği bilinmektedir. Her devlet aynı miktarda zarar görmez. Zarar, devletin savunma gücü ve saldırı yapan aktörün gücüne bağlı olarak değişmektedir. Bu ihtimaller göz önüne alındığında, ulusların üzerinde olabilecek bir kuruluş düşüncesi, en azından olayların çok büyük boyutlara ulaşmadan engellenmesini sağlayabilecektir. Böyle bir kuruluşta; katılan üyelerin ciddi derecede çalışıp, burada alınan kararlarınsa bağlayıcı olması gerekir. Sadece katılan devletler değil, tüm aktörler üzerinde etkili olmalıdır. Kuruluş, sadece siber alan odaklı olmalıdır. Diğer alanlarla ilgilenmek yerine, tek odak noktası siber alan olup, her türlü çalışma burada yapılmalıdır. Farklı alanlarda uzman kişilerin de, siber alanın ilgili olduğu alanlarındaki sorunlara çözüm geliştirilmesine yardımcı olmalıdır. Olabilecek en tarafsız biçimde ilerlenmelidir. Belirli sürelerde üye devletler yönetime sırayla gelmelidir. Aynı zamanda, ilk çalışmalar, devletlerin siber alana

[786] Dedeoğlu, *Uluslararası Güvenlik ve Strateji*, 83-84.

dair yeteneklerinin belirlenmesi olmalıdır. Eğitimin ön planda olması gereken kuruluşta, güncel antlaşma ve yasalar takip edilmelidir. Ortak çalışmalarla, sadece siber alana yönelik, tüm ulusların uyması gereken, uyumlu yasaların belirlenmesi sağlanabilir. Bu sayede, en azından siber suçlar ve saldırıların sınırlarının belirlenmesine yardımcı olacak adımlar atılabilir.

Kuruluşta; en gelişmiş sistemler ve devletlerin kapasiteleri paylaşılarak, devlet dışı aktörlerin saldırılarına karşı önlemlerin alınmasına yardımcı olabilir. Devletlerarasında, sadece siber alanda yaşanan bir anlaşmazlık ve tehdit üzerine tespitler yapılarak, politik açıdan, devlet ilişkilerinde bir tehdidin ortadan kaldırılmasına yönelik çalışmalar yapılabilir.

Siber alanın, güvenlik alanları içerisinde farklı bir boyutta olması sebebiyle; bazı konularda farklı yaklaşılması gerekir. Güvenlik alanının geliştirilmesi için; eğitim en önemli noktadır. Eğitim için; bu kuruluşta, her devletten en az bir temsilci ya da grup bulunmalıdır. Herhangi bir gelişmede, yeni teknolojinin ortaya çıkışında, her devletin buna ulaşması için belirli eğitim ve standartların öğrenimi kuruluş içerisinde yapılmalıdır.

Ulusal düzeyde, internette belirli ayrım ve sınırlamalar olmalıdır. Ancak bu kontrol ve sınırlama, kişi hak ve özgürlüklerine ters düşecek biçimde değil, daha çok filtreli bir internet yapısı şeklinde olmalıdır. Bu sınırlamalar; internetin kontrol edilemez yapısını düzenlemeye yardımcı olabilecektir. Aynı zamanda, devletlere zarar verebilecek örgütlerin, erişim hakkı olmayan üçüncü kişilerin, her an her bilgiye erişmesinin önüne geçebilecektir. Ancak, bilgi erişimini tamamen yok etmemelidir. Hükümetler, aynı sistemden bilgi paylaşımı yapmaktadır. Ağları belirli ölçüde filtrelemek; hükümetler için önemli verilerin, iletilmesi gereken taraflara açık olmasını sağlayıp, bilgiye erişmemesi gereken taraflara kapalı olması, güvenli bilgi aktarımı ve sistemi oluşacağını gösterir. Daha önemlisi; aktörlerin siber alana daha çok eğilmesi, bunun için çalışmalar yapma isteğinde olması gerekir.

Genel anlamda; uluslararası sistem, anarşik olmasına karşın, belirli konularda üzerinde düzenlemelerin yapılmasına açık bir yapıdadır. Siber alansa; sınırı olmayan bir alandır. Bu iki alanın küresel sistem içerisinde bir arada olması, pek çok olasılık ve tehdidi bir araya getirir. NATO, Avrupa Birliği gibi yapılar, oluşumunda belirli tehditler üzerinden, ihtiyaç duyulduğu için bir araya gelmiştir. Siber alan da, bir kuruluş oluşturulması, en azından standart ya da teknolojik

düzenlemelerden ileri bir seviyede, politik, hukuksal, eğitimi barındıran önemli bir yapılanmaya ihtiyaç duymaktadır. Siber alan, gün geçtikçe büyümekte, gelişmelerine devam etmektedir. Ancak, bunun yeni tehditler getireceği bilinmektedir. Günümüzde, bir savaş ihtimali üzerinde yaşayan, bunun oluşmaması için çalışmalar yapan devletler, siber alanın getireceği bir savaşa karşı daha ciddi çalışmalar yapmalıdır. Her devlet kendi çalışmalarını yürütür. Ancak, ilerleyen dönemlerde, teknolojinin geleceği, tehditlerin getirecekleri tam olarak bilinmez. Günümüzde belirlenen standartlar, yapılan antlaşmalar, oluşturulan, devletlere bağlı olmayan kuruluşlar, her devleti kapsamadığı gibi, her koşul için ortak çözümler vermemektedir. Ancak, bunların hepsinin bir arada, tek kuruluş altında toplanması; dağınık bulunan, belirlenmiş hareket çizelgelerinin toparlanmasını, olası bir tehditte verilecek en hızlı cevabın ortaya çıkmasını sağlayacaktır. Siber alanda, bugün söylenen ya da yapılan girişimler, bir gün sonra eski kalabilir. Ancak, eğitimler sayesinde, çözümlerin uzun soluklu olması sağlanabilir. Her şeyden önce; belirli bir birliğin sağlanması, pek çok olumsuzluğun önüne geçilebileceğini gösterir.

DÖRDÜNCÜ BÖLÜM

GENEL DEĞERLENDİRME

Uluslararası alanda önemli birçok çalışma yapılmıştır. Çalışmaların en önemlilerinden biri güvenliktir. Güvenlik; birey, toplum ve sistemleri kapsarken, her alanda kendini göstermektedir. Genel yapılan tanımlamalar yetersiz kalmakta, ancak tam bir tanımlama yapılması zor olmaktadır. Zorluğu; aktörün içinde bulunduğu şartlar ve algılamalarına göre, güvenlik ve güvensizliğin ortaya çıkışının değişim göstermesi kaynaklıdır. Güvenlik her alanda görülmekte, her yapının içerisinde çalışılması ve korunması gereken özelliklerden biri haline gelmesine sebep olmaktadır.

Güvenlik üzerine en bilinen çalışmalar, uluslararası alanda yapılmıştır. Pek çok devlet ve örgütün çalışmalar yaptığı bu alan, kendi içerisinde bölümlere ayrılmaktadır. Günümüzdeyse ön plana çıkmaya başlayan bir güvenlik alanı bulunmaktadır. Birçok alanda, uluslararası sistemde çalışma yapan aktörler, çağımızın önemli yapılarından biri haline gelen, siber alanda da güvenlik çalışmalarına başlamıştır. Ancak, çalışmalar yeterli değildir. Alan olarak, önemi yeni ortaya çıkmış, çalışmaları bu paralelde dikkat çekici olmaya başlamıştır. Siber alan, daha çok teknolojik yapılar içerisinde düşünülmektedir. Ancak, tek bir alana hapsedilmesi, çalışma alanlarını kısıtlar. Siber alan, tek bir alan ya da teknolojiyle kısıtlı değildir. Pek çok alan ve sistemin içerisine yayılmış bir yapısı vardır. Siber alan, özellikle uluslararası alanda, ciddi boyutlarda kendini göstermeyi başarmış, üzerinde tek başına çalışılması gereken bir önem kazanmıştır.

Siber alandan söz edildiğinde ilk akla gelen internettir. Ancak, siber alan daha çok; elektronik cihazları, siber sistemler üzerinden bağlı bütünlüğün tamamını kapsayan, geniş bir alandır. Aynı zamanda, sistemler dışında kullanıcılar ve sistem üzerindeki iletişimi de kapsamaktadır. Günümüzde siber alandaki iletişimin sağlayıcısı internet olduğu için, alandan söz edildiğinde ilk

akla gelen önemli yapılardan olmuştur. İnternet ortamı; ilk, üniversiteler arasında iletişimi sağlamak amaçlı çıkmıştır. Sadece belirli bir grup içerisinde iletişim için ortaya çıkmış olması, güvenlik kaygısı duyulmamasına sebep olmuştur. İnternet geliştikçe, problem ve tehditler o derece ortaya çıkmaya başlamıştır. Ancak, güvenlik amaçlı çalışmalar, tehditler ilerlemeye başladıktan sonra daha çok ortaya çıkmıştır. İnternetin iletişim konusunda aracı bir yapı olması, oluşacak bir tehditte ayrıca ciddi önem taşımaktadır.

Tehditler, özellikle siber alanda birçok sonuç ortaya çıkarmaktadır. Tehditlerin ortaya çıkmasındaysa belirli aktörlerin bulunduğu bilinmektedir. Bazı olaylarda, siber alanda önemli aktörlerden biri olan hackerlar akla gelir. Ancak, hackerlar sadece olumsuz anlamda düşünülmemelidir. Hackerlar yaptıkları eylemlere göre sınıflandırılırlar. Hackerlar; siber alana dair en çok bilgi sahibi olan, bu alanda belirli eylemler gerçekleştiren kişiler içerisindedir. Yaptıkların eylemlere ve sonuçlarına göre hackerlar kendi içlerinde ayrılmaktadır. Ancak, siber alandaki tüm tehditler hackerlar tarafından gerçekleşmemektedir. Siber alana herkesin erişim imkânı bulunmaktadır. Herkesin kullanım amacı farklıdır. Bir kısım günlük amaçlı kullanırken, bir kısım uluslararası alanı etkileyecek düzeyde çalışmalar yaparlar. Bu çalışmalarla olumlu ve olumsuz sonuçlar ortaya çıkar.

Siber alan önemli olarak iki ana biçimde tehdit altına girer. Bilgisayar ortamı üzerinden ve stratejik siber tehditler olarak ikiye ayırmak mümkündür. Bilgisayar ortamı üzerinden gelebilecek tehditler; daha çok yazılım ve sistem üzerinden tehditlerdir. Ancak, kullanım biçimlerine göre tehdit boyutları değişebilmektedir. Teknik sorunları içerebilirken, aynı zamanda, stratejik amaçlı tehditler de ortaya çıkabilmektedir. Bilgisayar ortamındaki tehditlerin, kullanım şekillerine göre, stratejik bir tehdide dönüşme olasılığı her zaman altta yatan sonuçlardan biridir. Stratejik tehditler; uluslararası alanda, aktörler arası gerginliklere sebep olup, belirli amaçlar üzerinden yapılmaktadır. Stratejik tehditlerin önemli olmasının sebebi; uluslararası alanda etkili olarak, önemli sonuçlar ortaya çıkartabilecek kadar etkili olabilmesidir. Ayrıca, bir amaç için araç haline dönüşmesi, uluslararası alanda, özellikle izlenen politikalar üzerinden önem kazanmasına sebep oluştur. Siber alanda en tehlikeli stratejik tehditler; terör ve savaştır. Siber terör; insanlarda korku yaratıp, bunu yaşatmak için belirli çalışmalara bu alanı dâhil ederek yapmayı içerir. Alanın herkese açık bir biçimde erişimi ve üzerinden iletişim sağlanmasıysa pek çok konuda siber terör için bazı

koşulları kolaylaştırmaktadır. Siber savaş; belirli aktörler arasında, belirli sınırlara dayanarak yapılan savaşlardır. Alan üzerinden ilerleyen savaşlar, günümüzde farklı bir boyutta ilerlemektedir. Aktörlerse daha çok devletlerdir. Bu sebeple; uluslararası ilişkiler alanında önem kazanmaya başlamıştır. Daha önemlisi; siber alan üzerinden istihbarat yapılabilmektedir. İstihbarat, en önemli bilgilere erişimi sağlayabilir. Siber alanda; en önemli bilgiler, veriler içerisinde bulunmaktadır. Genellikle erişilen veriler, normal bir biçimde ele geçirilmesi zor, ciddi derecede önem taşıyan verilerdir. Günümüzde pek çok devletin önemli bilgilerini siber alana taşımış olmasıysa, özellikle istihbaratta dikkat edilmesi gerektiğini göstermektedir. İstihbarat, diğer alanlardan ayrı düşünülmesi gereken bir çalışmadır. İstihbaratın hangi taraf için kullanıldığı önemlidir. İstihbarat yapılan ülke için bu tehditken, istihbarat yapan ülke için bu savunmasına bir katkıdır. İstihbarat hem savaş stratejisi olarak kullanılabilirken, aynı zamanda bir savunma stratejisi olarak düşünülebilir. Uluslararası alanda, özellikle devletler gibi önemli aktörlerin uğrayacağı saldırılara karşı, belirli savunma yöntemleri geliştirilmesi gerekmiştir. Saldırıların gittikçe tehlikeli boyutlara çıkması, savunma üzerine çalışılması gerektiğini göstermiştir.

Günümüzde, aktörler savunma için kendilerini geliştirmekte, çalışmalar yapılırken, geçmişini bilerek yapılması önemli bir nokta olmaktadır. Alanın geçmişini bilmek, geleceğinde oluşacak tehdit ihtimallerini değerlendirmeye yarayacak en önemli özelliktir. Siber alanın geçmişinde; elektronik sistemlerin, uluslararası alanda, belirli çalışmalar amaçlı kullanılması yatmaktadır. Elektronik sistemlerin bağlı olduğu yapılar, siber alana girmektedir. Bu sebeple; siber alan, eskiden beri önemli yapılardan olmuştur. Ancak, özel olarak bir çalışma üzerinde gösterilmemiştir. Önceki dönemlerde siber alan üzerinde ayrı çalışılmadığı için, alanın geçmişine bakıldığında, başka olaylar içerisinden çıkartmak mümkün olmaktadır. Günümüzde yapılan çalışmalarda zorluk çıkmasının altında yatan sebeplerden biri bu olmaktadır. Bir alanda çalışmalar yapılacağı zaman, öncelikle geçmişindeki olaylara bakmak gerekir. Ancak, zamanında ayrı bir alan olarak önemli görülmemiş olması, günümüz çalışmalarına yansımıştır.

Siber alan için yapılan çalışmaları, özellikle politikaları, devletler ve örgütler yapmıştır. Siber alanın özel bir alan olmasından, ayrıca, çalışmalara geç başlanmasından dolayı, istenilen ölçüde sonuçlar alınamamıştır. Siber alanın sınırlarının olmamasıysa farklı sorunlar ortaya çıkarmıştır. Devletler ve örgütlerin

çalışmaları belirli sınırlar içerisinde kalmıştır. Ancak, olaylar, tek bir sınır içerisinde kalamamıştır. Siber alanın kendi yapısı gereği, ortaya çıkan bir olay, anında çeşitli aktörü etkileyecek konuma gelmiştir. Etki alanı, tehditlerin tehlike boyutuna çıkabilecek ölçüde gelişmesine sebep olmuştur. Bu sebeple; hem güvenlik alanında hem uluslararası alanda çalışılması gereken bir konuma gelmiştir.

Günümüzde, siber alanda çeşitli uluslararası çalışmalar yapılmıştır. Siber alanda bir siber savaş ihtimaliyse yüksektir. I. Dünya Siber Savaşı yaşandığı bu dönemde, olayların zamanla daha tehlikeli boyutlara gelme ihtimali vardır. Birçok olayda, fiziksel savaşların eşiğinden dönülmüştür. Aynı zamanda, pek çok olay sonucu biriken, gerginleşen bir uluslararası sistem ve ilişkiler mevcuttur. Günümüz koşullarında, daha gergin bir ortamda bulunduğumuz bir gerçektir. Böyle bir ortamda, her çeşit tehlikenin ortaya çıkma ihtimali vardır. Günümüzdeki tehditler, her an farklı biçimde, fiziksel bir savaşa dönüşmeye sebep olacak altyapıya sahiptir. Özellikle siber tehditlerin sorumlusunun belli olmadan ilerleyen bir yapısı olması, uluslararası alan için, ilişkilerde yıpratıcı bir rol oynamaktadır. Uluslararası alanda, siber tehditlerin henüz büyük sonuçlar oluşturmaması, olaylara gereken ciddiyet verilmemesine sebep olmaktadır. Ancak, tehditlerin ilerleyiş hızına göre, çalışmalar yapılmasına rağmen yeterli olmamaktadır. Siber tehditlerin sonuçlarının bilinmemesiyse daha büyük bir problem oluşturmaktadır. Yapılan çalışmalarda, uluslararası anlamda kesin bir bağlayıcılık bulunmamaktadır. Siber alan, kesin bir sistem ya da aktöre bağlı değildir. Devletlerin yaptıkları bu çalışmalarla, sadece kendi sınırları içerisinde geçerli olması, tehlikelerin önüne tam anlamıyla geçilmesine engel olmaktadır. Bir tehlikenin önüne geçmek için; öncesinde belirli çalışmalar yapılıp, yaşanan olaylardan ders çıkartılarak, belirli bir sistem kurulması gerekir. Kurulan sisteminse tarafsız olup, her üyeye açık, aynı zamanda eğitim ve eksiklikler için çalışmalar yürütebilmesi gerekir. Siber alanın sınırlarının olmayışının zorluklarıyla baş edebilecek çalışmalar, belirli sınırların çizilmesini sağlamalıdır. Siber alan daha farklı görülerek, çalışmalar bu yönde olduğu sürece, yaşanacak olaylarda tepkiler daha dikkatli, hatta önüne geçilebilecek şekilde olacaktır.

Siber alan, bir gün önceki gelişmelerden ileride olmaktadır. Sadece sistemsel olarak değil, teknoloji, düşünce hatta politikalar açısından hızlı şekilde gelişme göstermektedir. Gelişmelere sebep olan aktörler olmakta, ancak, amacın

dışında kullanımın önlenmesi esas noktadır. Siber alan, başka alanlar içerisinde kalmayıp önem verilmesi, üzerinde daha çok çalışılması gereken bir noktaya gelmiştir. Sadece belirli bir alanın içerisinde düşünmek, siber alanın kendi kullanım alanlarında sorun oluşturur. Siber alanın, sadece mühendislik alanında düşünülmesi, teknoloji ve dijital sistemler üzerinde olmasından kaynaklıdır. Ancak siber alana bağlı olan; ekonomi, politika, askeri, uluslararası alanların yaptığı siber çalışmalar, tek bir alana ait olarak söz edilirse, geride kalmasına sebep olacaktır. Bu sebeple; siber alanda yapılan çalışmalar, uluslararası alanda, özel bir konumda değerlendirilerek, siber alan altında toplanıp, incelenmesi daha doğru olacaktır. Çeşitli alanların çalışmalarının bir arada toplanabileceği bir yapının bulunması, atılacak adımlarda önemli yer tutacaktır. Günümüzde, tek başına bahsedilen siber alanın güvenliği için yapılan çalışmalar, uluslararası alanda belirli bir önem görse bile, yeterli değildir. Yeterince önem verilmemesi, ileride yaşanacak olaylarda, sistemlerin önemli kısımlarında problem yaşanacağını gösterir. Bu sebeple; bütün aktörlerin, uluslararası alanda, siber güvenliğin önemine özel bir ilgi göstermesi, yaşanabilecek tehlikeli savaşlarınsa önüne geçebileceği düşüncesini arttıracaktır.

Genel olarak; uluslararası alandaki çalışmalar, gün geçtikçe çeşitlenip, farklı alanlar biçiminde ilgi görmeye başlamıştır. Özellikle güvenlik alanının, uluslararası alanda önemli bir yeri vardır. Ancak, kendisi üzerinde kesin bilgilerle çalışılamaması, gün geçtikçe yenilenen bir alan olması bazı zorluklar çıkarabilmektedir. Alanın kendi içerisinde, gelişmelerle ortaya çıkan siber alan, önem açısından yeterince ilgiyi yeni görmeye başlamıştır. Siber alanın genel içyapısına bakıldığında; sadece mühendislik alanının bir yapısı gibi görünmektedir. Ancak, pek çok alanın içerisinde dallarını barındıran özel bir yapıdır. Özellikle uluslararası alandaki yerinin önem kazandığı bilinmektedir. Siber alanın, pek çok alan içerisinde görülmesi, günümüzdeki teknolojinin, sistemin ve bilginin bu alana taşınmış olması kaynaklıdır. Siber alanın kullanımının yaygınlaşması, çeşitli kolaylıklar sağlamıştır. Ancak, kolaylıklar olumsuz amaçlar için de aynı derecede olmuştur.

Siber alanda önemli yeri olan internet, iletişim amaçlı kullanılması en önemli özelliğidir. Ancak, iletişimin kullanım amacı, siber alanın güvenliği açısından dikkat edilmesi gereken bir biçim almıştır. Siber alanda sadece iletişim değil, önemli altyapıların çalışma sistemleri de buraya bağlıdır. Bu sebeple;

devletler ve örgütler, uluslararası alanda, siber alan üzerinde çalışmalar yapmaktadır. Yeterli olmamasıysa, yeni çalışmalara itmiştir. Caydırıcı kurallar, belirli bir kesim için işe yaramaktadır. Bağlayıcı olmaması, problemi oluşturmaktadır. Bağlayıcılığın sağlanması için siber alanın belirli bir sınır ve aktöre bağlı olması gerekir. Günümüzdeyse bunu sağlayacak bir aktör ya da bir sınır bulunmamaktadır. Bağlayıcı olmaması; bu alanda belirli çalışmalar yapılmasını gerektirirken, eksik kısımları da giderilmelidir. Alanla alakalı, sadece bunu üstlenecek bir kuruluş bulunması gerekir. Ulusları aşan bir yapıda olması, hiçbir ayrım gözetmeden, sadece siber alanla alakalı çalışılmasını sağlayacaktır. Günümüzdeki bütün örgütlerin, bütün devletler ya da sistemlerden bağımsız olduğu söylenemez. Bu sebeple; özel bir yapı oluşturulması, siber alanın özelliklerinin tam olarak ortaya konulması açısından bağımsız olmasını sağlar. Belirli bir yapının oluşturulması, pek çok açıdan olumlu sonuçlar ortaya koyacaktır. Ancak, günümüz yapısında, aktörler arası rekabet ve gerginliklerin bu çalışmalarda etkisinin nasıl olacağı tahmin edilememektedir.

Uluslararası alanda, devletlerarası ilişkinin gerginliği; ufak bir sorunda kopacak kadar ciddi görünmektedir. Geçmişte yapılan antlaşma ve sözleşmelerin daha az önemi kalmıştır. Sistemlerin değişimi, eski anlaşma ve düzenin yetersiz kalmaya başlamasına sebep olmuştur. Günümüzde uluslararası sistem olarak önemli bir değişim ve gelişme sürecine girilmeye başlandığından söz edilebilmektedir. Henüz çok yeni bir değişim süreci olmasına karşın, en önemli etkiler teknoloji ve siber alanı kapsamaktadır. Siber alan artık önemli bir yere sahip olmaya başlamıştır. Siber alanda oluşacak bir gerginlik, her an bir uluslararası sorun çıkmasına sebep olabilecektir. Ortaya çıkacak bir sorun, sadece tek bir ülkeyi değil, her ülkeyi etkileyebilecek bir kapasitededir. Teknolojinin eskisinden fazla ilerlemiş olması, Soğuk Savaş Dönemindeki tehditlerin kat kat üzerinde olduğunu göstermektedir. Siber alandaki gerginliklerin fiziksel alana yansıması, Soğuk Savaş Dönemindeki tehditlerin üzerinde boyutlarda olabileceğini gösterir. Soğuk Savaş Dönemindeki tehditler, günümüzde dahi hâlâ tedirgin edici derecede bir seviyeye ulaşmıştır. Günümüzdeyse, Soğuk Savaş Dönemi tehditlerini geride bırakacak derecede ilerlendiğinden söz etmek mümkündür. Özellikle teknolojik açıdan; hem sistemsel olarak, hem eğitim açısından hem de savunma sistemlerinde büyük adımlar atılmıştır. Her sistemin siber alana bağlı olması, alanın ciddiyetini ortaya koymaktadır. Aynı zamanda,

pek çok devletin önemli belgelerinin sistem üzerinde veri olarak saklanması, siber alanı daha önemli kılmaktadır. Bu sebeple; siber alan eskisinden çok önem verilip, üzerinde çalışılması gereken bir alan olmuştur. Dünya Savaşları döneminde, devletler belirli amaçlar altında NATO'yu kurmuştur. Özellikle kuruluşunun temelinde; bir tehdide karşı birlik olmak yatmaktadır. Günümüzde benzer, ancak, farklı boyutta, siber alan için ayrı bir önlem alınmalıdır. İki tedbir arasındaki tek fark; NATO, kurulduğu dönemde, devletler birbirine karşı tedbir ve birlik için bir araya gelmiştir. Siber alan sadece devlet ya da grup üzerinden ilerleyen bir yapı değildir. Tehdit alanı geniştir. Sadece bir devlet değil, bir birey bile bir devleti tehdit edecek güce sahip olmaktadır. Siber alanın etkisi ve gücü kesin bir biçimde belirlenememiştir. Siber alanda ekonomi ve bilgi birikimi, en önemli yapıdır. Bilgi ve ekonomisini doğru şekilde sağlayan aktör, siber alanda rahat biçimde güçlenebilecektir. Güçlenen aktörse, uluslararası sistemde, güçler dengesini değiştirebilecek bir ilerleme sağlayabilecektir. Güçler dengesinde oluşacak bir değişimse, gergin bir uluslararası sistem için tehdit oluşturmaktadır. Bu sebeple; siber alan, çalışmalarla, özel ilgi gösterilmesi gereken bir alandır. Kendi adına bir kuruluşu hak edecek ölçüde olan bu alan, sadece tek bir yapı altında değil, genel bir yapı olarak düşünülmelidir. Tek bir sınırda kalması, çalışmaların da sadece o sınırlarda olmasına yol açar. Sınırlı bir çalışmaysa, günümüzdeki çalışmalar gibi, geçici ve yetersiz bir sonuç ortaya çıkartacaktır. Uluslararası alanda, siber güvenliğin sağlanması için, her alandan kişilerle çalışılarak, bir sistem ve çalışmalar geliştirilip, özel politika ve antlaşmalar sağlanması gerekir.

Yapılan çalışmaların günümüzde az oluşu ve siber alanın hızlı bir biçimde ilerlemesi her tehlikeye açık bir sistem içerisinde bulunduğumuzu göstermektedir. Gerginlikler ve sistemsel değişikliklerin yaşandığı, günümüz uluslararası sisteminde, her an oluşacak bir problem ya da savaş ihtimali içerisinde bulunduğumuz bilinmektedir. Henüz büyük bir problem çıkmamasının sebebi; siber alanın yeni oluşudur. Ayrıca, kullanım açısından henüz sınırlarının bilinmemesi, kullanıcılarınsa sadece belirli bir bölümünü kullanmasıdır. Yapılan siber saldırıların henüz tespit edilememesiyse, günümüzdeki gerginlikleri durduran bir noktadır. Siber alanda yapılan bütün çalışmalar, gün geçtikçe daha çok gelişmektedir. Devletler ve örgütler, önemli olaylar sonrasında siber alana dikkat etmeye başlamışlardır. Ancak, siber alanın ve uluslararası sistemin kendi yapısından dolayı yeterli değildir. Belirli önlemler ve çalışmalarla daha çok önem

gösterilmeye başlanması gereken alanda yapılan çalışmalar az görünmektedir. Ancak, kısa süre içerisinde büyük atılımlar yapılmıştır. İlerleyen dönemlerde daha iyi ve ciddi çalışmalar yapılması beklenen alanda, eğitim ve bilginin doğru kullanılması, büyük adımlar atılabileceğini göstermektedir. Dikkat edilmesi gereken; siber alandaki gelişmeleri daha özenle takip ederek, çalışmalarını, kendi alanı üzerinden yürütmektir.

SONUÇ

Bu çalışmada, uluslararası siber güvenlik ve siber ortamdaki tehditlerin fiziksel bir savaşa dönüşme ihitmali üzerine yapılabilecek çalışmalar hakkında bir inceleme yapılmıştır. Genel anlamda, öncelikle önemli yaklaşımlar üzerinden güvenlik tanımı yapılmaya çalışılmıştır. Güvenlik tanımı ışığında, günümüzde önem kazanmış siber alan ve onun güvenliğinden söz edilmiştir. Siber alan hakkında konular ayrı başlıklar altında incelenerek, bir teorik çerçeve oluşturulmuştur. Siber alan içerisinde özelliklerinden söz edilmiş ve tarihsel alt yapısı incelenmiştir.

Çalışmada öncelik olarak; teorik çerçeveyle, güvenlik ve siber güvenlik ayır ayrı incelenip, tehditlerinden bahsedilmiştir. Uluslararası ilişkilerde önemli bir yere sahip olan siber güvenliğin tanımının yapılması amacıyla ayrıca bir güvenlik tanımı yapılmıştır. Ancak, esas önemli olan, siber güvenliktir. Günümüzde daha çok önem kazanana bu alan ve özellikleri, yapılan ve yapılacak çalışmalar için önemlidir. Özellikle tüm cihazlar ve buna bağlı ortamları kapsayan siber alanın açıklanması, siber alandaki tehditlerin de önemini gösteren nokta olmuştur. Siber alanda tehditlerin çok çeşitli olduğundan bahsedilmiştir. Kişilerin yapmış olduğu kredi kartı numaralarının çalınması gibi bireysel suçlar siber alan içerisinde olsa da, uluslararası bir niteliği çok yüksek olmadığından daha az bahsedilmiştir. Ancak, siber savaşlar, siber terör uluslararası alanda ciddi sonuçlara sebep olduğu için önemli noktalardan olmuştur.

Tarihsel altyapıda; Birinci Dünya Savaşı Dönemi, başlangıç tarihi olarak alınmıştır. Bitiş noktası olarak günümüz belirlenmiştir. Özellikle, siber alanda önemli gelişmeler bu tarihlerde gerçekleşmiştir. Siber alanın elektronik bir biçimde savaşlara dâhil olmaya başlaması, teknolojinin hızla ilerlemesiyle internet yapısının ortaya çıkması önemli gelişmelerden olmuştur. Siber alanın gelişmesi ve günümüzdeki yapısına ulaşması, tarihteki birçok gelişmeye göre hızlı bir biçimde olduğu görülmüştür. İlk dönemde daha yardımcı bir yapısı olan siber alan ve

kullanımı, Soğuk Savaş Döneminde daha ön plana çıkmaya başlamıştır. Ancak, esas önemli konumunu, yakın dönem ve günümüze yaklaşıldığında almıştır.

Teorik bir çerçeve oluşturulduktan sonra, bu çerçeve üzerinden; ABD, Çin Halk Cumhuriyeti, Rusya Federasyonu, Federal Almanya Cumhuriyeti, İngiltere, Türkiye Cumhuriyeti devletleri ve Avrupa Birliği, NATO, Birleşmiş Milletler, Avrupa Konseyi örgütlerinin yaptıkları politikalar incelenmiştir. Aynı zamanda, gerginliklerin oluşma sebebi ve politikaların gelişmesinde önem taşıyan önemli olaylardan söz edilmiştir. Çeşitli olaylar içerisinde en dikkat çekici olanı; Stuxnet'tir. Stuxnet siber alanda ortaya çıkan en tehlikeli olaylardan biridir. Nükleer bir tesise, bu isimde bir solucanla saldırı yapılmıştır. Ancak, sonucunda olabilecek bir hata düşünülmemiştir. Tek bir hatayla tesiste oluşacak bir problem; sadece bulunduğu devlete değil, birçok aktörü etkileyecek niteliktedir. Bu gibi olaylar, bir tehdidin daha büyük tehlikelere yol açabileceğini göstermiştir.

Devletler ve örgütler üzerinden, fiziksel bir savaş ortaya çıkmasını engelleyecek çalışmalardan ayrıca bahsedilmiştir. Devlet ve örgütlerin yapmış oldukları çalışmalar önemli olmakla beraber yetersiz kaldığı da görülmektedir. Özellikle; ABD, Çin Halk Cumhuriyeti, Rusya Federasyonu bu konuda en önemli çalışmaları yapmış, ancak, yine günümüzde yetersiz kalabilmektedir. Bu üç devlet içerisindeyse, çalışmalarına aynı düzeyde devam edildiği sürece, Çin Halk Cumhuriyeti'nin siber alanda lider olabileceği dikkat çekicidi. Örgütlerin çalışmalarıysa daha az bağlayıcı olduğu için daha çok devletlere öneri biçiminde görülebilmektedir. Ciddi bir yaptırımı olmaması, örgütlerin daha geri planda kalmasına sebep olmuştur. Bu bölüm sonucunda; ilerde oluşabilecek tehditlere karşı yapılabilecek çalışmalar ortaya çıkmıştır. Ancak, devlet ve örgütlerin yaptığı çalışmaların hızlı bir biçimde geçersiz kalabildiği görülmüştür. Teknoloji ve siber alanın hızlı ilerlemesi, her geçen saniye politika ve çalışmaların yetersiz kalmasına sebep olmuştur.

Çıkan sonuçla; siber alanda güvenlik için özel bir kuruluşa ihtiyaç olduğu görülmüştür. Aynı zamanda, kuruluş içerisinde, yapılması gereken çalışmalardan üçüncü bölümde söz edilmiştir. Kuruluşun izlemesi gereken yöntemlerse bölüm içerisinde verilmiştir. Ancak yapılabilecek bir kuruluş için, yine en önemli öncelik eğitim olmaktadır. Eğitim ve bilginin doğru sağlanması, pek çok tehdidin önüne geçilmesinde etkili olacaktır.

Genel olarak; siber güvenlik üzerine çeşitli tehditler ortaya konmuştur. Devletler ve örgütlerin yaptığı çalışmaların belirli ölçüde kaldığı görülmüştür. Ancak, çalışmaların, özellikle teknoloji konusunda yetersiz kaldığı görülmüştür. Çalışmaların hızlı bir biçimde eski kaldığı dikkat çekicidir. Bazı devletler, yapılan çalışmalarda öncü görünmüş, bazıları geride kalmıştır. Örgütlerde; siber alanda çalışmalar yapmıştır. Ancak, bu çalışmalar yetersiz kalmıştır. Özellikle, örgütlerin bağlayıcı olmaması, caydırıcılığın yetersiz kalmasına sebep olmuştur. Bu da örgütlerin geri kalmalarına bir sebeptir. Hiçbir örgütünse tek amacı siber güvenlik değildir. Bu da; istenildiği ölçüde çalışmalar ortaya çıkmamasına neden olmuştur.

Uluslararası alanda bir siber savaşın devam ediyor oluşu önemli bir problemdir. Siber savaşın devam etmesi, yapılan çalışmaların yetersiz kalması, ciddi bir tehlike oluşturur. Bu sebeple; siber alanda yapılan çalışmalar arttırılmalıdır. Özellikle, eğitim ve kurumlar içerisinde, ayrı önem verilmelidir.

Çalışmada önerilen çözüm dışında başka bir sonuç daha ortaya çıkmaktadır. Siber alan, tek bir bölüm içerisine hapsedilmemelidir. Sadece mühendislik alanında değil, sosyal bilimlerde de yeni çalışmalar yapılması gerekir. Tehdit, günümüzde önemsiz gibi görülebilmektedir. Ancak, siber alanın hayatımızın her noktasını kapsadığı bilinmektedir. Siber alanın çeşitli alanlarda kendisini göstermesi, o alanları da tehdide açık bir konuma getirmiştir. Siber alan, planlanacak yeni çalışmalarla, beklenenden daha düzenli ve güvenli bir alana dönüşecektir. Aynı zamanda, siber alanda oluşabilecek bir savaş ihtimalinin önüne geçilmesini sağlayacaktır. Herhangi bir savaş ihtimali, tüm devletler ve bireyler için büyük, olumsuz sonuçlar ortaya çıkarır. Sadece maddi değil, manevi hasarlar oluşturarak, güvende olma durumunun ortadan kalkmasına sebep olacaktır. Bu sebeple; çalışmalar arttırılmalı, siber alana ayrı bir önem verilmelidir. Her alan içerisinde, ayrı bir biçimde incelenerek, özel bir önem gösterilmelidir.

KAYNAKÇA

"1. Siber Dünya Savaşı mı Başladı?." *Hürriyet Haber*. 28.12.2014. E.T.: 24 Ekim 2018. url: http://www.hurriyet.com.tr/avrupa/1-siber-dunya-savasi-mi-basladi-27856461.

"ABD ve Rusya Arasında Dijital Soğuk Savaş." *Hürriyet Haber*. 17.06.2019. E.T.: 16 Ağustos 2019. url: http://www.hurriyet.com.tr/dunya/abd-ve-rusya-arasinda-dijital-soguk-savas-41246160.

"Almanya'da Yüzlerce Siyasetçiye Siber Saldırı." *NTV Haber*. 04.01.2019. E.T.: 18 Ağustos 2019. url: https://www.ntv.com.tr/dunya/almanyada-yuzlerce-siyasetciye-siber-saldiri,tW74mFffvkm8o1g1h7FAsw?_ref=infinite.

"Ankara'da 'Bombalı Saldırı Olacak Söylentisi' Tunalı Hilmi Caddesini Boşattı." *SonDakika.com*. 15.03.2016. E.T.: 20 Temmuz 2018. url: https://www.sondakika.com/haber/haber-ankara-da-bomba-saldiri-olacak-soylentisi-tunali-8263166/.

"Ankara'daki Terör Saldırısı Sonrası Sokaklar Boş Kaldı." *Hürriyet Haber*. 15.03.2016. E.T.: 20 Temmuz 2018. url: http://www.hurriyet.com.tr/kelebek/magazin/ankaradaki-teror-saldirisi-sonrasi-sokaklar-bos-kaldi-40069679.

"Çin Ordusu Bilgisayarlarından Windows'u Kaldırıyor." *Hürriyet Haber*. 29.05.2019. E.T.: 17 Ağustos 2019. url: http://www.hurriyet.com.tr/teknoloji/cin-ordusu-bilgisayarlarindan-windowsu-kaldiriyor-41229612.

"Çin'in Siber Güvenlik Kanunu Yürürlükte." *Milliyet Teknoloji*. 02.06.2017. E.T.: 29 Eylül 2018. url: http://www.milliyet.com.tr/cin-in-siber-guvenlik-kanunu-teknoloji-haber-2461609/.

"International Intergovernmental Organizations." İçinde *Global Initiatives to Secure Cyberspace*, editör: Seymour Goodman ve Michael Portnoy, 11-32. Amerika: Springer, 2009.

"İngiltere'den Yeni Milli Güvenlik Yaklaşımı." *HaberTürk*. 28.03.2018. E.T.: 1 Ekim 2018. url: https://www.haberturk.com/ingiltere-den-yeni-milli-guvenlik-yaklasimi-1894107.

"Private-Public and Non-Governmental Organizations (NGOs)." İçinde *Global Initiatives to Secure Cyberspace*, editör: Seymour Goodman ve Michael Portnoy, 65-96. Amerika: Springer, 2009.

"Russian 'Invasion' of Crimea Fuels Fear of Ukraine Conflict." *The Guardian.* 28.02.2014. E.T.: 17 Ağustos 2019. url: https://www.theguardian.com/world/2014/feb/28/russia-crimea-white-house.

"Rusya'dan ABD'ye Siber Savaş Uyarısı." *Hürriyet Haber.* 17.06.2019. E.T.: 17 Ağustos 2019. url: http://www.hurriyet.com.tr/dunya/rusyadan-abdye-siber-savas-uyarisi-41246672.

"Rusya'ya Yönelik Siber Saldırılar ABD ve Avrupa'dan Yayılıyor." *Hürriyet Haber.* 28.06.2019. E.T.: 17 Ağustos 2019. url: http://www.hurriyet.com.tr/teknoloji/rusyaya-yonelik-siber-saldirilar-abd-ve-avrupadan-yayiliyor-41257587.

"Stuxnet ve Uluslararası Hukuk: Bir siber saldırının anatomisi." *Siber Bülten.* E.T.: 20 Ekim 2018. url: https://siberbulten.com/makale-analiz/stuxnet-ve-uluslararasi-hukuk-bir-siber-saldirinin-anatomisi/.

"Teledienstegesetz," E.T.: 2 Ekim 2018, url: https://dejure.org/gesetze/TDG.

"Türk Ordusunun Yeni Kuvveti Siber Savunma." *Hürriyet Haber.* 06.06.2016. E.T.: 20 Ağustos 2019. url: http://www.hurriyet.com.tr/teknoloji/turk-ordusunun-yeni-kuvveti-siber-savunma-40113652.

"Uluslararası Siber Güvenlik Federasyonu." *Uluslararası Siber Güvenlik Federasyonu* 2 (2017): 24-27.

"WannaCry Saldırısının Ardında Yatan Gerçekler." *CNN Türk.* 16.05.2017. E.T.: 10 Ağustos 2019. url: https://www.cnnturk.com/teknoloji/wannacry-saldirisinin-ardinda-yatan-gercekler.

ABD Savunma Bakanlığı. "The DoD Cyber Strategy." E.T.: 16 Ağustos 2019. url: https://archive.defense.gov/home/features/2015/0415_cyber-strategy/final_2015_dod_cyber_strategy_for_web.pdf.

ABD Savunma Bakanlığı. *DoD Strategy for Operating in Cyberspace.* Amerika: Temmuz 2011. E.T.: 17 Eylül 2018. url: https://csrc.nist.gov/CSRC/media/Projects/ISPAB/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf.

ABD Siber Komutanlığı. "About Us." E.T.: 16 Ağustos 2019. url: https://www.cybercom.mil/About/

ABD Siber Komutanlığı. "The Creation of U.S. Cyber Command." E.T.: 16 Ağustos 2019. url: https://www.cybercom.mil/About/History/.

Ağaoğulları, Mehmet Ali. *Sokrates'ten Jakobenlere Batı'da Siyasal Düşünceler.* İstanbul: İletişim Yayınlar, 2011.

Akdeniz, Gökşin. "Hacker Etiği." *Hack Kültürü ve Hacktivism: Yeni bir Siyaset Biçimi, Mustafa Akgül'e Armağan.* Derleyen: Ali Rıza Keleş, ve Yetkin Sal, 9-15. İstanbul: Alternatif Bilişim Yayınları, Temmuz 2013. E.T.: 27 Mart 2017. url.: https://ekitap.alternatifbilisim.org/files/hack-kulturu-ve-hacktivizm.pdf.

Akgül Durakçay, F. "Uluslararası İlişkilerde Liberal Yaklaşımlar ve Güvenlik Anlayışı," içinde *Uluslararası İlişkilerde Güvenlik: Teorik Değerlendirmeler*, derleyen: Emre Çıtak ve Osman Şen 7-21. İstanbul: Uluslararası İlişkiler Kütüphanesi, Eylül 2014.

Aktaş, Onur. *Siber Güvenlik: Hacking Atölyesi.* Ankara: Gazi Kitabevi, Ağustos 2017.

Akyıldız, M. Alparslan. *Uygulamalarla Siber Güvenliğe Giriş.* Ankara: Gazi Kitabevi, Ağustos 2015.

Alman Federal Adalet ve Tüketici Koruma Bakanlığı. "Act on the Federal Office for Information Security." E.T.: 2 Ekim 2018. url: http://www.gesetze-im-internet.de/englisch_bsig/englisch_bsig.html.

Alman Federal İçişleri Bakanlığı. "Cyber-Sicherheitsstrategie für Deutschland 2016." E.T.: 2 Ekim 2018, url: https://www.bmi.bund.de/cybersicherheitsstrategie/BMI_CyberSicherheitsStrategie.pdf.

Alman Federal Resmi Gazetesi. "Zweites Gesetz zur Bekämpfung der Wirtschaftskriminalität." E.T.: 2 Ekim 2018. url: https://www.bgbl.de/xaver/bgbl/text.xav?SID=&tf=xaver.component.Text_0&toc

f=&qmf=&hlf=xaver.component.Hitlist_0&bk=bgbl&start=%2F%2F*%5B%40node_id%3D%27288748%27%5D&skin=pdf&tlevel=-2&nohist=1.

Altınkaynak, Mustafa. *Uygulamalı Siber Güvenlik ve Hacking.* İstanbul: Abaküs Yayınları, Mayıs 2017.

Aslan, Özgür., ve Öner, Selcen. "İnternet Ekonomisi." *İletişim Dergisi* 26 (Ocak 2006): 5-19. E.T.: 6 Temmuz 2018. url: http://dergipark.gov.tr/download/article-file/212226.

Austin, Greg. "Middle Powers and Cyber-Enabled War: The Imperative of Collective Security." İçinde *Securing Cyberspace,* editör: Cherian Samuel ve Munish Sharma, 23-56. Yeni Delhi: Pentagon Press, 2016.

Avrupa Komisyonu. "Cybersecurity Strategy of the European Union: an Open, Safe, and Secure Cyberspace." E.T.: 3 Ekim 2018. url: https://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf.

Avrupa Komisyonu. "The Directive on Security of Network and Information Systems (NIS Directive)." E.T.: 3 Ekim 2018. url.: https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive.

Avrupa Konseyi. *Octopus Conference 2019.* Fransa: Mayıs 2019. E.T.: 25 Ağustos 2019. url: https://rm.coe.int/octopus-conference-2019-outline/1680948eba.

Avrupa Konseyi. "Commitee of Experts on Terrorism (2003-2017)." E.T.: 24 Ağustos 2019. url: https://www.coe.int/en/web/counter-terrorism/codexter.

Avrupa Konseyi. "Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data." E.T.: 15 Ekim 2018. url: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680078b37.

Avrupa Konseyi. "Convention on Cybercrime." E.T.: 15 Ekim 2018. url.: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680081561.

Avrupa Konseyi. "Cybercrime Convention Committee." E.T.: 25 Ağustos 2019. url: https://www.coe.int/en/web/cybercrime/tcy.

Avrupa Konseyi. “Cybercrime Programme Office (C-CPOC).” E.T.: 25 Ağustos 2019. url: https://www.coe.int/en/web/cybercrime/cybercrime-office-c-proc-.

Avrupa Konseyi. “Global Action on Cybercrime Extended (GLACY +).” E.T.: 25 Ağustos 2019. url: https://www.coe.int/en/web/cybercrime/glacyplus.

Avrupa Konseyi. “Global Project on Cybercrime Phase I.” E.T.: 16 Ekim 2018. url: https://www.coe.int/en/web/cybercrime/global-project-phase-i.

Avrupa Konseyi. “Octopus Cybercrime Community.” E.T.: 16 Ekim 2018. url.: https://www.coe.int/en/web/octopus/home.

Avrupa Konseyi. *Article 15 Conditions and Safeguards under the Budapest Convention on Cybercrime.* Fransa: Kasım 2011. E.T.: 25 Ağustos 2019. url: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802f2464.

Avrupa Parlamentosu ve Konseyi. “European Directive on Data Retention.” E.T.: 3 Ekim 2018. url: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32006L0024&from=EN.

Avrupa Parlamentosu ve Konseyi. “European Directive on Protection of Personal Data and Privacy-Directive 95/46/E.C.” E.T.: 3 Ekim 2018. url: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:31995L0046&from=en.

Avrupa Parlamentosu ve Konseyi. “Privacy and Electronic Communications Directive 2002-Directive 2002/58/EC.” E.T.: 3 Ekim 2018. url: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32002L0058&from=EN.

Avrupa Parlamentosu ve Konseyi. “The Directive on Security of Network and Information Systems (NIS Directive).” E.T.: 3 Ekim 2018. url: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016L1148&from=EN.

Avrupa Parlamentosu. “EU Cyber Defense Policy Framework.” E.T.: 3 Ekim 2018. url: http://www.europarl.europa.eu/meetdocs/2014_2019/documents/sede/dv/sede160315eucyberdefencepolicyframework_/sede160315eucyberdefencepolicyframework_en.pdf.

Baldwin, David A. *Power and International Relations: A Conceptual Approach.* Amerika: Princeton University Press, 2016. E.T.: 14 Temmuz 2018. ISBN: 978-1-4008-8100-0.

Baran, Paul. "On Distributed Communication Networks." Kaliforniya: The RAND Corporation, Eylül 1962. E.T.: 4 Ağustos 2019. url: https://www.rand.org/content/dam/rand/pubs/papers/2005/P2626.pdf.

Başaran, Alper. "Siber Savaş Tarihinden Bazı Olaylar." *Alper Başaran.* 25 Temmuz 2014. E.T.: 10 Temmuz 2018. url.: http://alperbasaran.com/siber-savas-tarihinden-bazi-olaylar/.

Başaran, Alper. *Siber Kıyamet.* İstanbul: Arion Yayınevi, Ekim 2017.

Başaran, Alper. *Siber Savaş Cephesinden Notlar.* İstanbul: Arion Yayınevi, Mayıs 2016.

Bayraktar, Gökhan. *Siber Savaş ve Ulusal Güvenlik Stratejisi.* İstanbul: Yeniyüzyıl Yayınları, 2015.

Bencsath, Boldizsar, Pek, Gabor, Buttyan, Levente, and Felegyhazi, Mark. "The Cousins of Stuxnet: Duqu, Flame and Gauss." *Future Internet* 4 (2012): 971-1003. E.T.: 13 Temmuz 2018. doi: 10.3390/fi4040971.

Benlisoy, Foti. "Anarşizm: Gönüllü Düzene Övgü" içinde *19. Yüzyıldan 20. Yüzyıla Modern Siyasal İdeolojiler*, derleyen: H. Birsen Örs, 351-411. İstanbul: İstanbul Bilgi Üniversitesi Yayınları, Ekim 2010.

Bıçakçı, Salih. *21. Yüzyılda Siber Güvenlik.* İstanbul: İstanbul Bilgi Üniversitesi Yayınları, Ağustos 2013.

Bilgi Teknolojileri ve İletişim Kurumu, *Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı* (Türkiye: 2013), E.T.: 20 Ağustos 2019, url: https://www.btk.gov.tr/uploads/pages/2-1-strateji-eylem-plani-2013-2014-5a3412cf8f45a.pdf.

Bilgi Teknolojileri ve İletişim Kurumu. "Siber Güvenlik Stratejisi ve Eylem Planı." E.T.: 20 Ağustos 2019. url: https://www.btk.gov.tr/siber-guvenlik-stratejisi-ve-eylem-plani.

Bilgi Teknolojileri ve İletişim Kurumu. *2019-2023 Stratejik Planı.* Türkiye: 2019. E.T.: 20 Ağustos 2019. url: https://www.btk.gov.tr/uploads/pages/yayinlar-stratejik-planlar/btk-2019-2023-stratejik-plani.pdf.

Bilgi Teknolojileri ve İletişim Kurumu. *Siber Güvenliğin Sağlanması: Türkiye'deki Mevcut Durum ve Alınması Gereken Tedbirler.* Türkiye: 2009. E.T.: 20 Ağustos 2019. url: https://www.btk.gov.tr/uploads/undefined/sg.pdf.

Birdişli, Fikret. *Teori ve Pratikte Uluslararası Güvenlik.* Ankara: Seçkin Yayınları, Ocak 2014.

Birleşik Krallık Hükümet Sitesi. "National Cyber Security Strategy 2016 to 2021." E.T.: 1 Ekim 2018. url: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf.

Birleşik Krallık Hükümet Sitesi. "National Security Capability Review." E.T.: 1 Ekim 2018, url: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/705347/6.4391_CO_National-Security-Review_web.pdf.

Birleşik Krallık Hükümet Sitesi. "Protecting and Promoting the UK in a Digital World." E.T.: 1 Ekim 2018. url: https://www.gov.uk/government/news/protecting-and-promoting-the-uk-in-a-digital-world--3.

Birleşik Krallık Hükümeti Sitesi. "National Security Strategy and Strategic Defence and Security Review 2015 A Secure and Prosperous United Kingdom." E.T.: 1 Ekim 2018. url: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/555607/2015_Strategic_Defence_and_Security_Review.pdf.

Birleşik Krallık Ulusal Arşiv. "Computer Misuse Act 1990." E.T.: 1 Ekim 2018. url: https://www.legislation.gov.uk/ukpga/1990/18/contents.

Birleşmiş Milletler. "Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders." E.T.: 10 Ekim 2018. url: https://digitallibrary.un.org/record/432663/files/A_CONF.187_15-EN.pdf.

Bologna, Sandro., Fasani, Alessandro., ve Martellini, Maurizio. "Cyber Security and Resilience of Industrial Control Systems and Critical Infrastructures." İçinde *Cyber Security: Deterrence and IT Protection for Critical Infrastructures,* editör: Maurizio Martellini, 56-72. Amerika: Springer, 2013.

Bulut, Remzi. "SSCB'nin Dağılması ve Rusya Federasyonu'nun Serbest Piyasaya Geçişi." *Mehmet Akif Ersoy Üniversitesi İktisadi ve İdari Bilimler*

Fakültesi Dergisi Cilt: 1-Sayı: 2 (2014): 7-19. E.T.: 30 Eylül 2018. url: http://dergipark.gov.tr/download/article-file/231924.

CCDCOE. "About Us." E.T.: 22 Ağustos 2019. url: https://ccdcoe.org/about-us/.

CCDCOE. *Conceptual Views Regarding the Activities of the Armed Forces of the Russian Federation in the Information Space.* Rusya: 2011. E.T.: 30 Eylül 2018. url: http://www.ccdcoe.org/strategies/Russian_Federation_unofficial_translation.pdf.

Center of Internet Security. *October: National Cybersecurity Awareness Mont.* E.T.: 15 Eylül 2018. url: https://www.cisecurity.org/blog/october-national-cybersecurity-awareness-month/.

CERN. "The Birth of the Web." E.T.: 4 Ağustos 2019. url: https://home.cern/science/computing/birth-web.

Chandrasekaran, Pravin. "Kautilya: Politics, Ethics and Statecraft." (2006). E.T.: 17 Temmuz 2018. url: https://www.researchgate.net/publication/24116687_Kautilya_Politics_Ethics_And_Statecraft.

Cheng, Dean. *Cyber Dragon.* Amerika: PRAEGER, 2017.

Chip. "Tarihin En Etkili 50 Bilgisayar Virüsü." E.T.: 12 Temmuz 2018. url: https://www.chip.com.tr/galeri/tarihin-en-etkili-50-bilgisayar-virusu_2025_49.html.

Clarke, Richard A., ve Knake, Robert K. *Siber Savaş.* Çeviren: Murat Erduran. İstanbul: İKÜ Yayınevi, Nisan 2011.

Clausewitz, Carl von. *Savaş Üzerine.* Çev. Selma Koçak. İstanbul: Doruk Yayınları, 2015.

Clausewitz, Carl von. *Savaşın Esasları.* Çev.: Gökhan Aydın. İstanbul: Doruk Yayınları, Nisan 2017.

Clough, Jonathan. "A World Of Difference: The Budapest Convention on Cybercrime and The Challenges Of Harmonisation." *Monash Üniversitesi Hukuk Dergisi* 40-3 (2014): 698-736. E.T.: 16 Ekim 2018. url: https://www.monash.edu/__data/assets/pdf_file/0019/232525/clough.pdf.

Colleran, Jeanne. *Theatre and War.* New York: Palgrave Macmillan, 2012.

Copeland, Jack. “Introduction.” İçinde *Colossus: The Secrets of Bletchley Park’s Codebreaking Computers*, editör: Jack Copeland, 1-8. New York: Oxford University Press, 2006.

Cyber Policy Portal. E.T.: 23 Ağustos 2019. url: https://cyberpolicyportal.org/en/.

Çakmak Haydar., ve Altunok, Taner. *Suç, Terör ve Savaş Üçgeninde Siber Dünya.* Ankara: Barış Platin Yayınevi, Mayıs 2009.

Çelikpala, Mitat., Bıçakçı, Salih., ve Ergun, F. Doruk. “Türkiye’de Siber Güvenlik.” *Ekonomi ve Dış Politika Araştırma Derneği* (2016): 28-73. E.T.: 30 Eylül 2018. url: http://edam.org.tr/document/CyberNuclear/SiberKitapTR/edam_siber_guvenlik_b2.pdf.

Çıtak, Emre. *Güvenlik ve İstihbarat.* İstanbul: Yeniyüzyıl Yayınları, 2017.

Çiftçi, Hasan. *Her Yönüyle Siber Savaş.* Ankara: TÜBİTAK Popüler Bilim Kitapları, Temmuz 2017.

Darıcılı, Ali Burak. *Siber Uzay ve Siber Güvenlik.* Bursa: Dora Yayıncılık, Aralık 2017.

DARPA. “ARPA Is Born.” E.T.: 4 Ağustos 2019. url: https://www.darpa.mil/about-us/timeline/dod-establishes-arpa.

Davis, Patty., Wallace, Kelly., ve Weaver, Lisa Rose. “U.S. Spy Plane, Chinese Fighter Collide.” *CNN News*, 01.04.2001. E.T.: 16 Ağustos 2019. url: http://edition.cnn.com/2001/US/04/01/us.china.plane.02/index.html.

Dedeoğlu, Beril. *Uluslararası Güvenlik ve Strateji.* İstanbul: Yeniyüzyıl Yayınları, 2014.

Deibert, Ron., ve Rohozinski, Rafal. *Tracking GhostNet: Investigating a Cyber Espionage Network.* ABD: Munk Centre International Studies, 2009.

Denning, Dorothy E. “Cyberterrorism.” *Naval Postgarduated School* (2000): 1-9, E.T. 20 Temmuz 2018, url: https://calhoun.nps.edu/handle/10945/55351.

Der.: Rosen, Michael. ve Wolff, Jonathan. *Siyasal Düşünce.* Çev.: Sevda Çalışkan ve Hamit Çalışkan. Ankara: Dost Kitabevi Yayınları, Temmuz 2006.

Dunn Cavelty, Myriam. *Cyber Security and Threat Politics: US Efforts to Secure the Information Age.* Amerika: Routledge, 2008.

Ehala, Martin. “The Bronze Soldier: Identity Threat and Maintenance in Estonia.” *Journal of Baltic Studies* 40/1 (2009): 139-158. E.T.: 22 Temmuz 2018. Doi: 10.1080/01629770902722294.

Emeklier, Bilgehan. “Thomas Hobbes ve John Locke’un Güvenlik Anlayışının Karşılaştırmalı Analizi” *Güvenlik Stratejileri Dergisi.* Sayı: 13 (2011): 99-123. E.T.: 1 Haziran 2018. url: http://dergipark.ulakbim.gov.tr/guvenlikstrtj/article/view/5000098892,

Erbschloe, Michael. *Trojans, Worms, and Spyware.* ABD: Elsevier Butterworth–Heinemann Publisher, 2005.

Eren, Mehmet. *Avrupa Birliği’nin Siber Güvenlik Politikası.* İstanbul: Beta Yayınları, Mart 2017.

Ergil, Doğu. “Uluslararası Terörizm.” *Ankara Üniversitesi Siyasal Bilgiler Fakültesi Dergisi* 47-3 (1992): 139-143. E.T.: 21 Temmuz 2018. url.: http://dergiler.ankara.edu.tr/dergiler/42/457/5195.pdf.

Ergün, İsmail. *Siber Suçların Cezalandırılması ve Türkiye’de Durum.* Ankara: Adalet Yayınları, 2008.

Ersanel, Nedret. *Siber İstihbarat.* İstanbul: Hayy Kitap, Ekim 2005.

European Union. “Critical Infrastructure.” E.T.: 21 Ağustos 2019. url: https://ec.europa.eu/home-affairs/what-we-do/policies/crisis-and-terrorism/critical-infrastructure_en.

European Union. “The EU Cybersecurity Act.” E.T.: 21 Ağustos 2019. url: https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-act.

Federal Alman Hükümeti. “Der Digitalrat - Experten, Die Uns Antreiben.” E.T.: 18 Ağustos 2019. url: https://www.bundesregierung.de/breg-de/themen/digitalisierung/der-digitalrat-experten-die-uns-antreiben-1504866.

Federal Alman Hükümeti. “The Digital Strategy of the German Government.” E.T.: 18 Ağustos 2019. url: https://www.bundesregierung.de/breg-en/search/the-digital-strategy-of-the-german-government-1550216.

Federal Bureau of Investigation. “Mission & Priorities.” E.T.: 16 Ağustos 2019. url: https://www.fbi.gov/about/mission.

Federation of American Scientists. *Executive Order EO 13010 Critical Infrastructure Protection.* E.T.: 15 Eylül 2018. url: https://fas.org/irp/offdocs/eo13010.htm.

Federation of American Scientists. *Presidential Decision Directive/NSC-63*. E.T.: 15 Eylül 2018. url: https://fas.org/irp/offdocs/pdd/pdd-63.htm.

Federation of American Scientists. *Presidential Policy Directive/PPD-20*. Amerika: 2012. E.T.: 17 Eylül 2018. url: https://fas.org/irp/offdocs/ppd/ppd-20.pdf.

Federation of American Scientists. *Regulations on Safeguarding Computer Information Systems*. E.T.: 27 Eylül 2018. url: https://fas.org/irp/world/china/docs/computer_code.htm.

Ford, Ken. *Run the Gauntlet: The Channel Dash 1942*. ABD: Osprey Publishing, 2012.

Forouzan, Behrouz A. *TCP/IP Protocol Suite*. New York: The McGraw-Hill Companies, 2010.

Foucault, Michel. *Güvenlik, Toprak, Nüfus: 1977-1978*. Çeviren: Ferhat Taylan. İstanbul: İstanbul Bilgi Üniversitesi Yayınları, Aralık 2013.

Gallarotti, Giulio M. "Smart Power: Definitions, Importance, and Effectiveness." *Division II Faculty Publications* 163 (2014): 1-53. E.T.: 14 Temmuz 2018. url: http://wesscholar.wesleyan.edu/div2facpubs/163.

Geers, Kenneth. *Strategic Cyber Security*. Estonya: CCDCOE Yayınları, Haziran 2011. E.T.: 28 Haziran 2018. url: https://ccdcoe.org/publications/books/Strategic_Cyber_Security_K_Geers.PDF.

Ghernaouti, Solange. *Cyber Power: Crime, Conflict and Security in Cyberspace*. Switzerland: EPFL Press, 2013.

Gibson, William. *Neuromancer*. New York: ACE Book, 2004.

Giles, Keir. "Russia's National Security Strategy to 2020." *Zürih Federal Teknoloji Enstitüsü* (2009). E.T.: 17 Ağustos 2019. url: https://www.files.ethz.ch/isn/154909/RusNatSecStrategyto2020.pdf.

Goldstein, Joshua S. ve Pevehouse, Jon C.. *International Relations*. Amerika Birleşik Devletleri: Pearson Longman, 2012, 10. Basım.

Graham, James., Howard Richard., ve Olson, Ryan. *Cyber Security Essentials*. Amerika: CRC Press, 2011.

Greathouse, Craig B. "Cyber War and Strategic Thought: Do the Classic Theorists Still Matter?." İçinde *Cyberspace and International Relations: Theory, Prospects and Challenges*, editör: Jan-Frederik Kremer ve Benedikt Müller, 21-40. London: Springer Publishing, 2014.

Grimes, Roger A. *Hacking the Hacker: Learn from the Experts Who Take Down Hackers.* Kanada: Wiley Yayınları, 2017.

Güneştaş, Murat, Başıbüyük, Oğuzhan, ve Yılmaz, Kamil. "Siber Terörizm: Motivasyon ve Yöntem." içinde *Siber Suçlar: Tehditler, Farkındalık ve Mücadele*, derleyen: Fatih Tombul, Murat Güneştaş ve Oğuzhan Başıbüyük, 85-114. Ankara: Global Politika ve Strateji Yayınları, Ocak 2015.

Habertürk, *Trump'tan Yeni Siber Güvenlik Stratejisi,* E.T.: 21 Eylül 2018, url: https://www.haberturk.com/trump-tan-yeni-siber-guvenlik-stratejisi-2149858.

Halopeau, Bruno. "Terrorist Use of the Internet." İçinde *Cyber Crime and Cyber Terrorism Investigator's Handbook*, derleyen: Babak Akhga, Andrew Staniforth, ve Francesca Bosco, 122-132. Amerika: Elsevier Yayınları, 2014. ISBN: 978-0-12-800743-3.

Hekim, Hakan. "Oltalama (Phishing) Saldırıları." içinde *Siber Suçlar: Tehditler, Farkındalık ve Mücadele*, derleyen: Fatih Tombul, Murat Güneştaş ve Oğuzhan Başıbüyük, 57-84. Ankara: Global Politika ve Strateji Yayınları, Ocak 2015.

Heywood, Andrew. *Siyaset.* Editör: Buğra Alkan. Ankara: Adres Yayınları, Şubat 2011.

Himma, Kenneth Einar. *Internet Security: Hacking, Counterhacking, and Society.* America: Jones and Bartlett Yayınevi, 2007.

Homeland Security. "Critical Infrastructure Sectors." E.T.: 15 Ağustos 2019. url: https://www.dhs.gov/cisa/critical-infrastructure-sectors.

Homeland Security. "In Focus." E.T.: 16 Ağustos 2019. url: https://www.dhs.gov/focus.

Homeland Security. *2009 Cyberspace Policy Review.* E.T.: 15 Eylül 2018. url: https://www.dhs.gov/publication/2009-cyberspace-policy-review.

https://threatmap.checkpoint.com/ThreatPortal/livemap.html

https://wikileaks.org/-Leaks-.html

Hurwitz, Roger. "A New Normal? The Cultuvation Of Global Norms As Part Of A Cybersecurity Strategy." İçinde *Conflict and Cooperation in Cyberspace,* Editör: Panayotis A. Yannakogeorgos ve Adam B. Lowther, 233-264. Amerika: Taylor & Francis Group, 2014.

IBM. "IBM's ASCC Introduction." E.T.: 3 Ağustos 2019. url: https://www.ibm.com/ibm/history/exhibits/markI/markI_intro.html.

ICANN. “About ICANN.” E.T.: 23 Ekim 2018. url: https://www.icann.org/resources/pages/welcome-2012-02-25-en.

International Telecommunications Union. “Making an IMPACT on Cybersecurity.” E.T.: 23 Ağustos 2019. url: https://www.itu.int/net/itunews/issues/2009/08/22.aspx.

Janelle, Donald G., ve Hodge, David C. “Information, Place, Cyberspace, and Accessibility,” içinde *Information, Place, and Cyberspace: Issues in Accessibility*, editör: Donald G. Janelle ve David C. Hodge, 3-12. ABD: Springer, 2000.

Jayawardane, Sash., Larik, Joris., ve Jackson, Erin. “Cyber Governance: Challenges, Solutions, and Lesson for Effective Global Governance.” *Policy Brief* 17 (Kasım 2015): 3-18. E.T. : 6 Temmuz 2018. url: http://www.thehagueinstituteforglobaljustice.org/wp-content/uploads/2015/12/PB17-Cyber-Governance.pdf.

Jeffery, Renée. *Evil and International Relations: Human Suffering in an Age of Terror*. New York: Palgrave Macmillan, 2008.

Johnson, Thomas A. “Cyber Intelligence, Cyber Conflicts, and Cyber Warfare.” İçinde *Cyber Security,* editör: Thomas A. Johnson, 155-198. ABD: CRC Press, 2015.

Kabine Ofisi. “About Us.” E.T.: 19 Ağustos 2019. url: https://www.gov.uk/government/organisations/cabinet-office/about#responsibilities.

Kabine Ofisi. *Cyber Security Strategy of the United Kingdom.* İngiltere: Haziran 2009. E.T.: 1 Ekim 2018. url: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/228841/7642.pdf.

Kabine Ofisi. *Interim Cyber Security Science And Technology Strategy.* İngiltere: Kasım 2017. E.T.: 1 Ekim 2018. url: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/663181/Embargoed_National_Cyber_Science_and_Technology_Strategy_FINALpdf.pdf.

Kabine Ofisi. *The National Security Strategy of the United Kingdom.* İngiltere: Mart 2008. E.T.: 19 Ağustos 2019. url:

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/228539/7291.pdf.

Kabine Ofisi. *The National Security Strategy of the United Kingdom: Update 2009 Security for the Next Generation.* İngiltere: Haziran 2009. E.T.: 1 Ekim 2018. url: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/229001/7590.pdf.

Kabine Ofisi. *The UK Cyber Security Strategy: Protecting and Promoting the UK in a Digital World.* İngiltere: 2011. E.T.: 1 Ekim 2018. url: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf.

Kaya, Sezgin "Uluslararası İlişkilerde Konstrüktivist Yaklaşımlar." *Ankara Üniversitesi Siyasal Bilgiler Fakültesi Dergisi.* Cilt. 63 Sayı: 3 (2008): 83-111. E.T.: 23 Haziran 2018. url: http://www.politics.ankara.edu.tr/dergi/pdf/63/3/6-Kaya-Sezgin.pdf

Keleştemur, Atalay. *Siber İstihbarat.* İstanbul: Level Kitap, Ağustos 2015.

King, Laura A.. *The Science of Psychology: An Appreciative View.* New York: McGraw-Hill, 2008.

Kizza, Joseph Migga. *Computer Network Security and Cyber Ethics*. ABD: McFarland & Company, Inc., Publishers, 2014.

Klipper, Sebastian. *Cyber Security.* Kiel: Springer Vieweg, 2015. E.T.: 30 Haziran 2018. DOI: 10.1007/978-3-658-11577-7.

Köylü, Hüseyin Cem. "Dünden Bugüne Internet Explorer." *Chip,* 5 Nisan 2012. E.T.: 6 Temmuz 2018. url: https://www.chip.com.tr/haber/dunden-bugune-internet-explorer_32928.html.

Kraliyet Parlamentosu. "Strategic Defence and Security Review." E.T.: 1 Ekim 2018. url: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/62482/strategic-defence-security-review.pdf.

Kremling, Janine., ve Sharp Parker, Amanda M. *Cyberspace, Cybersecurity, and Cybercrime.* ABD: SAGE Publications, 2017.

KURGAN. *Siber Mücadeleye Giriş.* İstanbul: Kutlu Yayınevi, Ocak 2018.

Küçük, Mustafa. "Uluslararası İlişkilerde Sosyal İnşacılık," içinde *Uluslararası İlişkiler Teorileri*, derleyen: Ramazan Gözen, 325-377. İstanbul: İletişim Yayınları, 2014.

Leitner, Maria., Pahi, Timea., ve Skopik, Florian. "Situational Awareness for Strategic Decision Making on a National Level." İçinde *Collaborative Cyber Threat Intelligence,* editör: Florian Skopik, 225-275. Amerika: CRC Press, 2018.

Lerner, K. Lee., ve Wilmoth Lerner, Brenda. *Encyclopedia of Espionage, Intelligence, and Security.* ABD: Thomson Gale, 2004.

Levy, Steven. *Hackers: Heroes of the Computer Revolution.* America: O'Rielly, 2010).

Liu, Alex X. *Firewall Design and Analysis.* ABD: World Scientific Publishing, 2011.

Malik, Ashfaq Ahmad., Mahboob, Athar., Khan, Adil., ve Zubairi, Junaid. "Application of Cyber Security in Emerging C4ISR Systems and Related Technologies." İçinde *Cyber Security Standards, Practices and Industrial Applications: Systems and Methodologies*, editör: Junaid Ahmed Zubairi ve Athar Mahboob, 223-258. Amerika: Information Science Reference, 2012.

Mazanec, Brian M., ve Thayer Bradley A. *Deterring Cyber Warfare: Bolstering Strategic Stability in Cyberspace.* Basingstoke: Palgrave Macmillan, 2015. DOI: 10.1057/9781137476180.0005.

Meer, Sico van der. "Defence, Deterrence, and Diplomacy: Foreign Policy Instruments to Increase Future Cybersecurity." İçinde *Securing Cyberspace: International and Asian Perspectives,* editör: Cherian Samuel ve Munish Sharma, 95-105. Hindistan: Pentagon Yayınları, 2016.

Mevzuat Bilgi Sistemi. "5237 Sayılı Türk Ceza Kanunu." E.T.: 20 Ağustos 2019. url: http://www.mevzuat.gov.tr/Metin.Aspx?MevzuatKod=1.5.5237&MevzuatIliski=0&sourceXmlSearch=.

Mevzuat Bilgi Sistemi. "Elektronik Haberleşme Kanunu." E.T.: 20 Ağustos 2019. url: http://www.mevzuat.gov.tr/MevzuatMetin/1.5.5809.pdf.

Mevzuat Bilgi Sistemi. "Elektronik İmza Kanunu." E.T.: 20 Ağustos 2019. url: http://www.mevzuat.gov.tr/MevzuatMetin/1.5.5070.pdf.

Mevzuat Bilgi Sistemi. "İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi

Hakkında Kanun." E.T.: 20 Ağustos 2019. url: https://www.mevzuat.gov.tr/MevzuatMetin/1.5.5651.pdf.

Mitnick Security Consulting. "About Kevin Mitnick: CEO, Team Leader, and Chief White Hat Hacker." E.T.: 9 Temmuz 2018. url: https://www.mitnicksecurity.com/about/kevin-mitnick-worlds-most-famous-hacker-biography.

Ng, Chee Keong., Pan, Lei., ve Xiang, Yang. *Honeypot Frameworks and their Applications: A New Framework.* Avustralya: Springer, 2018.

North Atlantic Treaty Organization. "Brussels Summit Declaration." E.T.: 6 Ekim 2018. url: https://www.nato.int/cps/ic/natohq/official_texts_156624.htm.

North Atlantic Treaty Organization. "Bucharest Summit Declaration." E.T.: 4 Ekim 2018. url: https://www.nato.int/cps/en/natolive/official_texts_8443.htm?mode=pressrelease.

North Atlantic Treaty Organization. "Chicago Summit Declaration." E.T.: 5 Ekim 2018. url.: https://www.nato.int/cps/ra/natohq/official_texts_87593.htm?selectedLocale=en.

North Atlantic Treaty Organization. "Lisbon Summit Declaration." E.T.: 5 Ekim 2018. url.: https://www.nato.int/cps/en/natolive/official_texts_68828.htm.

North Atlantic Treaty Organization. "Prague Summit Declaration." E.T.: 4 Ekim 2018. url: https://www.nato.int/cps/en/natohq/official_texts_19552.htm.

North Atlantic Treaty Organization. "Wales Summit Declaration." E.T.: 5 Ekim 2018. url.: https://www.nato.int/cps/ic/natohq/official_texts_112964.htm.

North Atlantic Treaty Organization. "Warsaw Summit Communiqué." E.T.: 5 Ekim 2018. url.: https://www.nato.int/cps/su/natohq/official_texts_133169.htm.

Nye, Joseph S. Jr. "Get Smart: Combining Hard and Soft Power." *Foreign Affairs* (2009). E.T.: 5 Ağustos 2019. url: https://www.foreignaffairs.com/articles/2009-07-01/get-smart.

Nye, Joseph S. Jr., ve Welch, David A. *Küresel Çatışmayı ve İşbirliğini Anlamak*. Çeviren: Renan Akman. İstanbul: Türkiye İş Bankası Kültür Yayınları, Ekim 2013.

Omand, David. "Understanding Digital Intelligence: A British View." İçinde *National Security and Counterintelligence in the Era of Cyber Espionage,* editör: Eugenie de Silva, 97-121. ABD: Information Science Reference, 2016.

Önal, Huzeyfe. " Siber Savaşlarda En Kritik Bileşen Siber İstihbarat." *Uluslararası Siber Güvenlik Federasyonu* 2 (2017): 44-47.

Özeren, Süleyman. "Cyberterrorism and International Cooperation: General Overview of the Available Mechanisms to Facilitate an Overwhelming Task." İçinde *Responses to Cyber Terrorism,* editör Centre of Excellence Defence Against Terrorism, 70-88. Ankara: IOS Yayınları, 2008.

Öztürk, Zeynel A. "Şifreleme Nedir, Nasıl Çalışır?" *Chip,* 17 Mart 2015. E.T.: 17 Haziran 2019. url: https://www.chip.com.tr/haber/sifreleme-nedir-nasil-calisir_54659.html.

Parziale, Lydia., Britt, David T., Davis, Chuck., Forrester, Jason., Liu, Wei., Matthews, Carolyn., and Rosselot, Nicolas. *TCP/IP Tutorial and Technical Overview.* Amerika Birleşik Devletleri: IBM/Redbooks, Aralık 2006. E.T.: 3 Temmuz 2018. url: https://www.redbooks.ibm.com/pubs/pdfs/redbooks/gg243376.pdf.

Perlroth, Nicole. "Researchers Find Clues in Malware." *The New York Times*. 30 Mayıs 2012. E.T.: 13 Temmuz 2018. url: https://www.nytimes.com/2012/05/31/technology/researchers-link-flame-virus-to-stuxnet-and-duqu.html.

Ponniah, Kevin, ve Marinkovic, Lazara. "The Night the US Bombed a Chinese Embassy." *BBC News*, 07.05.2019. E.T.: 16 Ağustos 2019. url: https://www.bbc.com/news/world-europe-48134881.

Popjanevski, Johanna. "From Sukhumi to Tskhinvali: The Path to War in Georgia." İçinde *The Guns of August 2008,* editör: Svante E. Cornell ve S. Frederick Starr, 143-163. New York: M.E. Sharpe, 2009.

President of Russia. "G8 Summit." E.T.: 17 Ağustos 2019. url: http://en.kremlin.ru/events/president/news/18358.

Raud, Mikk. "China and Cyber: Attitudes, Strategies, Organisation." *NATO CCDCOE* (2016): 6-27. E.T.: 29 Eylül 2018. url: https://ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_CHINA_092016_FINAL.pdf.

Richards, Julian. *Cyber War.* ABD: Palgrave MacMillan, 2014.

Russell, John. *Chechnya – Russia's 'War on Terror'.* New York: Routledge, 2007.

Ryan, Johnny. *A History of the Internet and The Digital Future.* Londra: Reaktion Books, 2010.

Schmitt, Michael N. "Tallinn Manual on The International Law Applicable to Cyber Warfare." *NATO.* Amerika: Cambridge University Press, 2013. E.T.: 22 Temmuz 2018. url: http://csef.ru/media/articles/3990/3990.pdf.

Schneider, Grant. "President Trump Unveils America's First Cybersecurity Strategy in 15 Years." *The White House*. (Eylül 2018). E.T.: 21 Eylül 2018. url: https://www.whitehouse.gov/articles/president-trump-unveils-americas-first-cybersecurity-strategy-15-years/.

Shaheen, Salma. "Offense–Defense Balance in Cyber Warfare." İçinde *Cyberspace and International Relations: Theory, Prospects and Challenges,* editör: Jan-Frederik Kremer ve Benedikt Müller, 77-94. London: Springer Publishing, 2014.

Singer, P. W. "Saklanacak Yer Yok." *Popular Science* 35 (2015): 71-75.

Singer, P. W. "Sıfırla Birlerin Savaşı." *Popular Science* 29 (2014): 36-41.

Singer, P. W., ve Friedman, Allan. *Siber Güvenlik ve Siber Savaş.* Çeviren: Ali Atav. Ankara: Buzdağı Yayınevi, Mart 2015.

Skopik, Florian., Settanni, Giuseppe., ve Fiedler, Roman. "The Importance of Information Sharing and Its Numerous Dimensions to Circumvent Incidents and Mitigate Cyber Threats." İçinde *Collaborative Cyber Threat Intelligence,* editör: Florian Skopik, 129-186. Amerika: CRC Press, 2018.

Smith, Rupert. *Utility of Force.* New York: Vintage, 2008.

Springer, Paul J. *Cyber Warfare.* Amerika: ABC-CLIO, 2015.

Steed, Danny. "The Strategic Implications Of Cyber Warfare." İçinde *Cyber Warfare: A Multidiciplinary Analysis,* editör: James A. Green, 73-95. New York: Routledge, 2015.

Stiennon, Richard. "A Short History of Cyber Warfare." İçinde *Cyber Warfare,* editör: James A. Green, 7-32. Amerika: Routledge, 2015.

Stout, David. "Youth Sentenced in Government Hacking Case." *The New York Times.* 23 Eylül 2000. E.T.: 9 Temmuz 2018. url.: https://www.nytimes.com/2000/09/23/us/youth-sentenced-in-government-hacking-case.html.

Strayer, Timothy W., Lapsely, David., Walsh, Robert ve Livadas, Carl. "Botnet Detection Based on Network Behavior." İçinde *Botnet Detection:*

Countering the Largest Security Threat, editör: Wenke Lee, Cliff Wang ve David Dagon, 1-24. New York: Springer, 2008.

Şen, Osman. "Klasik Realizmin Güvenliğe Bakışı ve Kökenleri," içinde *Uluslararası İlişkilerde Güvenlik: Teorik Değerlendirmeler*, derleyen: Emre Çıtak ve Osman Şen, 23-32. İstanbul: Uluslararası İlişkiler Kütüphanesi, Eylül 2014.

T.C. Ulaştırma, Denizcilik ve Haberleşme Bakanlığı. "2016-2019 Ulusal Siber Güvenlik Stratejisi." E.T.: 20 Haziran 2018. url: http://www.udhb.gov.tr/doc/siberg/2016-2019guvenlik.pdf.

T.C. Ulaştırma, Denizcilik ve Haberleşme Bakanlığı. "Kurumsal SOME Kurulum ve Yönetim Rehberi." E.T.: 30 Eylül 2018. url: http://www.udhb.gov.tr/doc/siberg/Kurumsal_SOME_Reh_V1.pdf.

Terkeşli, Ramazan. "Yetkisiz Erişim ve Web Uygulama Güvenliği." İçinde *Siber Suçlar: Tehditler, Farkındalık ve Mücadele*, derleyen: Fatih Tombul, Murat Güneştaş ve Oğuzhan Başıbüyük, 115-138. Ankara: Global Politika ve Strateji Yayınları, Ocak 2015.

The Ministry of Foreign Affairs of the Russian Federation. *Doctrine of Information Security of the Russian Federation.* Rusya: Aralık 2016. E.T.: 30 Eylül 2018. url: http://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/2563163.

The Ministry of Foreign Affairs of the Russian Federation. *National Security Concept of the Russian Federation.* Rusya: Ocak 2000. E.T.: 30 Eylül 2018. url: http://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/589768.

The OWASP Foundation. "OWASP Top 10 – 2017: The Ten Most Critical Web Application Security Risks." E.T.: 18 Ekim 2018. url: https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf.

The Russian Government. "Federal Security Service." E.T.: 17 Ağustos 2019. url: http://government.ru/en/department/113/.

The White House. *International Strategy for Cyberspace.* Amerika: Mayıs 2011. E.T.: 17 Eylül 2018. url: https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

The White House. *National Cyber Strategy of the United States of America.* Amerika: Eylül 2018. E.T.: 21 Eylül 2018. url:

https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

The White House. *The National Strategy To Secure Cyberspace.* Washington: Şubat 2003. E.T.: 15 Eylül 2018. url: https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf.

TIKK, Eneken., ve OORN, Reet. "Legal and Policy Evaluation: International Coordination of Prosecution and Prevention of Cyber Terrorism." içinde *Responses to Cyber Terrorism,* editör Centre of Excellence Defence Against Terrorism, 89-103. Ankara: IOS Yayınları, 2008.

Tombul, Fatih. "Kamu Yönetiminde Siber Suçlara Karşı Kullanıcılarda Farkındalık Oluşturulmasının ve Kurumsal Bilişim Güvenlik Politikalarının Oluşturulmasının Önemi." İçinde *Siber Suçlar: Tehditler, Farkındalık ve Mücadele,* derleyen: Fatih Tombul, Murat Güneştaş ve Oğuzhan Başıbüyük, 141-168. Ankara: Global Politika ve Strateji Yayınları, Ocak 2015.

TÜBİTAK. *Elinizin Altındaki Gerçekler: Buluşlar ve Teknoloji, Savunma ve Güvenlik.* Editör: Tom Jackon. Çeviri: Fahri Öz. Ankara: TÜBİTAK Popüler Bilim Kitapları, Ekim 2014.

Türkiye Bilişim Derneği. "Siber Güvenlik ve Kritik Altyapı Güvenliği Çalışma Grubu Nihai Rapor Sürüm 1.0." E.T.: 30 Eylül 2018. url: http://www.kamu-bib.org.tr/kamubib-17/wp-content/uploads/2015/10/Kamu-BIB-CG1-Siber-Guvenlik-ve-Kritik-Altyapilar.pdf.

Türkiye Büyük Millet Meclisi. *Sanal Ortamda İşlenen Suçlar Sözleşmesinin Onaylanmasının Uygun Bulunduğuna Dair Kanun Tasarısı ve Dışişleri Komisyonu Raporu (1/676).* Ankara: 2012. E.T.: 22 Ekim 2018. url: https://www.tbmm.gov.tr/sirasayi/donem24/yil01/ss380.pdf.

Türkiye Siber Güvenlik Kümelenmesi. "Hakkında." E.T.: 20 Ağustos 2019. url: https://siberkume.org.tr/hakkinda/.

Tzu, Sun. *Savaş Sanatı.* Çeviren: Pulat Otkan ve Giray Fidan. İstanbul: Türkiye İş Bankası Kültür Yayınları, Mart 2017.

Ulusal Güvenlik Sistemi. *Chaff - Radar Countermeasures.* E.T.: 17 Haziran 2019. url: https://www.globalsecurity.org/military/systems/aircraft/systems/chaff.htm.

Ulusal Siber Güvenlik Merkezi. "About the NCSC." E.T.: 1 Ekim 2018. url: https://www.ncsc.gov.uk/information/about-ncsc.

United Nations Digital Library. *Seventh United Nations Congress on the Prevention of Crime and the Treatment of Offenders.* Milan: 1985. E.T.: 23 Ağustos 2019. url: https://digitallibrary.un.org/record/114498?ln=en.

United Nations General Assembly. *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security.* United Nations General Assembly. 2015. E.T.: 23 Ağustos 2019. url: https://undocs.org/A/70/174.

United Nations Office for Disarmament Affairs. "UNIDIR Launches Cyber Policy Portal and Announces Date, 6 June 2019, for its Cyber Stability Conference 2019 in New York." E.T.: 23 Ağustos 2019, url: https://www.un.org/disarmament/update/unidir-launches-cyber-policy-portal-and-announces-date-6-june-2019-for-its-cyber-stability-conference-2019-in-new-york/.

United Nations System. "Action on Cybercrime and Cyber Security." E.T.: 23 Ağustos 2019. url: https://www.unsystem.org/content/action-cybercrime-and-cyber-security.

Ünal, Ahmet Naci. *Siber Güvenlik ve Elektronik Bileşenleri.* Ankara: Nobel Yayınları, 2015.

Ünal, Ahmet. "Dağıtık Servis Dışı Bırakma (DDOS) Saldırıları: Güncel Yöntemler ve Mücadele." içinde *Siber Suçlar: Tehditler, Farkındalık ve Mücadele*, derleyen: Fatih Tombul, Murat Güneştaş ve Oğuzhan Başıbüyük, 11-36. Ankara: Global Politika ve Strateji Yayınları, Ocak 2015.

Ünal, Mehmet., ve Gözübenli, Murat. "İnternet ve Kolluk." içinde *Siber Suçlar: Tehditler, Farkındalık ve Mücadele,* editör: Fatih Tombul, Murat Güneştaş ve Oğuzhan Başıbüyük, 223-238. Ankara: Global Politika ve Strateji Yayınları, Ocak 2015.

Ventre, Daniel. "Riots in Xinjiang and Chinese Information Warfare." İçinde *Cyberwar and Information Warfare,* editör: Daniel Ventre, 285-366. Amerika: Wiley-ISTE, 2011.

Virkar, Shefali. "The Mirror Has Two Faces: Terrorist Use of the Internet and the Challenges of Governing Cyberspace." İçinde *National Security and Counterintelligence in the Era of Cyber Espionage,* editör: Eugenie de Silva, 1-27.ABD: Information Science Reference, 2016.

Vogelgesang, Waldemar, Winter, Rainer, and Wetzstein, Thomas A. *Auf digitalen Pfaden Die Kulturen von Hackern, Programmierern, Crackern und Spielern.* Leverkusen: Westdeutscher Verlag, 1991. E.T.: 7 Temmuz 2018. ISBN 978-3-322-92485-8.

Waks, Leonard J. *Education 2.0: The LearningWeb Revolution and the Transformation of the School.* ABD: Paradigm Publishers, 2013.

Warkentin, Merrill., Schmidt, Mark B., ve Bekkering, Ernst. "Steganography." İçinde *Cyber Warfare and Cyber Terrorism,* editör: Lech J. Janczewski ve Andrew M. Colarik, 50-56. Amerika: Information Science Reference, 2008. ISBN: 978-1-59140-992-2. E.T.: 28 Temmuz 2018.

Weiner, Norbert. *Cibernética E Sociedade* Brasil: Culturix, 1968.

Winkler, Ira. *Spies Among Us.* Kanada: Wiley Yayıncılık, 2005.

Winston, Brian. *Media, Technology and Society: A History From the Telegraph to the Internet.* New York: Routledge, 1998.

World Intellectual Property Organization. "The Criminal Code of The Russian Federation." E.T.: 18 Ağustos 2019. url: https://www.wipo.int/edocs/lexdocs/laws/en/ru/ru006en.pdf.

Yalçın, Hasan Basri. *Ulusal Güvenlik Stratejisi.* İstanbul: SETA, Kasım 2017.

Yalvaç, Faruk. "Savaş ve Barış." İçinde *Devlet ve Ötesi,* derleyen: Atilla Eralp, 251-285. İstanbul: İletişim Yayınları, 2014.

Yannakopoulos, John. *HyperText Transfer Protocol: A Short Course.* Yunanistan, Ağustos 2003. E.T.: 3 Temmuz 2018. url: http://condor.depaul.edu/dmumaugh/readings/handouts/SE435/HTTP/http.pdf.

Yeşilyurt, Hamdi. "Uluslararası Siber Güvenlik Perspektifinde Siber Güvenlik." içinde *Siber Suçlar: Tehditler, Farkındalık ve Mücadele*, derleyen: Fatih Tombul, Murat Güneştaş ve Oğuzhan Başıbüyük, 169-193. Ankara: Global Politika ve Strateji Yayınları, Ocak 2015.

Yılmaz, Kamil., Güneştaş, Murat., ve Başıbüyük, Oğuzhan. "Siber Terörizm: Motivasyon ve Yöntem." İçinde *Siber Suçlar: Tehditler, Farkındalık ve Mücadele*, derleyen: Fatih Tombul, Murat Güneştaş ve Oğuzhan Başıbüyük, 85-114. Ankara: Global Politika ve Strateji Yayınları, Ocak 2015.

Yılmaz, Sait, ve Salcan, Olay, *Siber Uzay'da Güvenlik ve Türkiye.* İstanbul: Milenyum Yayınları, Şubat 2008.

Yiğittepe, Levent. *Avrupa Birliği'nde Güvenlik Politikaları ve Arayışları.* İstanbul: Cinius Yayınları, Şubat 2017.

Yiğittepe, Levent. *NATO Güvenlik Politikaları ve Terörle Mücadele Stratejileri.* İstanbul: Cinius Yayınları, Şubat 2017.

ÖZGEÇMİŞ

KİŞİSEL BİLGİLER

Soyisim, İsim : Yasemin Güryuva

Uyruğu : T.C.

Doğum Tarihi ve Yeri : 05/11/1991 ANKARA

Medeni Hali : Bekâr

Telefon Numarası : 0536 277 87 35

E-posta : yaseminguryuva@gmail.com

EĞİTİM

Derece	Kurum	Mezuniyet Yılı
Ön Lisans	Anadolu Üniversitesi	2017
Lisans	Başkent Üniversitesi	2014
Lise	Çankaya 50. Yıl Lisesi	2009

YABANCI DİL

İyi Seviyede İngilizce

Başlangıç Seviyesi Almanca

DİĞER BİLGİLER

Sertifika:

Beden Dili Ve Hitabet, Atatürk Ve Liderlik, İş Hayatında Liderlik Konulu Seminerler (6-14 Kasım 2010).

Başkent Üniversitesi Stratejik Araştırmalar Merkezi Ve Bahçeşehir Üniversitesi Stratejik Araştırmalar Merkezi Algılama Yönetimi Sertifika Programı (13-20-27 Nisan 2013)

TBMM Yasama Bilgilendirme Eğitimine Katılım Sertifikası (15.07.2013-19.07.2013)

T.C. İçişleri Bakanlığı Avrupa Birliği Ve Dış İlişkiler Dairesi Başkanlığı Staj Belgesi (9-20 Eylül 2013)

Başkent Üniversitesi Kariyer Programına Destek Sertifikası (Rektörlük Tarafından Verilmiştir) (2014)

Sosyal Sorumluluk Projelerine Destek Sertifikası (Dekanlık Tarafından Verilmiştir)

ORSAM Ortadoğu Yaz Okulu Seminer Programı Katılım Sertifikası (25-29 Temmuz 2016)

3. Ulusal Çevre Kongresi Katılım Sertifikası (24-28 Eylül 2016)

İlgi Alanları Resim, müzik, kitap

Sosyal Aktiviteler

- Başkent Üniversitesi BENVOG öğrenci girişiminde yönetim kurulunda 2012-2013 yılları arasında pek çok sosyal sorumluluk projesinde bulundum.
- Başkent Üniversitesi 2012-2014 yılları arasında SİBU Topluluğunda yönetim kurulunda yer almış bulunup aynı zamanda topluluğun dergisinde de görev almış bulunmaktayım.
- Başkent Üniversitesi 2013-2014 öğrenim yılı süresinde Öğrenci Konseyinde alt komisyonda görev yapmış bulunmaktayım.

Her üçünde de hem okulumuz için hem de görev aldığımız yerlerde pek çok önemli işler başarmış olup pek çok projede yer almış bulunmaktayım.

STAJ BİLGİLERİ

Temmuz 2013 Türkiye Büyük Millet Meclisi

Eylül 2013 Türkiye Cumhuriyeti İçişleri Bakanlığı Avrupa Birliği ve Dış İlişkiler Dairesi Başkanlığı