T.C.
HARP AKADEMİLERİ
STRATEJİK ARAŞTIRMALAR ENSTİTÜSÜ

21. YÜZYILDA ULUSAL GÜVENLİĞİN SAĞLANMASINDA SİBER İSTİHBARATIN ROLÜ

ULUSLARARASI İLİŞKİLER ANA BİLİM DALI
YÜKSEK LİSANS TEZİ

Hazırlayan
Cuma ÖZÇOBAN

Tez Danışmanı
Yrd. Doç. Dr. Şamil ÜNSAL

İSTANBUL – 2014

(BU SAYFA BOŞ BIRAKILMIŞTIR)

TEZ TANITIM FORMU

YAZAR ADI SOYADI	**:**	Cuma ÖZÇOBAN
TEZİN DİLİ	**:**	Türkçe
TEZİN ADI	**:**	21. Yüzyılda Ulusal Güvenliğin Sağlanmasında Siber İstihbaratın Rolü
ENSTİTÜ	**:**	Stratejik Araştırmalar Enstitüsü
ANA BİLİM DALI	**:**	Uluslararası İlişkiler
TEZİN TÜRÜ	**:**	Yüksek Lisans
TEZİN TARİHİ	**:**	29.05.2014
SAYFA SAYISI	**:**	109
TEZ DANIŞMANLARI	**:**	Yrd. Doç. Dr. Şamil ÜNSAL
DİZİN TERİMLERİ	**:**	Siber İstihbarat, Ulusal Güvenlik, Siber, Güvenlik.
TÜRKÇE ÖZET	**:**	Bu çalışmadaki amaç, 21. yüzyılda küreselleşen ve farklılaşan dünyada, yeni güvenlik ortamının beraberinde getirdiği risk ve tehdit türleri içerisinde bulunan ve ulusal güvenliğin korunması açısından önem taşıyan siber istihbaratın, devletlerin bekasının korumasında ne derece önemli olduğunu ortaya koymaya çalışmaktır.
DAĞITIM LİSTESİ	**:**	1. Stratejik Araştırmalar Enstitüsüne 2. YÖK Ulusal Tez Merkezine

Bu tezin içerdiği hususlar bireysel görüşlerimi yansıtır, Türk Silahlı Kuvvetlerinin görüşlerini yansıtmaz.

Cuma ÖZÇOBAN

T.C.
HARP AKADEMİLERİ
STRATEJİK ARAŞTIRMALAR ENSTİTÜSÜ

21. YÜZYILDA ULUSAL GÜVENLİĞİN SAĞLANMASINDA SİBER İSTİHBARATIN ROLÜ

ULUSLARARASI İLİŞKİLER ANA BİLİM DALI
YÜKSEK LİSANS TEZİ

Hazırlayan
Cuma ÖZÇOBAN

Tez Danışmanı
Yrd. Doç. Dr. Şamil ÜNSAL

İSTANBUL – 2014

STRATEJİK ARAŞTIRMALAR ENSTİTÜSÜ MÜDÜRLÜĞÜNE

Cuma ÖZÇOBAN'ın "21. Yüzyılda Ulusal Güvenliğin Sağlanmasında Siber İstihbaratın Rolü" adlı tez çalışması, jürimiz tarafından ULUSLARARASI İLİŞKİLER ana bilim dalında YÜKSEK LİSANS tezi olarak kabul edilmiştir.

Başkan

Prof. Dr. Tolga YARMAN

Üye

Yrd. Doç. Dr. Şamil ÜNSAL
(Danışman)

Üye

Yrd. Doç. Dr. Mehmet Sinan ALTUNÇ

ONAY
Yukarıdaki imzaların, adı geçen öğretim üyelerine ait olduğunu onaylarım.
/ 06 / 2014

Zekeriya TÜRKMEN
Dr. Öğ. Alb.
Enstitü Müdürü

ÖZET

21. yüzyılda bilim ve teknoloji alanındaki ilerlemeler güvenliğin yeni boyutlarının ortaya çıkmasına neden olmuştur. Uluslararası sistemin dengesini bozan organize suçlar, yasadışı göç, insan kaçakçılığı, siber terör ve siber savaş gibi yeni tehdit algılamaları ulusal güvenliğin kapsamını değiştirmiştir. Bu tehditler arasında siber uzaydan gelebilecek saldırılar çok daha ön plana çıkmaktadır.

İnternet kullanımının inanılmaz büyüme hızı ve bilgisayarların hayatın bir parçası haline gelmesi "siber uzay" kavramının daha sık kullanılmasına neden olmaktadır. Özellikle son yıllarda gelişen ve büyüyen siber uzay, beraberinde olası siber saldırılarla karşı karşıya kalınmasına sebep olmaktadır. Yapılan siber saldırılarının sebeplerinden biride siber uzayda yer alan bilgilere ulaşabilmektir. Bilgiye ulaşma adına 21. yüzyıl büyük fırsatlar sunmakta ve bunların başında siber uzay gelmektedir. Siber uzay ayrıca, kritik bilgilere de ulaşma imkânı sunmaktadır. Gelişmiş ve gelişmekte olan ülkelerin özel ve kamu kurumlarının alt yapı sistemleri siber uzaya bağımlı hale gelmekte ve ulusal güvenlikleri açısından kritik bir konuma ulaşmaktadır.

Devlet veya özel sektör eliyle yürütülen kritik alt yapı sistemleri, giderek siber uzaya bağımlı hale gelmektedir. Sağlıktan ekonomiye, savunma sistemlerinden yaşamsal kaynaklara kadar pek çok alanın, elektronik sistemler ve internet üzerinden kontrol edilmeye başlanmasıyla birlikte, siber uzaydan gelebilecek siber saldırılar ulusal güvenlik açısından önemli bir yer teşkil etmektedir. Siber uzaydaki kritik bilgilerin korunması da ulusal güvenliği sağlamada en üst seviyede önem arz ettiği değerlendirilmektedir. Devletlerin ulusal güvenlikle ilgili kritik bilgileri de siber uzayda yer almaktadır. Rakip veya hasım devletler, çeşitli gruplar, hackerlar bu bilgilere ulaşmak maksadıyla siber istihbarat çalışmaları yapmaktadırlar.

Bu çalışma, 21. yüzyılda ulusal güvenliğin tesis edilmesinde siber istihbarat faaliyetlerinin ne derece önemli olduğunu belirlemek için yapılmıştır. Soğuk Savaş sonrası dönemde güvenlik alanındaki değişimlere değinilmiş, yeni anlayış çerçevesinde ulusal güvenlik kavramı açıklanmıştır. Çalışmada, ulusal güvenliğin sağlanmasında yeni bir boyut olarak hayatın her aşamasında yer alan siber uzayın önemi üzerinde durularak, bu alandaki siber saldırılarla mücadelede siber istihbaratın gerekliliği açıklanmaya çalışılmıştır.

SUMMARY

The advances in science and technology in the 21st century security has led to the emergence of a new dimension. Destabilize the international system, organized crime, illegal migration, human trafficking, new threats such as cyber terrorism and cyber warfare have changed the scope of national security perceptions. These threats of cyber attacks that could come from cyber space are much more to the fore.

Incredible growth rate of internet usage and computer to become a part of life "cyber space" concept has led to more frequent use. Especially in recent years, developing and growing cyber space, together with a possible cyber attack has caused faced. In one of the causes of cyber attacks in cyberspace is to reach the information contained. Offers great opportunities to access information on behalf of the 21st century and the beginning of their cyberspace come. Cyberspace also offers critical information reach out. Private and public institutions of developed and developing countries, the infrastructure of becoming dependent on cyber space systems and national security are critical to reach a position .

Perpetrated by the state or private sector critical infrastructure systems, are becoming increasingly dependent on cyberspace. Health, economics, defense systems to vital resources many areas of electronic systems and internet control with the introduction cyberspace could come from cyber attacks, national security is an important place poses. Protection of critical information in cyberspace in providing the highest level of national security that is considered important. State of the critical information related to national security in cyberspace is located. Competitor or a hostile country, various groups, hackers obtain this information for the purpose of cyber intelligence work do.

This study on the establishment of national security in the 21st century cyber intelligence activities is done to determine what is crucial. Post-Cold War period has been referred to the changes in the security field, the new national security concept is explained in the framework of understanding. In this study, a new dimension in ensuring national security at every stage of life as the emphasis on the importance of cyberspace in this area in the fight against cyber attacks have tried to explain the need for cyber intelligence.

İÇİNDEKİLER

KISALTMALAR

ABD	:	AMERİKA BİRLEŞİK DEVLETLERİ
AR-GE	:	ARAŞTIRMA VE GELİŞTİRME
ARPA	:	ADVANCED RESEARCH PROJECT AGENCY
ARPANET	:	ADVANCED RESEARCH PROJECTS AGENCY NETWORK
ATM	:	AUTOMATED TELLER MACHINE
CIA	:	CENTRAL INTELLIGENCE AGENCY
CNN	:	CABLE NEWS NETWORK
CORPI	:	COPENHAGEN PEACE RESEARCH INSTİTUTE
CD	:	COMPACT DISC
DVD	:	DIGITAL VERSATILE DISC
FAPSI	:	FEDERAL AGENCY OF GOVERNMENT COMMUNICATIONS AND INFORMATION
GCHQ	:	GOVERNMENT COMMUNİCATIONS HEADQUARTERS
GDO	:	GENETİĞİ DEĞİŞTİRİLMİŞ ORGANİZMALAR
IMF	:	INTERNATIONAL MONETARY FUND
INTERNET	:	INTERCONNECTED NETWORKS
IP	:	INTERNET PROTOCOL ADDRESS
IRC	:	INTERNET RELAY CHAT
LAN	:	LOCAL AREA NETWORK
MİT	:	MİLLİ İSTİHBARAT TEŞKİLATI
M.Ö.	:	MİLATTAN ÖNCE
NATO	:	NORTH ATLANTIC TREATY ORGANİZATION
NGO	:	NON-GOVERNMENTAL ORGANISATION
NSA	:	NATIONAL SECURITY AGENCY
PROMIS	:	THE PROSECUTOR'S MANAGEMENT INFORMATION SYSTEM

RSA	**:**	RON RİVEST, ADİ SHAMİR, AND LEN ADLEMAN
SCADA	**:**	SUPERVISORY CONTROL AND DATA ACQUISITION
SQL	**:**	STRUCTURED QUERY LANGUAGE
TÜBİTAK	**:**	TÜRKİYE BİLİMSEL VE TEKNOLOJİK ARAŞTIRMA KURUMU
UEKAE	**:**	ULUSAL ELEKTRONİK VE KRİPTOLOJİ ARAŞTIRMA ENSTİTÜSÜ
VB.	**:**	VE BENZERİ

TABLOLAR LİSTESİ

HARİTALAR LİSTESİ

SAYFA

ŞEKİLLER LİSTESİ

SAYFA

GRAFİKLER LİSTESİ

SAYFA

ÖN SÖZ

Ulusal güvenlik kavramı 20. yüzyılda sadece ülke topraklarını korumak anlamına gelirken, 21. yüzyıl başlarında bu tanım yeterli görünmemektedir. 21. yüzyılda ulusal güvenliğin sağlanması çok boyutlu olarak ele alınmalı ve çalışmalar bu yönde yapılmalıdır. Uluslararası sistemin dengesini bozan organize suçlar, yasadışı göç, siber terör, siber istihbarat ve siber savaş gibi yeni tehdit algılamaları ulusal güvenliğin kapsamını değiştirmiştir.

21. yüzyılda ülkelerin özel ve kamu kurumlarının alt yapı sistemleri siber uzaya bağımlı hale gelmekte ve ulusal güvenlikleri açısından siber uzayın önemi artmaktadır. Günümüzde siber uzay kritik bilgilerin ele geçirilmesi için en büyük sistem haline gelmiştir. Rakip veya hasım devletler, çeşitli gruplar, hackerlar bu bilgilere ulaşmak maksadıyla siber istihbarat çalışmaları yapmaktadırlar. Bu gelişmeler ışığında, siber uzayda ulusal güvenliklerini sağlamak amacıyla siber istihbarata yatırım yapacak ülkelerin ilerleyen yıllarda sayısının ve bu konuya ayrılan ekonomik kaynakların daha da artacağı öngörülmektedir.

Bu tez çalışmasında 21. yüzyılda küreselleşen ve farklılaşan dünyada, yeni güvenlik ortamının beraberinde getirdiği risk ve tehdit türleri incelenmiştir. Çalışma ulusal güvenliğin korunması açısından önem taşıyan siber istihbaratın, devletlerin bekasının korumasında ne derece önemli olduğunun ortaya çıkarılmasını hedeflemektedir.

Yapılan tez çalışmayla ilgili olarak, öncelikle yüksek lisans eğitimi görmeme imkân tanıyan Kara Kuvvetleri Komutanlığı'na; çalışmamın her safhasında beni yönlendiren ve desteğini esirgemeyip yoğun çalışma temposu içinde kıymetli vakitlerini ayıran tez danışmanım, değerli hocam Yrd. Doç. Dr. Şamil ÜNSAL'a; iki yıl boyunca derslerde ve ders dışında bilgi ve tecrübelerini bizimle paylaşan değerli öğretim üyelerimize; yüksek lisans öğrenimi boyunca bilimsel çalışma ortamının sağlanmasına çok değerli katkıları olan SAREN idari kadrosuna; birlikte öğrenim gördüğüm sınıf arkadaşlarıma ve daha rahat bir çalışma ortamına sahip olmamı sağlayan ve gösterdiği fedakârlık ve manevi destekle daima yanımda olan aileme teşekkür ederim.

Cuma ÖZÇOBAN

GİRİŞ

Günümüzde önemli bir haberleşme sistemi olan internet 1960'da ABD Savunma Bakanlığı tarafından ARPANET adıyla kurulmuş ve 1990'dan sonra hızla gelişerek bugünkü halini almıştır. İnternet coğrafi olarak birbirinden ne kadar uzak olursa olsun dünyadaki siber uzaya bağlı bütün bilgisayarları birbirine bağlayabilmektedir. İnternet sayesinde mesafeler izafi olarak küçülmüş; dünyanın herhangi bir yerindeki bilgiye erişim hızı oldukça artmıştır. Basit bir fare tıklamasıyla dünyanın diğer ucundaki bilgiye saliseler içinde ulaşmak mümkün hale gelmiştir.

21. yüzyılda bilginin yanında, bilgiyi üreten, kullanan ve yöneten bilgi çağına girilmiştir. İçinde bulunulan çağın beraberinde getirdiği doğru bilgiye kısa sürede ulaşabilmek bütün kişiler, örgütler ve devletler için gereklilik haline gelmiştir. Bilgiye hâkim olan ve onu yöneten devlet, gücü elinde tutabilmektedir. Bu aşamada sahip olunan bilginin korunması ve yukarıda sayılan kullanıcılar tarafından ele geçirilememesi büyük önem arz etmektedir. Günümüzde siber uzay bilginin ele geçirilmesi için en büyük sistem haline gelmiştir.

Bilgiye ulaşma adına 21. yüzyıl büyük fırsatlar sunmakta ve bunların başında siber uzay gelmektedir. Siber uzay ayrıca, kritik bilgilere de ulaşma imkânı sunmaktadır. Gelişmiş ve gelişmekte olan ülkelerin özel ve kamu kurumlarının alt yapı sistemleri siber uzaya bağımlı hale gelmekte ve ulusal güvenlikleri açısından kritik bir konuma ulaşmaktadır. Bu fırsatlardan yararlanmak isteyen ülkelerde siber istihbarat faaliyetlerine önem vererek ve bu alanda on binlerce personel çalıştırarak ülkelerinin milli menfaatleri doğrultusunda çalışmalarını devam ettirmektedirler. Teknolojik gelişmelerin hızına bakıldığında ilerleyen yıllarda siber istihbarat faaliyetlerinin ulusal güvenlik açısından daha da önemli hale geleceği öngörülmektedir.

Siber uzay sunduğu fırsatlarla beraber çeşitli siber risklerde getirmektedir. Bunlar arasında siber terör, siber suç, siber istihbarat, siber saldırı, siber savaş vb. riskler yer almaktadır. Siber uzayın büyük bir hızla ilerlemesi nedeniyle bu risklerde, siber uzayın her bir parçasında ve seviyesinde hissedilmektedir. Siber uzay, önceleri maddi çıkar elde etmek, kötü niyetli amaçlar için kişisel olarak veya farklı suç örgütleri tarafından çeşitli amaçlarca kullanılırken artık günümüzde devletlerin etkin olarak kullanabileceği bir noktaya gelmiştir. 21. Yüzyıl çeşitli siber kavramlarının çok

daha sık kullanılacağı ve uygulamalarının gün geçtikçe daha çok görüleceği bir dönem olacaktır.

İnternet'in ve bilgisayar ağlarının toplumun bütün katmanlarına yayılması ve devletlerin birçok kamu sektöründe bu teknolojileri kullanılmasına paralel olarak, istihbarat örgütleri de bu teknolojilerden yoğun olarak yararlanmaktadırlar. Dünyadaki birçok ülke siber saldırı faaliyetlerini tespit etmeye ve önlem almaya çalışmaktadır. Hazırlanan raporlar ve tespit edilen örnek olaylar siber istihbaratın ulaştığı boyutu gözler önüne sermektedir. Dolayısıyla istihbarat kurumlarının bugüne kadar yeterince üstünde durmadıkları siber istihbarat çalışmalarının ulusal güvenliği sağlamada en üst seviyede önem arz ettiği değerlendirilmektedir.

Devletler teknolojik gelişmeler ışığında faaliyetlerini siber uzaya taşımak zorunda kalmaktadırlar. Bu çerçevede devletlerin sahip oldukları tüm veriler, bilgiler siber uzayın bir parçası haline gelmektedir. Bu doğrultuda devletlerin ulusal güvenlikle ilgili kritik bilgileri de siber uzayda yer almaktadır. Rakip veya hasım devletler, çeşitli gruplar, hackerlar bu bilgilere ulaşmak maksadıyla siber istihbarat çalışmaları yapmaktadırlar.

Bu çalışmadaki temel amaç, 21. yüzyılda küreselleşen dünyada farklılaşan güvenlik ortamının beraberinde getirdiği yeni risk ve tehdit türleri içerisinde bulunan ve ulusal güvenliğin korunması açısından fazlasıyla önem taşıyan siber istihbaratın, devletlerin bekasının korumasında ne derece önemli olduğunu ortaya koymaya çalışmaktır.

Siber istihbarat ile ilgili birçok ülke çalışmalar yürütmektedir. Ancak hiçbir ülke siber istihbarat sistemini ve bu alanda sahip olduğu imkân ve kabiliyetleri açıklamamaktadır. Ülkelerin siber istihbarat faaliyetleri ile ilgili çalışmaları çoğunlukla gizli olduğundan, ilgili bölümlerde mümkün olduğu kadar yasal mevzuatla birlikte daha çok haber ve rapor gibi unsurlardan yola çıkarak inceleme yapılmıştır.

Bu çalışmada siber istihbarat alanında öne çıkan ülkelerin siber istihbarat sistemleri açıklanmaktadır. Bu sebeple ilgili bölüm sadece ABD, Çin ve Rusya ele alınarak sınırlandırılmıştır.

Araştırmada kullanılan veriler; kütüphaneler, akademik veri tabanları, bilimsel yayın tarama siteleri, medya ve internet arşivleri, resmi internet sitelerinden elde

edilen birincil ve ikincil kaynaklardan istifade edilerek belgesel tarama yöntemi ile elde edilmiştir.

Tezin birinci bölümünde öncelikle güvenlik kavramı açıklanarak, güvenlik teorilerinin düşünsel temelleri ışığında, realist, neorealist, liberal, marksist, kopehhag ekolü teorileri, güvenlik çerçevesinde ele alınmıştır. Birinci bölümün devamında ise ulusal güvenlik kavramı çok boyutlu olarak değerlendirilmiştir. Günümüzün ulusal güvenlik anlayışı ve klasik güvenlik anlayışı arasındaki farklar irdelenmiştir. Daha sonra ise istihbarat tarihi genel hatlarıyla ele alınmış, devamında ise çalışma için anahtar bir kavram olan istihbarat kavramı ele alınarak, istihbarat çarkına değinilmiş ve müteakiben elde edilişi bakımından istihbarat türleri olan açık kaynak istihbaratı, insan istihbaratı ve teknik istihbarat açıklanmıştır.

İkinci bölümde genel bir çerçeve dâhilinde siber istihbaratın anlaşılması maksadıyla çeşitli kavramlar ele alınmıştır. Öncelikle siber istihbarat kavramının ortaya çıkmasının en önemli unsuru olan internet kavramı açıklanmış, müteakiben siber, siber uzay, hacker, siber saldırı, siber terörizm, siber savaş kavramları açıklanmıştır. Müteakiben ise siber saldırı kavramı çerçevesinde, siber uzayda tehdit ve tehlike oluşturan araç ve yöntemler irdelenmiştir. Burada yer alan araç ve yöntemler bu bölümde sayılanlarla sınırlı olmayıp siber uzayda en çok karşılaşılan tehdit ve tehlike vasıtaları açıklanmıştır.

Üçüncü bölümde öncelikle siber istihbarat kavramı ve siber istihbarat elde etme yöntemleri ayrıntılı olarak açıklanmıştır. Daha sonra ise ulusal güvenlik ve siber istihbarat ilişkisi ele alınmıştır. Müteakiben bu ilişkinin daha iyi anlaşılabilmesi maksadıyla geçmişte yaşanmış siber istihbarat örnek olayları incelenerek, uygun olduğu değerlendirilenlere yer verilmiştir. Bölüm sonunda ise siber istihbarat alanında ön plana çıkan ABD, Rusya ve Çin siber istihbarat sistemleri incelenmiştir.

BİRİNCİ BÖLÜM
GÜVENLİK VE ULUSAL GÜVENLİK ALGILAMASI

1.1. GÜVENLİK ALGILAMASI

1.1.1. Kavramsal Olarak Güvenlik

Güvenlik kavramı ilk insanın varoluşundan itibaren hayatımıza girmiş ve günümüze gelene kadar çeşitli evrelerden geçmektedir. Bu nedenle tarihin hangi dönemine bakılırsa bakılsın güvenlik kavramı bir süreç içerisinde değerlendirilmektedir. Korunma isteğiyle ortaya çıkan ve koruma dürtüsüyle kurumsallaşma eğilimine giren güvenlik, fonksiyonel olarak; personel güvenliği, sektör güvenliği, kamu güvenliği ve ulusal güvenlik gibi çeşitli alanları ihtiva etmektedir.[1] Özellikle ulusal güvenlik, devletler için tarih boyunca varlıklarının muhafazası ve devamı noktasında önemli bir yer teşkil etmektedir.

Maslow'un ihtiyaçlar hiyerarşisi teorisinde fizyolojik gereksinimlerden sonra ikinci sırada belirtilen güvenlik gereksinimi, insanın bekasını devam ettirebilmesi adına vazgeçemeyeceği bir olgudur. Güvenlik ne demektir sorusunun tüm zamanlar ve mekânlar için geçerli olacak tek bir cevabı yoktur. Aktörleri devletten, bireye kadar değişiklik göstermektedir. Güvenliği, özünde tartışmalı değil de yeterince açıklanmamış bir kavram olarak tanımlamak daha doğrudur.[2] Güvenlik kavramı üzerine yapılan birçok çalışmaya rağmen hâlâ herkesçe kabul görmüş bir güvenlik tanımının yapılamaması bu kavramın çok boyutluluğu ile doğrudan ilişkilidir.

Türkçede güvenlik kelimesi, itimat ya da inanmak anlamına gelen güven (küven) kökünden türetilmiştir. 8 ile 11'nci yüzyıl arasında Orta Asya Türkçesinde ün, nam, iktidar anlamında kullanılan "küve" ya da "küv" kelimeleri, kelimenin etimolojik kökenini oluşturmaktadır. Böbürlenmek, mağrur olmak anlamına da gelen "küven" kökünden dolayı kelime 19'ncu yüzyıla dek genelde olumsuz anlamda kullanılmıştır. Güvenlik ise sıfatlardan soyut ad ya da adlardan işlev belirten ad türeten –lik ekinin eklenmesiyle elde edilir. Bu haliyle günümüz Türkçesinde kullanılan "güvenlik" dil devrimi bünyesinde türetilmiş bir kelimedir.[3]

---

[1] Sait Yılmaz, ***21. Yüzyılda Güvenlik ve İstihbarat***, Milenyum Yayınları, İstanbul, 2007, s.210.
[2] David A. Baldwin, "Güvenlik Kavramı", Çev. Çiğdem Şahin, ***Uluslararası Güvenlik Sorunları,*** ASAM Yayınları, Ankara, 2004, 1-36, s.32.
[3] Sevan Nişanyan, ***Sözlerin Soyağacı***, Everest Yayınları, İstanbul, 2009, s.219.

Her dilde bu anlamı içeren bir kavram olmasına karşın güvenlik kelimesinin uluslararası alanda daha fazla kullanılan İngilizce karşılığı "security" kelimesidir. "Security" kavramı etimolojik olarak Latince iki kelimeden oluşmaktadır. Latincede "se" (sız-siz) "cura" (dert) anlamına gelmektedir. Bu iki kelimenin birleşmesinden meydana gelen güvenlik kavramı köken itibariyle "dertsiz", derdi olmayan anlamına gelmektedir.[4]

"Güvenlik" kavramı batı geleneğinde zihnin felsefi ve psikolojik durumunu ifade eden anlamında ilk olarak Cicero ve Lucretius tarafından "securitas" olarak oluşturulmuş ve 1. yüzyıldan itibaren de "Pax Romana" bağlamında temel bir siyasi kavram olarak kullanılmıştır. Ancak, güvenliğin Thomas Hobbes (1651) ile başlayan ve "güvenlik" kavramını otoriter "süper devlet'in doğuşu" (Hobbes'un iç savaşın önlenmesine adanmış Leviathan'ı) ile bağlantılı olarak ele alan Thucydides'den etkilenmiş diğer bir kökeni de vardır. Arends "bu yüzden çağdaş 'güvenlik' kavramı a) antik Atinalıların imparatorluklarının yıkılmasını önleme niyetleri, b) Roma 'securitas'ının dini çağrışımları ve c) Hobbesçu iç savaşı önleme amacının 'hayali' bir birleşimidir" diye iddia etmiştir.[5]

Türk Dil Kurumu sözlüğünde güvenlik, "Toplum yaşamında yasal düzenin aksamadan yürütülmesi, kişilerin korkusuzca yaşayabilmesi durumu, emniyet"[6] olarak tanımlanmıştır. Güvenlik kelimesi en basit tanımıyla tehditler, kaygılar ve tehlikelerden uzak olma hissi anlamına gelmektedir. Birçok yazar ve düşünür güvenliği tanımlama yoluna gitmişlerdir. David Baldwin 1997 yılında yayınladığı, "Güvenlik Kavramı" isimli makalesinde güvenliği kısaca, "Sahip olunan değerlerin korunması"[7] olarak tanımlamıştır.

Değerlerin, tehditlerin ve tehlikelerin her geçen gün daha hızlı değiştiği bir dünyada, güvenlik tanımının sabit kalması beklenemez. Günümüz dünyasında güvenlik hususunun değişim yaşadığı aşikârdır. Hem devletler hem de insanlar arasında yaşanan güvenlik algısının değişimi, bu hususun anlaşılmasını zor

[4] Muhittin Demiray ve İsmail Hakkı İşcan, "Uluslararası Sistemde Güvenlik Kavramının Değişimi Ekonomik ve Jeopolitik Arka Planı", ***Dumlupınar Üniversitesi Sosyal Bilimler Dergisi***, 2008, Sayı:21, 141-170, s.150.
[5] Hans Günter Brauch, "Güvenliğin Yeniden Kavramsallaştırılması: Barış, Güvenlik, Kalkınma ve Çevre Kavramsal Dörtlüsü",***Uluslararası İlişkiler Akademik Dergisi***, Cilt 5, Sayı 18, 2008, 1-47, s.2-3.
[6] Türk Dil Kurumu Resmi İnternet Sayfası, http://www.tdk.gov.tr/index.php?option=com_gts&arama=gts&guid=TDK.GTS.50f852315d7c99.55582901, (Erişim tarihi: 11.01.2014).
[7] David A. Baldwin, "The Concept of Security", ***Rewiew of International Studies***, 1997, Vol:23, Issue:01, p.11.

kılmaktadır. Değerlerin değişmesi ile güvenlik kavramının kapsamı ve içeriği değişebildiği gibi yeni değerlerin ortaya çıkmasıyla yeni güvenlik türleri ile tanışmak mümkün olmaktadır. Örneğin, ilk insan topluluklarında, sahip olunan bireysel değerler hayatta kalma, aç kalmama ve barınma ihtiyaçları iken günümüzde özgürlük, zenginleşme, onur gibi daha birçok değere kavuşmasıyla bireysel güvenlik tanımının içeriği de genişlemiştir.[8] Gelecekte de içeriğinin genişlemeye devam edeceği aynı zamanda yeni güvenlik türlerinin de ortaya çıkabileceği öngörülmektedir.

Güvenlik, tehlikeden uzak olma durumu, insanoğlunun var olduğu günden itibaren en önemli meselelerden birisi olmuş, bireyden, topluma ve devlet oluşturma sürecinde önemini korumuştur. Tarihi süreç içerisinde güvenlik insan için fizyolojik ihtiyaçlardan sonra gelmiş ve gelmeye devam etmektedir. Tıpkı insanlar gibi diğer tüm canlılar ve devletler güvenliklerini sağlamak maksadıyla büyük emek harcamaktadırlar.

Güvenlik kavramı, tehdit ve risk algılamaları ile sürekli değişikliğe uğramaktadır.[9] Güvenlik ve tehdit, karşılıklı ve sürekli olarak birbirlerini tetikleyen iki kavramdır. Algılanan tehdide göre alınan güvenlik tedbirleri de farklılık göstermektedir. Soğuk Savaş'ın hüküm sürdüğü dönemde devletlerin güvenliği caydırıcılık esasına dayandırılmıştır. Buna göre, her hangi bir devlet revizyonist amaçlarla hareket edip sistemi baştan şekillendirmeye çalıştığında, diğer güçler, 'güçler dengesi' prensibi gereği, bir araya gelip karşı bir dengeleyici blok oluşturmaktaydılar. Başka devletleri güvensizliğe itecek politikaların bu politikaları uygulayanlar açısından maliyetli olacağının gösterilmesine dayanan caydırıcılık politikası, karar alıcıların rasyonel hareket ettiklerini varsaymaktaydı.[10]

Yirminci yüzyılın ilk yarısını belirleyen, iki dünya savaşı yaşanmıştır. Dimağlarda, bu dönemin tortusu olarak hemen herkesin herkesle, üstelik tüm dünya ölçeğine tırmandırılabilecek askeri çatışmalara girişebileceği, çok acı biçimde ortaya çıkmıştır.[11] Soğuk Savaş döneminde güvenlik, daha çok bir ülke silahlı kuvvetlerinin karşı ülkelerde yarattığı tehdit ve buna karşı alınan tedbirler olarak gündeme

[8] Fatih Beren, ***Demokrasi ve Özgürlüğün Teminatı Olarak İçgüvenlik İstihbaratı***, Alfa Yayınları, İstanbul, 2011, s.1.
[9] Bekir Aydoğan ve Hakan Aydın, ***a.g.e.,*** s.30.
[10] Tarık Oğuzlu, "Dünya Düzenleri ve Güvenlik: Ulus-Devlet Güvenlik Anlayışı Aşılıyor mu?", ***Güvenlik Stratejileri Dergisi,*** 2007, Yıl: 3, Sayı: 6, 7-41, s.13.
[11] Tolga Yarman, ***Teknoloji Alanında Türkiye'nin Güvenlik İhtiyaçları Ne Şekilde Karşılanabilir: Değişen Dünya Düzeni ve Türk Savunma Sanayi***, Işık Üniversitesi, 2003, s.1.

gelmiştir. İki kutuplu dünya düzeninin de demir perdenin yıkılmasını müteakip oluşan yeni dünya düzeni içerisinde tehdit ve buna bağlı olarak güvenlik algılamaları da değişmiştir.[12] Soğuk Savaş döneminde güvenlik elli yıl boyunca, sivil özgürlüklerin askıya alınmasını, yapılan savaşları ve kaynakların etkili şekilde yeniden tahsis edilmesini haklılaştırmak için kullanılagelmiş önemli bir kavramdır.[13] Kısaca Soğuk Savaş döneminde güvenlik kavramı birçok ülke tarafından yapılan faaliyetleri haklı göstermek maksadıyla örtü olarak kullanıldığı söylenebilir. Bu dönemde zaman içersinde güvenliğin yeni boyutları ortaya çıkmıştır. Yeni güvenlik boyutlarının ortaya çıkması, beraberinde güvenlikle ilgili farklı fikirlerin, görüşlerin oluşmasına sebep olmuştur.

Bireyin güvenliğinden toplumun güvenliğine, devletin güvenliğinden sistemin güvenliğine kadar her alanda klasik güvenlik tanımı ve araçları yetersiz kalmaya başlamış; bu değişim-dönüşümü yakalamaya çalışan güvenlik kavramsallaştırmaları gündeme gelmiştir.[14] Dolayısıyla kim için, hangi tehditlere karşı, hangi değerlerin korunması amacıyla, hangi araçları kullanarak, ne kadar maliyette, hangi zaman dilimi içerisinde ve ne kadar koruma planlandığı bir taraftan da güvenlik tür ve modelini ortaya koymaktadır.[15] Bu çerçevede birçok kişi tarafından farklı tür ve modelde güvenlik ele alınmıştır. Bu bağlamda bunlardan bazılarını incelediğimizde;

Beril Dedeoğlu güvenlik kavramını asal olarak birkaç tür ve modelde ifade etmiştir. Bunlar;[16]

a) Uluslar arası sistemin bütünü ya da bütününe yakının güvenliği,

b) Coğrafi ya da işlevsel alt sistemlerin, bölgelerin güvenliği,

c) Devletin Güvenliği,

d) Toplumun güvenliği,

e) Toplumsal alt grupların güvenliği,

---

[12] Ahmet Küçükşahin ve Tamer Akkan, "Değişen Güvenlik Algılamaları Işığında Tehdit ve Asimetrik Tehdit", ***Güvenlik Stratejileri Dergisi,*** 2007, Yıl: 3, Sayı: 5, 41-66, s.43.

[13] David A. Baldwin, "Güvenlik Kavramı", Çev. Çiğdem Şahin, ***Uluslararası Güvenlik Sorunları***, ASAM Yayınları, Ankara, 2004, 1-36, s.7.

[14] Nihal Ergül, "Yeni Güvenlik Anlayışı Kapsamında Birleşmiş Milletler'in Rolü ve Uygulamaları", ***Teoriler Işığında Güvenlik, Savaş, Barış Ve Çatışma Çözümleri,*** BİLGESAM Yayınları, 2012, 163-208, s.165.

[15] Fatih Beren, ***a.g.e.***, s.35.

[16] Beril Dedeoğlu, ***Uluslararası Güvenlik ve Strateji***, Yeniyüzyıl Yayınları, İstanbul, 2008, s.24-25.

f) Bireylerin güvenliği.

Hans Günter ise güvenlik kavramının farklı türlerini aşağıdaki tablo ile ifade etmiştir.

Tablo-1: Genişletilmiş Güvenlik Kavramları[17]

Genişletilmiş Güvenlik Kavramları			
Güvenlik Kavramları	**Gösterilen (Kimin Güvenliği?)**	**Risk Altındaki Değer (Neyin Güvenliği?)**	**Tehdit Kaynağı/Kaynakları (Kimden/Neden Korunma?)**
Ulusal Güvenlik [Siyasi, Askeri Boyut]	Devlet	Egemenlik, Toprak Bütünlüğü	Diğer Devlet, Terörizm (Devlet Dışı Aktörler)
Toplumsal Güvenlik [Boyutu]	Milletler, Toplumsal Gruplar	Ulusal Birlik, Kimlik	(Devletler) Milletler, Göçmenler, Yabancı Kültürler
İnsan Güvenliği	Bireyler, İnsanlık	Beka, Hayat Kalitesi	Devlet, Küreselleşme, Küresel Çevre Sorunları (GEC), Doğa, Terörizm
Çevresel Güvenlik [Boyutu]	Ekosistem	Sürdürülebilirlik	İnsanlık
Cinsiyet Güvenliği	Cinsiyet İlişkileri, Yerli Halk, Azınlıklar	Eşitlik, Kimlik, Dayanışma	Ataerkillik, Totaliter/Erkteke lci Kurumlar (Hükümetler, Dinler, Elitler, Kültür), Hoşgörüsüzlük

Sait Yılmaz ise güvenliğin kapsamını şu tabloyla ifade etmiştir;

[17] Hans Günter Brauch, ***a.g.e.***, s.11.

Tablo-2: Güvenliğin Kapsamı[18]

Kapsam	Nitelik	Tür
Askeri	Devlet Kaynaklı	* Savaş(Konvansiyonel, Nükleer) * Savaş benzeri operasyonlar * Düşük yoğunluklu savaşlar * Barışı koruma operasyonları * Devlet terörü, yıkıcı faaliyetler * Örtülü operasyonlar/faaliyetler
	Devlet Dışı Aktörler	* Terör * Gerilla faaliyetleri * İç savaş
Askeri Olmayan	Politik	* Zorlayıcı Diplomasi * Kontrol altına alma * Güvenlik ortamını şekillendirme
	Ekonomik	* Ekonomik yaptırımlar * Enerji Güvenliği * Dış borç - Finans oyunları * Ekonomik depresyon, İşsizlik * Yoksulluk, kıtlık, açlık
	Sosyal	* Misyonerlik * Kadın ve insan hakları ihlalleri * Etnik ve dini çatışmalar * Nüfus artışı, beyin göçü, çocuklar * Kültürel yozlaşma * Kimlik Problemleri * Irk ayrımcılığı * Cinsel konular * Şehirleşme
	Çevre	* Çevre kirliliği * Ozon delinmesi, asit yağmurları * Küresel ısınma, denizaltı kaynakları * Ormanların yok edilmesi * Çölleşme, biyo-çeşitlilik
	Sağlık	* Hastalıklar * Göç, beslenme * Yerinden edilmiş kişiler/mülteciler * Su ve su kirliliği
	Doğal Afetler	* Sel * Deprem * Kasırgalar * Volkan patlamaları * Yangınlar * Uzay cisimleri
	Kazalar	* Ulaştırma kazaları * Bina kazaları * Sanayi kazaları * Kişisel yaralanmalar
	Suçlar	* Narkotik * Adi suçlar * İnternet Suçları

[18] Sait Yılmaz, ***a.g.e.***, s. 212.

Güvenlik alanındaki ilk çalışmalar ABD'de İkinci Dünya Savaşı sonrasında başlamış ve başlangıçta dar bir kapsam içererek, uluslararası gerilimin daha çok askeri yönlerine odaklanmıştı. Güvenlik çalışmalarının Rönesans'ı, 1970'lerin ortasında Ford Vakfı'nın güvenlik sorunlarında çeşitli akademik merkezleri destekleme kararı alması ve güvenlik ile ilgili bilimsel bir forum haline gelen "International Security" dergisinin kurulması ile başladığı kabul edilmektedir.[19]

Soğuk Savaş döneminde güvenlik daha çok askeri anlamda tanımlanmıştır. Bu konulara 'yüksek politika' denilmiştir. Askeri konular dışındaki konuların, örneğin ekonomi, çevre, sağlık, göçler gibi, güvenlik sorunları olarak ortaya çıkması mümkün olmamıştır. Bu konular daha çok 'alçak politikanın' konuları olarak değerlendirilmişlerdir. Bu çerçevede düşünüldüğünde devleti yöneten askeri ve politik elitin güvenliğin tanımlanmasında en etkili birimler oldukları öne sürülebilir. Neyin güvenlik sorunu olup olmadığına bu elitler karar vermişlerdir.[20] Soğuk Savaş dönemi boyunca devleti yönetenler güvenlik kavramını, insanlar üzerindeki etkisinin askeri güvenlik algılamasıyla birleştirmiş ve diğer alanlarda ki güvenlik boyutlarına önem vermemiştir. Bunun önemli sebeplerinden birinin tehdit algılamasında Soğuk Savaş'ın birinci sırada yer alması oluşturmaktadır. Ancak Soğuk Savaş'ın bitimini müteakip güvenliğin diğer boyutları ortaya çıkabilmiştir.

1.1.2. Günümüzde Güvenlik

21. yüzyılın ilk çeyreğinde dünya da meydana gelen değişimler bugüne kadar ki dengeleri değiştirmiştir. Yeryüzü terör, işsizlik, açlık, iç çatışmalar, bilgi terörü, ekonomik dengesizlikler, etnik huzursuzluklar, siyasi istikrarsızlıklar, dinsel tehditlerle doludur.[21] Güvenlik kavramı sadece askeri bir kavram olmaktan çıkarak büyük ölçüde siyasi bir kavram haline dönüşmüştür. Özgürlük, demokrasi, serbest piyasa ekonomisi, ekonomik refah ve gelir paylaşımında adalet, güvenlik uygulamaları içinde yer almaya başlamıştır.[22] Güvenlik ve istihbarat faaliyetlerinin kapsam ve aktörleri genişlemiş, asimetrik güç dengesi içerisinde gittikçe daha teknolojik, farklı ve örtülü yöntemlere başvurulması ile uluslararası güvenlik ortamında kaos artmıştır.[23] Özellikle de bilim ve teknoloji alanındaki ilerlemeler, güvenliğin yeni boyutlarının ortaya çıkmasına neden

[19] Sait Yılmaz, ***a.g.e.***, s.17.
[20] Tarık Oğuzlu, ***a.g.m.***, s.14.
[21] Şamil Ünsal, "Milli Güç, Bileşenleri ve Vasıtaları", ***Türk Dünyası Araştırmaları***, 2010, Sayı: 187, 27-50, s.48.
[22] Bekir Aydoğan ve Hakan Aydın, ***a.g.m.***, s.34.
[23] Sait Yılmaz, ***a.g.e.***, s.277.

olmuştur. Güvenliğin yeni boyutlarının ortaya çıkmasıyla tehdit algılamaları içerisine özellikle siber uzay ve bu alandaki faaliyetler de girmiştir. Gelecekte de bu alandan gelebilecek tehditlerin artacağı öngörülmektedir.

Benzerlik ve farklılıkların eş zamanlı olarak iç içe girdiği ve arttığı 21. yüzyıl küresel sisteminde güvenlik ve tehdit kavramları da dönüşüme uğramaktadır. Geleneksel güvenlik düşüncesinden duyulan hoşnutsuzluk, güvenlik kavramının 'genişletilmesi' veya 'güncelleştirilmesi' için sık sık yapılan çağrılarda kendini göstermiştir.[24] Güvenliğin genişlemesi ve derinleşmesine paralel olarak "kim için, ne için, nerede, nereye kadar ve nasıl güvenlik?" soruları çerçevesinde alternatif güvenlik çalışmaları gündeme gelmektedir.[25]

Güvenliğin eskiden tek bir kavram olduğu ve sonraları farklı türlere ayrıştığı bilinmektedir. Değerleri korunması gereken aktörlere, ilgili değerlere, güvenliğin derecesine, tehdit türlerine, bu tehditlerle başa çıkmak için kullanılan araçlara, bunu gerçekleştirmenin maliyetlerine göre, güvenlik tayin edilebilmektedir.[26] Günümüzde yaşanan değişimler ve tehdit algılamaları doğrultusunda, siber güvenlik, bireysel güvenlik, toplumsal güvenlik, ulusal güvenlik, kolektif güvenlik, küresel güvenlik, bilgi güvenliği ve gıda güvenliği gibi birçok güvenlik türünden söz edildiği görülmektedir.

Güvenliğin birey veya grupların temel değerlerine olan tehditten arınma ölçüsüne göre göreceli bir kavram olduğu konusunda birleşen bilim adamları; yeni güvenlik anlayışının bireysel, ulusal ya da uluslararası düzeyden hangisine odaklanması gerektiği konusunda ortak bir fikre sahip değildirler.[27] Yeni güvensizlik ortamında coğrafi uzaklıkların ve fiziki sınırların önemi, artık büyük ölçüde azalmaktadır. Bu denli tehdit kaynakları, hem zaman-mekân ile çizilmiş sınırların dışına çıkmakta hem de maddi güvenlik alanlarının ötesinde psikolojik bir nitelik taşımaktadır. [28] Çağdaş güvenlik sorunlarının üç temel özelliği; yayılganlık, karmaşıklık ve belirsizlik (çeşitli olasılıklara açık olma) olarak kabul edilmektedir.[29]

Soğuk Savaş sonrası dünyada yaşanan değişimler sonucu klasik güvenlik anlayışının tek ve değişmez aktörü olan devletin güvenliğinin yanı sıra insan

---

[24] Ken Booth, "Güvenlik Ve Özgürleş(tir)me", ***Avrasya Dosyası Dergisi***, Cilt: 9, Sayı: 2, 2003, 51-70, s.58.
[25] Atilla Sandıklı ve Bilgehan Emeklier, "Güvenlik Yaklaşımlarında Değişim ve Dönüşüm", ***Teoriler Işığında Güvenlik, Savaş, Barış ve Çatışma Çözümleri,*** BİLGESAM Yayınları, 2012, 3-67, s.26.
[26] David A. Baldwin, "Güvenlik Kavramı", ***a.g.m.***, s.21.
[27] Sait Yılmaz, ***a.g.e.***, s.246.
[28] Atilla Sandıklı ve Bilgehan Emeklier, ***a.g.m.***, s.35.
[29] Sait Yılmaz, ***a.g.e.***, s.251.

güvenliği, toplum güvenliği ve küresel güvenlik vb. tartışmaların çerçevesinde, devlet güvenliğinin ötesinde farklı boyutlarda güvenliğin ele alınması gerektiği tartışılmaya başlanmıştır.

Toplumsal güvenlik, en yalın anlatımla "toplumsal değerlerin korunması" olarak ifade edilebilir. Toplumsal yaşamın sürdürülebilmesi, hatta daha kaliteli bir seviyeye taşınabilmesi için gerekli olan bütün etmenler toplumsal değer olarak tanımlanabilir. Bunlar aile, eğitim, kültür, meslek, sosyal ve ekonomik ilişkiler, adalet, güven vb. olarak örneklendirilebilir.[30] Toplumun, devletten sonra güvenliğin en asli ikinci unsuru olduğu kabul edilmektedir. Toplumsal güvenlik denildiğinde, dışarıdan kültürüne, diline, dinine, geleneklerine ve milli değerlerine yönelik tehditlere karşı koruma anlamına gelmektedir.

Güvenlik; bireyin, toplumun ve devletin varlığını koruyabilme durumunu ifade eder. Güvenlik, ilk olarak bireyin varlığı ve varlığını sürdürebilmesi açısından düşünülür ve insanlığın doğuşuyla sistemde kendine yer edinmiştir. Birey, kendini güvende hissettiği sürece topluma karışır ve toplumda rol üstlenir. Bu anlamda, toplumun da kendini güvende hissediyor oluşu, toplumu devletle bütünleştirir ve toplumda oluşan "güvende"lik hissi devlete de yansımış olur.[31]

Türk Dil Kurumu sözlüğünde birey kavramı kendine özgü nitelikleri yitirmeden bölünemeyen tek varlık, fert olarak tanımlanmıştır.[32] İnsan güvenliği ya da bireysel güvenlik olarak ifade edilen kavram, temelde bireyin güvenliğini ifade eder.[33] Günümüzde yaşanan değişimler çerçevesinde bireyselliğin ön plana çıkmasıyla, birey güvenliğinin öneminin her geçen gün daha da arttığı değerlendirilmektedir. İnsanlar bireysel güvenliklerini sağlama adına çok farklı alanlarda farklı çalışmalar yapmaktadırlar.

Bireyler için güvenlik kolaylıkla tanımlanamaz. Zira güvenlik faktörleri olan hayat, sağlık, statü, zenginlik ve özgürlük kavramları karmaşıktır ve bunların çoğu kaybedildiğinde geri gelmesi nerdeyse imkânsızdır. Diğer taraftan, bireyin kendini güvenli kılması demek, birçok açıdan kendisini hapsetmesi anlamına gelmektedir. Zira güvenliği bu çerçevede sağladığını düşünen birey kendini riske atmadan

[30] Fatih Beren, ***a.g.e.***, s.37.
[31] Bekir Aydoğan ve Hakan Aydın, ***a.g.e.***, s.27
[32] Türk Dil Kurumu Resmi İnternet Sayfası, http://www.tdk.gov.tr/index.php?option=com_gts&arama=gts&guid=TDK.GTS.52cee298dd1981.07897246, (Erişim tarihi: 09.01.2014).
[33] Fatih Beren, ***a.g.e.***, s.35.

güvenli bir yeri terk edemez hale gelecektir.[34] Bu sebeple bireylerde dâhil olmak üzere özgürlük ve güvenlik dengesinin güvenliğin tüm boyutlarında sağlanması gerektiği değerlendirilmektedir. Bu dengenin gelecekte de önemini koruyacağı ve tartışılacağı düşünülmektedir.

İletişim devrimiyle birlikte bireylerin güvenliği, savaş ve çatışmalar dışında da her an her yerden gelebilecek tehditlerle karşı karşıya kalabilmektedir. Bugün Şangay'daki bir hacker İstanbul'daki bir bilgisayara saldırıda bulunabilmekte ya da GDO'lu bir ürün dünyanın farklı bölgelerindeki insanların genetik kodlarını etkileyebilmektedir.[35] İletişim devrimi ve küreselleşme ile bireysel güvenlik çok daha hassas kırılgan hale gelmektedir. İnsanların sahip oldukları mahremiyet alanı gittikçe daralmaktadır. İnsanların çevresi adeta siber ağlarla çevrilidir. Siber uzay vasıtasıyla birçok kişisel bilgi kolaylıkla el değiştirebilmektedir.

Küresel güvenlik dediğimiz kavram ise daha geniş bir anlam ifade etmektedir. Küreselleşmeye çalışan dünya içerisinde uluslararası sistemin güvenliğinin sağlanması, bu sisteme yönelik tehditlerle mücadele edilmesi küresel güvenliğin ana konusunu oluşturmaktadır. Güvenlik tüm insanlıkla doğrudan ilişkilidir.[36] Küresel güvenlik, dünyanın tamamını ilgilendiren, ortak katkı yapılmadığı takdirde herkesin olumsuz olarak etkilenebileceği güvenliktir. Küreselleşme ile dünyanın adeta bir köy haline gelmesi nedeniyle, küresel güvenliğin gelecekte daha da ön plana çıkabileceği öngörülmektedir.

1.1.3. Güvenlik Teorilerinin Düşünsel Temelleri

Uluslararası ilişkiler alanındaki teorik çalışmalar Aristo ve Eflatun'a atıflar yaparak eski Yunan polis-devleti dönemine kadar geri götürülmektedir. Diplomasinin altın çağı olarak nitelenen 1648 – 1914 yılları arasındaki dönemde bile uluslar arası ilişkiler alanındaki çalışmalarda sürecin analizi yerine, uluslararası hukuk ve diplomasi tarihi üzerinde durulmuştur. [37] Uluslararası ilişkilerin akademik bir disiplin

[34] Haşim Türker, ***Avrupa Güvenlik ve Savunma Politikası***, Nobel Yayın Dağıtım, Ankara, 2007, s.9.
[35] Johan Eriksson and Giampiero Giacomello, "The Information Revolution, Security, and International Relations: (IR) Relevant Theory?", ***International Political Science Review****, Vol:* 27, No: 3, 2006, 221-244, pp.233-234.
[36] Şeref Çetinkaya, "Güvenlik Algılaması ve Uluslar arası İlişkiler Teorilerinin Güvenliğe Bakış Açıları", ***21. Yüzyılda Sosyal Bilimler Dergisi***, Sayı: 2, 2013, 239-260, s.245.
[37] Sait Yılmaz, ***a.g.e.***, s.7.

haline gelmesi 1919 yılında Galler Aberystwyth Üniversitesi'nde bir bölüm olarak açılması ile mümkün olmuştur.[38]

Uluslararası ilişkiler alanında ilk kuramsal yaklaşım, Batı düşünce tarzı içinde Anglo-Sakson geleneğin ürünü olan liberalizmin bir yansıması olarak "idealizm" Birinci Dünya Savaşı sonrasında on yıl kadar egemen bir görüş olarak kabul edilmiştir. İdealizm, bilimsel alanda bir teori olmaktan çok bir idealler demeti olarak uluslararası ilişkilerin nasıl yapılanması gerektiği hususu üzerinde durmuştur.[39] Birinci Dünya savaşı sonrası, Milletler Cemiyetine rağmen İkinci Dünya Savaşının yaşanması idealizmin yerine realist düşüncenin ön plana çıkmasına neden olmuştur.

1.1.3.1. Realist Teori ve Güvenlik

Uluslararası ilişkiler disiplinine ilişkin teorik yaklaşımlardan birisi olan Realizm, kökenleri Thucydides'e kadar uzanan ve sonrasında Niccolo Machiavelli, Thomas Hobbes tarafından devam ettirilen bir fikir akımı olarak yüzyıllar boyu varlığını sürdürmüştür. Ancak realizmin uluslararası ilişkiler alanında ilk özgün kullanımı Hans J. Morgenthau ile başlamış ve ulusal çıkar, güç ve uluslararası politika gibi kavramlar uluslararası sistemi açıklamada kullanılan terimler haline gelmiştir.[40]

Realizmin en önde gelen isimlerinden biri Machiavelli'dir. 16. Yüzyılda İtalyan Rönesans'ı döneminde yaşamış olan Machiavelli'nin (1469–1527) düşüncelerinde, dönemin siyasal ve sosyal karmaşasının izleri açıkça görülebilir. Yaşadığı dönemde İtalyan şehir devletleri arasındaki birliğin dağılmaya başlaması Machiavelli'yi devlet merkezli ve güce odaklı bir düşünce etrafında bir çare aramaya itmiştir. Çok başarılı bir diplomat olmamasına rağmen farklı görevler üstlenmesi, dikkatli gözlemlerde bulunmasına olanak sağlamıştır.[41]

Ulusal güvenliğin en iyi nasıl sağlanabileceği konusundaki tarihsel tartışmada, Hobbes, Machiavelli, Rousseau gibi yazarlar devlet egemenliğinin etkileri üzerine oldukça karamsar bir tablo çizmeye eğilimlidir. Uluslararası sistem, devletlerin kendi güvenliğini komşuları pahasına sağlamaya çalıştığı oldukça sert bir alan olarak

[38] Şeref Çetinkaya, ***a.g.m.***, s.245.
[39] Sait Yılmaz, ***a.g.e.***, s.7.
[40] Faruk Sönmezoğlu, ***Uluslararası İlişkiler Sözlüğü***, Der Yayınları, İstanbul,2000, s.585.
[41] Fikret Birdişli, "Ulusal Güvenlik Kavramının Tarihsel ve Düşünsel Temelleri", http://sbe.erciyes.edu.tr/dergi/2011-2/8-%20_149-169.%20syf._.pdf, (Erişim tarihi: 09.02.2014).

değerlendirilmiş ve devletlerarası ilişkiler, devletlerin sürekli olarak birbirinden faydalanmaya çalıştığı bir güç mücadelesi olarak görülmüştür. Bu görüşe göre, Kantçı anlamda bir kalıcı barışın sağlanması mümkün değildir. Devletlerin tek yapabileceği, devletlerden birinin tam bir hegemonya elde etmesini önlemek için, diğerlerinin gücünü dengelemeye çalışmaktır. Bu, İkinci Dünya Savaşı sonunda realist (veya Klasik Realist) düşünce ekolünü geliştiren Edward H. Carr ve Hans Morgenthau gibi yazarlarca paylaşılan bir görüştür.[42]

Realist görüşe göre, güvenliğin temelinde güç olduğu değerlendirilmiş ve dolayısıyla da güvenliğin güç ile sağlanılacağına inanılmıştır. Realist görüşe göre anahtar rol güçtedir. Güçlü bir ülke kendi güvenliği için gerekli önlemleri alarak tehditlere karşı caydırıcı bir rol oynayabilecek ve herhangi bir tehdit veya saldırı durumunda, kendini muhafaza edebilecektir.

Uluslararası politika alanında özellikle 1940'dan sonra 1970'lere kadarki çalışmaların ağırlık noktasını oluşturan klasik realist yaklaşımda güç kavramı ve bu bağlamda ulusal güç ve insan unsuru kritik bir öneme sahip olmuştur. Siyasal gerçeklik adı verilen realist paradigma da gerek uluslararası çatışmaların sonucunun belirlenmesinde gerekse diğer devletlerin davranışlarını etkileme konusunda devletlerin sahip oldukları kapasiteler büyük bir önem taşımaktadır. Realist yaklaşımı benimseyen yazarlar her ne kadar devletin kapasitesi ile askeri gücünü özdeşleştirseler de genelde ulusal gücün öğelerinin askeri olmayan unsurlarını da kapsadığını kabul etmektedirler.[43] Bunun sebepleri arasında milli gücün, askeri güce göre daha kapsamlı olması yer almaktadır. Askeri güç, milli gücü oluşturan unsurlar arasında yer almaktadır.

Realizm, temel olarak uluslararası ilişkileri; aktörlerin devletlerden ibaret olduğu, devletlerin rasyonel davranarak çıkarlarını maksimize edecek politikalar izledikleri, bu ilişkilerin de güçler arasında bir hiyerarşik yapılanmanın söz konusu olduğu bir güç dengesi içinde gerçekleştiği varsayımına dayanmaktadır. Realizme göre dünyanın ana aktörleri ulus-devletlerdir ve onların egemenliğine meydan okuyacak belirli kolektif yollar dışında, bir güç yoktur.[44] Realizmin güvensizliğe atfen tasarladığı güvenlik anlayışının merkezinde, "insan doğasının kötü olduğu" ön kabulü ve uluslararası politikayı açıklamada kullanılan "anarşi" metaforu

[42] John Baylis, "Uluslararası İlişkilerde Güvenlik Kavramı", ***Uluslararası İlişkiler Dergisi***, 2008, Cilt: 5, Sayı: 18, 69-85, s.71-72.
[43] Tayyar Arı, ***Uluslararası ilişkiler Teorileri***, Alfa Yayınları, İstanbul, 2006, s.163.
[44] Sait Yılmaz, ***a.g.e.***, s.9.

bulunmaktadır.[45] Buna göre uluslararası ortamda anarşi mevcuttur. Bu anarşi ortamında devletler sahip oldukları güçle doğru orantılı olarak çıkarlarını koruyup maksimize edebilmektedirler. Realizme göre, uluslararası alanda çıkarlarını korumak ve güvende olabilmek için devletlerin güçlü olması gerekmektedir.

Realist teorisyenlerin neredeyse hepsi, devletlerin gerekli ulusal güce sahip olabilmeleri için sürekli askeri hazırlık içinde bulunmalarının zorunluluğuna dikkat çekmektedir. Realist kurama göre anarşi ve güvensizliğin süreklilik kazandığı bir uluslararası ortamda güvende olmanın tek yolu, güç ve kapasite artırımına gitmektir.[46] Realistlere göre insanlar gibi devletler de bencildir. Realistler için uluslararası ilişkilerin temelinde kendi ulusal çıkarlarını maksimize etmeye çalışan devletler arasındaki güç mücadelesi yatmaktadır.[47] Bu mücadele sonucu gücünü devam ettirebilen devletler güvenliklerini sağlayabilecektir. Bu nedenle bütün devletler güvende olabilmek adına güçlerini korumanın yollarını aramaktadır.

Uluslararası ilişkiler teorileri içerisinde belki de en çok rağbet göreni olan realizme yönelik eleştiriler de bulunmaktadır. Devlet dışındaki tüm aktörleri bir bakıma yok sayması bu teorinin kısıtlayıcı yanını ortaya koymaktadır. Ayrıca tüm ilişkileri güç ekseni etrafında değerlendirerek politika üretiminin sadece çıkar esasına dayandığı varsayımı da uluslararası ilişkilerin tek bir ölçüt üzerinden gerçekleştiğini düşünmekle eş anlamlı olacaktır. Bu da sağlıklı sonuçlar elde etmeye engel teşkil edecektir.[48] Çıkarların politika üretmekte büyük bir ağılığının olduğu kabul görmekle beraber uygulanan politikaları ve ilişkilerin çerçevesini tek bir sebebe indirgemek hatalara sebebiyet verebileceği değerlendirilmektedir. İlişkilerin çerçevesine çok boyutlu olarak bakılmasının daha faydalı olabileceği öngörülmektedir.

Sonuç olarak realizm ile ilgili görüşleri kısaca özetlemek gerekirse, idealist düşünce ve bunun sonucu olarak hayata geçen kurumların İkinci Dünya Savaşı'nın çıkmasını engelleyememesi realizmi öne çıkartmış, savaştan sonra yeni dünya düzeninde realizmin etkisi hızla yayılmıştır. Realizm uluslararası sistemi anarşik olarak tanımlamış ve uluslararası sistemde devleti ana aktör olarak kabul etmiştir. Güvenlik, savunma ve ulusal çıkarlar öncelikli gündem konularını oluşturmuştur. Güç üzerinde duran realistler uluslararası sistemi de güç mücadelesi olarak

[45] Atilla Sandıklı ve Bilgehan Emeklier, ***a.g.m.***, s.6.
[46] Atilla Sandıklı ve Bilgehan Emeklier, ***a.g.m.***, s.6-7.
[47] Sait Yılmaz, ***a.g.e.***, s.9.
[48] Şeref Çetinkaya, ***a.g.m.***, s.248.

tanımlamışlardır. Devlet dışındaki aktörleri ise ön plana almamışlardır.[49] Kısaca güç mücadelesinde önde olan devletler uluslararası sistemde söz hakkına sahip olarak güvenliğin kapsamını istedikleri şekilde belirleme hakkına sahip olmaktadır.

1.1.3.2. Neorealist Teori ve Güvenlik

1970'lerden itibaren uluslararası alanda yeni aktörler ve yeni problemlerin ortaya çıkması, mevcut teorilerin yeniden düşünülmesini gerektirmiştir. Bu düşünceler sonucu; ''küreselleşme (globalizm)'', ''çoğulculuk (pluralizm)'', ''yapısalcılık (structuralizm)'' ve de ''neo-realizm'' gibi realizmin dayandığı varsayımlara karşı olan muhtelif yaklaşımlar ve paradigmalar ortaya çıkmıştır.[50]

Uluslararası ilişkiler alanında önde gelen teorilerden biri olan neorealizm, 1970'li yılların sonuna doğru ortaya çıkmıştır. Realizmin sorgulanmaya ve eleştirilmeye başlanması, neorealizmin doğmasına neden olmuştur. Neorealizmin en ünlü temsilcisi Kenneth N. Waltz'tır. Kendisi de bir realist olan Waltz, 1979'da basılan ''Theory of International Politics'' adlı çalışmasında ilginç fikirler ortaya koymakta ve o güne kadar bir sonuç olarak değerlendirilen ve anarşik bir ortam olarak görülen uluslararası yapının devletlerin davranışlarını sınırladığını söylemekte; ayrıca güç kavramına yeni anlamlar yüklemektedir.[51] O dönem içerisinde değerlendirildiğinde oldukça radikal bir bakış açısıdır. Ancak o dönemde ortaya çıkan uluslararası yapılar göz ardı edilmemelidir. Kısaca güçlü olan devlet her istediğini yapamamakta uluslararası yapı bunu kısıtlamaktadır.

Neorealizm ağırlıklı olarak uluslararası sistemin anarşik yapısı üzerinde durmaktadır. Neorealizm açısından güç, realizmde olduğu gibi önemlidir. Ancak gücü bir amaç olarak değil, araç olarak görmektedirler. Ama yine de devletin temel amacı güvenliği sağlamaktır. Farklı olan, bir devletin güvenliğini sağlarken artık sadece diğer devletleri değil, öteki uluslararası aktörleri de dikkate alması gerekliliğidir. Devletler için önemli olan kendi çıkarlarıdır. Uluslararası sistem anarşik olduğu için de devletler genel bir güvenlik oluşumu yönünde faaliyet gösteremezler.

---

[49] Cihan Günyel, ***Avrupa'nın Güvenlik ve Savunma Politikalarının Oluşum ve Gelişim Süreci***, Sosyal Bilimler Enstitüsü, Kadir Has Üniversitesi, İstanbul, 2011, s.19.
[50] Sait Yılmaz, "Güçsüz Güç", ***Stratejik Araştırmalar Enstitüsü Güvenlik Stratejileri Dergisi***, 2007, Yıl:3, Sayı:5,67-104, s.73.
[51] Tayyar Arı, ***a.g.e.***, s.187.

Başka bir ifade ile devletler bir uluslararası güvenlik sistemi kurmak isteseler bile, sistem anarşik olduğundan bunu yapamazlar.[52]

Uluslararası yapıda egemen olan anarşi devletlerde güvensizliğe yol açmaktadır. Savaş ve çatışma kavramları ise güvenlik ikilemi çerçevesinde değerlendirilmektedir. Güvenlik ikilemi kavramı, bir devletin kendi güvenliğini sağlamaya çalışırken aynı zamanda diğer devletlerin güvenliklerini azaltma yönünde bir etki yapmaktır. Yani bir devletin başka bir devletten tehdit algılayıp silahlanması durumunda buna karşın tehdit algılanan devletin de aynı şekilde cevap vermesini ifade etmektedir. Dolayısıyla neorealistler açısından savaşlar devletlerin bu ikilemi sonucunda meydana gelmektedir.[53]

Neorealizm, ilgi alanını daha çok politik ve askeri ilişkiler ile sınırlayan realizme karşı ekonomik boyutu da ele almıştır. Neorealistlere göre; ekonomik ilişkiler ve süreçler, güç ve siyaset açısından önemli etkiler yapabilmektedir.[54] Neorealzim, realizmden farklı olarak ekonomik gücün uluslararası ilişkilerde önemi üzerinde durmuştur. Ekonomik gücün de askeri güç gibi uluslar arası arenada etkilere sahip olduğunu öngörmektedir.

Tarih içindeki savaşlar, barışlar, anlaşmalar ve ittifaklar neorealist bir perspektiften incelendiği zaman, en önemli amacın devletin bekası olduğu görülmektedir. Bu bakış açısına göre devletler birbirlerini potansiyel tehdit olarak görmektedirler. Bu sebepten güvenliklerini düşünmek zorundadırlar. Çıkar çatışması olduğundan işbirliğine yanaşmamaktadırlar. Ancak çıkarlar doğrultusunda kısa süreli kolektif savunma mümkün olmaktadır. Devletler güvenliklerini sağlamak maksadıyla güce başvurmaktadırlar. Neorealizme göre devletler güçlerini, güvenliklerini sağlayana kadar maksimize etmelidirler. Bu bakış açısına göre güç amaç değil araç olmalıdır. Bu noktada neorealistler klasik realistlerden ayrılmaktadırlar. Çünkü klasik realistler gücü amaç olarak görmekte ve sürekli güçlenme isteği duymaktadırlar. Güç ve güvenlik arasında doğru orantılı bir ilişki bulunmaktadır.[55]

---

[52] Beril Dedeoğlu, ***a.g.e.***, s.45-46.
[53] Arif Behiç Özcan, ‘’Uluslararası Güvenlik Sorunları ve ABD’nin Güvenlik Stratejileri’’, Selçuk Üniversitesi, Sosyal Bilimler Enstitüsü, Uluslar arası İlişkiler Ana Bilim Dalı, Konya, 2004, ***Yayımlanmamış Yüksek Lisans Tezi***, s.21.
[54] Sait Yılmaz, ***a.g.e.***, s.12.
[55] Şeref Çetinkaya, ***a.g.m.***, s.248.

1.1.3.3. Liberal Teori ve Güvenlik

Liberalizm, Batı Avrupa'da ortaçağ düzeninin dağılmasıyla doğmuştur. Ortaçağ düzeni, Roma İmparatorluğunun yıkılışıyla oluşan otoritelerin kendi alanlarında hâkim olduğu, kilisece tanımlanmış uhrevi ve hemen hemen dünyevi alanlarda, nüfuzunu rakipsizce gerçekleştirdiği ve kilisenin kutsadığı imparatorun diğer otoritelerce tanındığı bir düzendir. Bu düzen, papa, imparator ve yerel güçlerin karşılıklı bağımlılığına dayanmaktadır. Kilise, diğerlerinin otorite ve iktidarlarının meşruiyet kaynağı olarak dinsel ilkeler sunan baskın güçtür. Dinsel meşruiyet bu dönem iktidar söylemlerinin temelidir.[56]

Liberalizm, bir ideoloji olarak özellikle İngiltere ve ABD'de 18. ve 19. yüzyıl siyasal ve ekonomik düşünce tarihinde etkili olmuştur. Klasik liberal düşünce, eşitlik, rasyonellik, özgürlük ve mülkiyet kavramları üzerine inşa edilmiştir. Liberalizm akımının öncüsü John Locke (1632–1704)'tur. Daha sonra da David Hume, Adam Smith, Montesquieu, Voltaire ve Kant bu akımın gelişmesinde önemli rol oynamışlardır.[57]

Liberalizmin, uluslararası politikayı açıklamaya yönelik bir uluslararası ilişkiler teorisi olarak görülmesi Birinci Dünya Savaşı sonrasında, uluslararası barış ve güvenliğin egemen kılınması ve çatışmaların önlenmesine ilişkin yürütülen çalışmaların bir sonucu olarak gündeme gelmiştir. Uluslararası liberal teori olarak da ifade edilebilecek olan XIX. yüzyıl liberalizminin temel özelliği, klasik liberal teorinin insan unsuru ve bireye yaklaşımını esas alarak, uluslararası ilişkilerde barış ve işbirliğinin analiz edilmesidir. Bu bağlamda klasik liberal teoride birey temel analiz birimi olarak anılırken, liberal uluslararası ilişkiler teorisinde analiz birimi sadece birey değildir, analiz düzeyi olarak plüralist bir yaklaşım benimsenerek, uluslararası ilişkiler ve devletin dış politikasında, birey, ulusal baskı grupları, devlet, uluslararası örgütler ve ulus aşırı örgütlenmeler (yani aktör düzeyinde) analiz edilmektedir.[58]

Liberaller, uluslararası ilişkilerin aktörleri arasında ulus-devletin yanında çokuluslu şirketler ve ulus aşan aktörleri (NGO'lar ve uluslararası organizasyonlar) de aktör listesine dâhil etmektedir. Bu kapsamda, ulus-devlet; ulusal çıkar peşinde

[56] Halis Çetin, "Liberalizmin Tarihsel Kökenleri", ***Cumhuriyet Üniversitesi İktisadi ve İdari Bilimler Dergisi,*** Cilt:3, Sayı:1, 79–96, s.80.
[57] Şeref Çetinkaya, ***a.g.m.***, s.253.
[58] Tayyar Arı, ***a.g.e.***, s.367.

koşan kendi içerisinde bir bütün veya birleşmiş bir aktör değil ona yön veren kendi çıkarları peşindeki bürokratik organizasyonların toplamıdır.[59]

Liberallere göre uluslararası ilişkiler sadece güç dengesine değil; karşılıklı etkileşim içerisindeki uluslararası düzeydeki yönetişim düzenlemeleri, uzlaşılmış hukuk kuralları, kabul edilmiş normlar, uluslararası rejimler ve kurumsal kurallar içerisinde yürütülmektedir. Liberallere göre devletlerin egemenliği sadece teorik ve yasal boyuttadır. Pratikte devletler kararların alınmasında tüm aktörler ile görüşmelerde bulunmalıdır. Devletler arasında karşılıklı bağımlılık uluslararası ilişkilerin önemli bir özelliğidir.[60] Devletler karar alırken diğer devletlerle etkileşim halinde bulunmaktadır. Böylece devletlerin belirli kurallar çerçevesinde hareket ettikleri varsayılmaktadır.

Liberallere göre ilişkiler savaşla değil işbirliği ile dengelenmelidir. Liberaller için de askeri güç önemlidir fakat realistler kadar ön planda değildir. Uluslararası ilişkilerin tek gündeminin güvenlik olmadığını, 20. Yüzyıldan itibaren gündemin çeşitlendiğini, refah, çevre ve modernleşme gibi konularının da devletlerin dış politikasını en az güvenlik kadar etkilediğini savunmaktadırlar. Devletlerin dış politika unsurunun sadece güvenlik faktörü olmadığını, para, göç, sağlık, çevre, ticaret gibi konularında güvenlik kadar önemli hale geldiğini ileri sürmektedirler.[61] Devletlerin dış politikasına etki eden unsur sadece güvenlik hususu değildir. Bunun yanında ekonomi, sağlık, göç gibi hususlarda devletlerin uluslararası ilişkilerini etkilemektedir.

Liberalizm uzun bir sürecin sonucu olarak günümüze siyasal, ekonomik ve uluslararası ilişkiler disiplininde yer edinerek gelmiştir. İnsanlık tarihindeki önemli siyasal, ekonomik, sosyal, dinsel gelişmeler liberalizmin doğmasına ve gelişmesine yardımcı olmuştur. Merkezine bireyi oturtan liberalizm, kişisel hak ve özgürlüklerden yola çıkarak toplumsal ve toplumlararası hak ve özgürlükleri de içine alan evrensel bir hak ve özgürlükler haline dönüşmüştür. Temelinde demokrasi, hak, özgürlük, eşitlik kavramlarını yerleştirmiştir. Uluslararası ilişkiler disiplininde de önemli bir ekol olmuş ve günümüzde bu konumunu devam ettirmektedir.[62]

[59] Sait Yılmaz, ***a.g.e.***, s.10.
[60] Sait Yılmaz, ***a.g.e.***, s.10-11.
[61] Tayyar Arı, ***a.g.e.***, s.368.
[62] Cihan Günyel, ***a.g.t.***, s.40.

1.1.3.4. Marksist Teori ve Güvenlik

Marksizm'in kurucusu olan Karl Marx (1818-1883) idealist bir düşünür olan Hegel'in diyalektik tarih felsefesinden yoğun bir şekilde etkilenmiştir. Hegel felsefesi sağ'dan sol'a geniş bir siyasi yelpazeyi etkilemişken Marx kendini sol kanat genç Hegelcilerden olarak kabul etmiş ve Hegel felsefesini kullanarak muhafazakâr Prusya hükümetini ve dini eleştirmiştir. Ağırlaşan siyasi şartlar nedeniyle Paris'e taşınan Marx, orada hümanist ilahiyat görüşleriyle ünlü Ludwing Feuerbach'dan (1804-1872) etkilenerek kendi materyalist politik ve ekonomik düşüncesini oluşturmaya başlamıştır. Bu arada daha sonra Marx'ın fikirlerini geliştirecek ve yaygınlaştıracak olan Engels'le (1820-1895) tanışmıştır. Bu nedenle Marksist düşünceyi incelerken genelde Marx ve Engels birçok yerde birlikte anılmaktadır.[63]

Marksist teori yapısalcılık veya dünya-sistemi teorisi olarak da tanımlanmaktadır. Realizm ve liberalizme göre daha az etkili ve yaygın olan marksist teorinin temelinde uluslararası ilişkilerin kapitalist ekonomik düzene sahip bir dünyada oluştuğu düşüncesi yatmaktadır. Bu ekonomik dünyanın en önemli aktörleri ise devletler değil sınıflardır ve bütün diğer aktörlerin davranışları ancak sınıf mücadelesi içerisinde açıklanabilir. Devletler, çokuluslu şirketler ve hatta uluslar arası organizasyonlar dünya ekonomik sisteminin hâkim sınıfının çıkarlarını temsil etmektedir.[64]

Marksist teori, devletlerin, ekonomik sınıfların, toplumların ve dolaylı da olsa bireylerin güvenlik sorunsallarını, uluslararası kapitalist sistemin yapısal krizleri çerçevesinde eleştirerek incelemiştir. Dolayısıyla sistem düzeyindeki bütüncül ve yapısalcı yaklaşımları, güvenliğin salt devlet merkezli ve siyasi-askeri açıdan ele alınmasının karşısında alternatif bir bakış açısının gelişimine katkı sağlamıştır.[65]

1.1.3.5. Kopenhag Ekolü Teorisi ve Güvenlik

Sovyetler Birliği'nin parçalanması, etnik ve ülke içi karışıklıklar gibi sosyo-politik olayların etkilemesiyle beraber güvenlik çalışmalarının içinde neorealistlerin güvenlik kavramsallaştırmasının, tehdit içerikleri ve insan yaşamının devamlılığı konusunda yeterince geniş olup olmadığıyla ilgili tartışmalar ortaya çıkmıştır.

---

[63] Fikret Birdişli, ***a.g.m.***, s.163.
[64] Sait Yılmaz, ***a.g.e.***, s.11.
[65] Atilla Sandıklı ve Bilgehan Emeklier, ***a.g.m.***, s.25.

Kopehnag Barış Araştırmaları Enstitüsü(Copenhagen Peace Research Institute), kısa adıyla CORPI, 1980'lerin sonlarında çalışmalarına başlamış, günümüzde faaliyetlerini Danimarka Enformasyon Teknoloji ve Araştırmaları Bakanlığıyla iş birliği içinde sürdüren bir araştırma merkezidir. Kopenhag Güvenlik Araştırmaları Okulu veya Kopenhag Okulu diye adlandırılan oluşumsa, enstitü kapsamındaki araştırma projelerinden biri olan Avrupa Güvenliği kapsamında çalışmalarını gerçekleştiren, Barry Buzan, Ole Waever, Morten Kelstrup ve Pierre Lemaitre'nin öncülüğünü yaptığı bilim adamlarının güvenlik konusunda gerçekleştirdikleri yeni teorik açılımlarıyla dikkat çeken çalışmaları sonucu ortaya çıkmış bir ekoldür.[66] Kopenhag ekolü teorisi, diğer uluslar arası ilişkiler teorileri ile karşılaştırıldığında ortaya çıkış şeklinin daha farklı olduğu görülmektedir. Kopenhag Ekolü teorisi bir araştırma projesi olarak ortaya çıkmıştır.

Kopenhag Okulu'nun önde gelen teorisyenlerinden Buzan 1983 yılında yayınladığı "Halklar, Devletler ve Korku" isimli kitabında klasik askeri odaklı güvenlik anlayışına çeşitli eleştiriler yöneltmiştir. 1990'larda da Ole Waever ve Jaap de Wilde Soğuk Savaş sonrası değişen koşullarda güvenliğin temel birimlerini ve değerlerini çeşitlendiren çoğulcu ve yapısalcı bir yaklaşım ortaya koymuşlardır.[67] Soğuk Savaş'ın sonlarına doğru birçok değerli araştırmacı klasik askeri güvenlik anlayışına yönelik eleştirilerde bulunmuştur.

Kopenhag Ekolü, erken dönem çalışmalarında dar veya geniş güvenlik kapsamı konusundaki tartışmalarla ilgili olarak artan memnuniyetsizliğini ortaya koymuştur. Daha sonraki çalışmalarında ise Kopenhag Ekolü, güvenlik ortamını önceden belirlenmiş olarak değerlendirdiklerinden ötürü neorealistlerin ve genişlemeden yana olanların güvenlik konusundaki tavırlarını çözüm bulamayan tarzda nitelendirmiştir. Bu şartlar altında Kopenhag Ekolü güvenliğe yönelik sistematik bir çalışma yapmayı uygun görmüş ve güvenlik konusunu, daha sosyal ve daha kapsamlı olabilecek şekilde genişletmeye çalışmıştır.[68]

Kopenhag Okulu'nun güvenlik çalışmalarına getirdiği en önemli katkılardan birisi insan topluluklarının güvenliğinin etkilendiği beş ana sektörü güvenlikleştirme

[66] Çiğdem Şahin, "Sözcelerin Gücü Adına, Güç Bush'ta Artık…", ***Uluslararası Güvenlik Sorunları,*** ASAM Yayınları, Ankara, 2004, 82-101, s.85.
[67] Övgü Kalkan Küçüksolak, "Güvenlik Kavramının Realizm, Neorealizm Ve Kopenhang Okulu Çerçevesinde Tartışılması", ***Turan Stratejik Araştırmalar Merkezi Dergisi***, 2012, Cilt: 4, Sayı:14, 202-208, s.204.
[68] Şeref Çetinkaya, ***a.g.m.***, s.254-255.

teorisine uyarlamasıdır. Kopenhag Okulu'nun burada öne çıkardığı husus askeri tehditlerin toplumlar için tek güvensizlik kaynağı olmadığıdır. Diğer sektörlerdeki güvensizlikler de bir tehdit kaynağı olarak hem kendi başına hem de askeri sektöre taşınarak bir güvensizlik kaynağı oluşturmaktadır. Güvenliği sektör temelinde incelemenin önemli bir katkısı, sektörler arasındaki özel ilişki tiplerinin tanımlanarak birbirinden etkileşimini de ortaya koymaktır. Bu sektörler, askeri güvenlik, siyasi güvenlik, ekonomik güvenlik, toplumsal güvenlik ve çevresel güvenliktir. Bu sektörler, askeri güvenlik, kuvvet temelli baskı ilişkileri; ekonomik sektör, ticaret, üretim ve finansa dair ilişkileri; siyasi sektör, iktidar, yönetim statüsü ve tanınmaya dair ilişkileri; toplumsal sektör kimlik ile ilgili ilişkileri ve çevresel sektör ise, insan faaliyetleri ve gezegendeki çevre konularındaki ilişkileri kapsamaktadır.[69]

1.2. ULUSAL GÜVENLİK ALGILAMASI

1.2.1.Kavramsal Olarak Ulusal Güvenlik

Birçok kavramda olduğu gibi ulusal güvenlik ile ilgili birçok tanım gerek kapsam, gerekse anlayış bakımından zamanla değişime uğramaktadır. Ulusal güvenlik anlayışı önceleri "savaş zamanı devletin güvenliğinin sağlanması maksadıyla barıştan itibaren askeri gücün hazırlanması ve bu gücün kullanılması ile ilgili bir strateji oluşturulması" şeklinde düşünülmüştü. Özellikle savunma alanındaki teknolojik gelişmelerin ve savaşın askeri gücün dışına çıkarak ulusal gücün tüm unsurlarını da içine alması sonucu, güvenlik kavramı da değişmiş, "ulusal güvenlik" kavramı bugünkü anlamına yakın bir çerçeveye oturmuştur.[70]

Spesifik bir anlama sahip olmayan, dolayısıyla kendisine atfedilen değerlere bağlı olarak anlam ifade eden ulusal güvenlik, farklı boyutlarda tanımlanabilen bir kavramdır. Örneğin, ulusal güvenlik kavramı sadece askeri boyuta indirgenerek ve olağan olmayan dönemlerde alınacak olan önlemleri de kapsayacak biçimde dar anlamda kullanılabilmektedir. Bu anlamıyla ulusal güvenlik, kısa ve özlü bir ifadeyle, bir ülkenin iç ve dış tehditlerden korunması biçiminde tanımlanabilir. Daha genel

[69] Nebi Miş, "Güvenlikleştirme Teorisi ve Siyasal Olanın Güvenlikleştirilmesi" http://www.aid.sakarya.edu.tr/uploads/Pdf_2011_6_14.pdf (Erişim Tarihi:15.01.2014).
[70] Sait Yılmaz, ***a.g.e.***, s.213.

anlamda, devlet düzenini korumak amacıyla alınan her türlü önlemin ulusal güvenlik kavramının içeriğini oluşturması şeklinde ve geniş olarak kavranılmasıdır.[71]

Ulusal güvenlik bir tanıma göre "Devletin anayasal düzeninin, ulusal varlığının ve bütünlüğünün uluslararası alanda siyasi, kültürel ve ekonomik dâhil bütün çıkarlarının ve ahdi hukukun her türlü dış ve iç tehditlere karşı korunması ve kollanmasıdır." [72] Ahdi hukuktan kasıt anlaşma ve antlaşmalarla gerçekleşen hukuku ifade etmektedir.

Ulusal güvenlik diğer bir tanıma göre ise "devlet denen soyut hukuki tüzel kişiliğe sahip varlığın, iç ve dış her türlü tehlikelerden korunmuş olarak varlığını hukuki, sosyal ve bağımsız olarak sürdürmesi" olarak da tanımlanmaktadır.[73] Ulusal güvenlik; kısaca belirtmek gerekirse, bir devletin ulusal çıkarlarının iç ve dış tehditlere karşı korunup kollanmasıdır. Güvenlik kavramı, devletin egemenlik alanı ve ulusun yüksek çıkarlarının bir başka rakip devlet tarafından müdahale edilmesi durumunda tehdit ve tehlikeye karşı gereken önleyici ve caydırıcı tedbirlerdir.[74] Bu haliyle ulusal güvenlik; ulusal çıkarlar, tehditler ve bu tehditlere karşı tedbir geliştirme kavramlarını içerir.[75] Ayrıca ulusal güvenlik kavramı, geleneksel olarak, korunması gereken değerler olan siyasal bağımsızlık ve toprak bütünlüğünü de içermektedir.[76] Bu açıklamalardan da anlaşılacağı üzere, ulusal güvenlik her ne kadar devletin içinde barınan tüm unsurların güvenliğini kapsasa da doğrudan devlete yönelik tehditlere karşı duyarlılığının, diğer tehditlere nazaran daha fazla olabilmektedir.[77] Doğrudan devlete yönelik tehdit olduğunda buna karşı gösterilecek reaksiyon diğer unsurlara yönelik olanlardan daha hızlı ve şiddetli olacaktır. Bunun nedeni tehdidin hedef olarak doğrudan devleti seçmesidir. Bu durumda da algılanan tehdidin derecesine göre gerekli tedbirler devlet tarafından alınacaktır.

Ulusal güvenlikte öne çıkan iki önemli kavram "ulusal çıkarlar" ve "tehditler"dir. Tehdit değerlendirmelerinin işlevi; belirlenecek tehdit/risklere karşı alınacak tedbirleri içeren ulusal güvenlik politikasının tespitine yön vermesidir. Her ülke, kendi

---

[71] Abdullah Torun, ***Ulusal Güvenlik ve Küreselleşme: Türkiye'nin Ulusal Güvenlik Politikasının Dönüşümünde Küreselleşmenin Rolü,*** Sosyal Bilimler Enstitüsü, Ankara Üniversitesi, Ankara, 2012, s.15.

[72] Harp Akademileri Yayınları, ***Milli Güvenlik Siyaseti ve Stratejisi***, Harp Akademileri Basımevi, İstanbul, 1996, s.25.

[73] Ömer Urhal, ***Küreselleşen Dünyada Güvenlik***, Adalet Yayınevi, Ankara, 2009, ss.67-68.

[74] Mesut Hakkı Caşın, ***Çağdaş Dünyada Uluslararası Güvenlik Stratejileri ve Silahsızlanma***, SSM Yayınları, Ankara, 1995, s.15.

[75] Sait Yılmaz, ***a.g.e.,*** *s.*214.

[76] David A. Baldwin, "Güvenlik Kavramı", ***a.g.m.***, s.15.

[77] Fatih Beren**,** ***a.g.e.***, s.38.

tehdit/risk algılamalarına göre bir ulusal güvenlik politikası belirlemektedir. Bu sebeple ülkeler, kendi tehdit/risk algılamaları çerçevesinde ulusal güvenlik politikalarını tespit etmeye yönelik ulusal güvenlik sistemleri oluşturmuşlardır.[78] Ulusal güvenliğe yönelik tehditlerin genel amacı, devleti zayıflatmak, işleyemez duruma getirmek, eğer mümkünse topraklarını paylaşmak ve ortadan kaldırmaktır.[79]

Ulusal çıkar kavramı ulusal güvenlikten daha önce kullanılmaya başlanmıştır. Ulusal güvenlikle ilgili dört temel ulusal çıkarın önem derecesi ise şu şekildedir:[80]

- "Beka" önem derecesi (Genellikle ülkenin toprak bütünlüğü ve ulusal birliği bu kategori içindedir ve bu konularda ülke savaşı göze almıştır).
- "Hayati" önem derecesi (Daha çok ileri düzeydeki savunma, bölgesel güvenlik ve ekonomik çıkarları kapsamakta ve savaş kesin olmamakla beraber savaş riski taşıyan çıkarları göstermektedir. Savaşı ileri bir tarihte muhtemel kılan güvenliğe yönelik tehditler de bu kapsamdaki çıkarlara işaret edebilir).
- "Çok Önemli" önem derecesi (Genellikle güç kullanımını gerektirmeyen ancak, hesaplanmış politikalar ve eylemler ile elde edilmeye çalışılan siyasi ve ekonomik düzeydeki çıkarları kapsamaktadır).
- "Önemli" önem derecesi (Genellikle tarihi ve kültürel değerler niteliğindeki ulusal çıkarların yer aldığı, insani ve kültürel politikaların uygulandığı, uzun vadeli çıkarlar olarak değerlendirilmektedir).

"Ulusal Güvenlik" kavramı İkinci Dünya Savaşı'nın ardından ABD Başkanı Herry S. Truman döneminde kongre tarafından çıkartılan "National Security Act" (Ulusal Güvenlik Yasası, 18 Ekim 1947) ile üne kavuşmuştur. Salt bir kavramdan çok politikaya atıf yapmaktadır. Bu tarihten sonra ulusal güvenlik kavramıyla birlikte ulusal güvenlik politikaları belirlenmeye başlanmıştır.[81] Ulusal güvenlik kavramının ilk kez dile getirildiği "Ulusal Güvenlik Yasası" ise başlangıçta her ne kadar Amerikan ulusal çıkarlarını korumak ve bu konuda kurumsal koordinasyonu sağlamak amacını taşımışsa da, Soğuk Savaş yıllarında "ulusal güvenlik" adeta bir ideolojiye dönüşerek sadece A.B.D müttefiklerinin sınırlarını komünizm tehlikesine

[78] Sait Yılmaz, ***a.g.e.***, s.223.
[79] Sait Yılmaz, ***a.g.e.***, s.220.
[80] Harp Akademileri Yayınları, ***Milli Güvenlik Siyaseti ve Stratejisi***, Harp Akademileri Basımevi, İstanbul, 1996, s.50-52.
[81] Arnold, Wolfers, "National Security: As an Ambiguous Symbol", ***Political Science Quarterly***, Vol: 67, No: 4, 1952, 481-502, p.482.

karşı korumanın ötesine geçip Batı değerlerine karşı her türlü meydan okumayı bertaraf edebilecek biçimde yeniden tanımlanmıştır.[82]

Ulusal güvenlik, İkinci Dünya Savaşı'nın sona ermesinden itibaren, akademik, politik uluslararası politika ve dış politika tartışmalarında, önemle konu edilmektedir.[83] Soğuk Savaş boyunca güvenlik çalışmaları, çoğunlukla devletin askeri tarafıyla ilgilenen bilim adamlarının yaptıkları çalışmalardan ibaret olmuştur.[84] Ulus-ötesi hareketlerin sınırlı olduğu, insanların kendi kimliklerini daha çok doğup büyüdükleri yer ile tanımladıkları, başka coğrafyalarda olanların devletlerin güvenliğini tam olarak etkilemediği bu zaman diliminde, güvenliğin sağlanmasında daha çok 'kendi kendine yardım' prensibi esas alınmıştır. Buna göre, her devlet kendi güvenliğinden öncelikli olarak kendisi sorumludur. Burada önemli olan husus bir devletin kendi vatandaşlarını negatif dış etkilerden, gerek ekonomik gerekse de askeri, olabildiğince korumasıdır. [85] Bu anlamda bir devletin güvenliği daha çok askeri güvenlik anlamına gelmektedir ve daha çok fiziki güvenliğin sağlanmasını ifade etmektedir.

1945-1990 dönemindeki güvenlik literatüründe görülen durağanlık ve tekdüzeliğin Soğuk Savaş konjonktürünün statik yapısını yansıtmaktadır. İki kutuplu sistemdeki güvenlik çalışmaları, Soğuk Savaş yıllarının hâkim teorisi realizm ve neo-realizmin etkisi altında ortaya çıkmış ve şekillenmiştir.[86] Soğuk Savaş Dönemi güvenlik algılaması askeri, ekonomik, ideolojik ve siyasal temeller üzerine kurulmuştur. Bu noktadan hareketle özellikle askeri güvenliğin sağlanması noktasında her iki tarafta oluşturulan NATO ve Varşova Paktı güvenlik kaygılarıyla hareket etmiştir.[87] NATO ve Varşova Paktı bu her iki bloğun karşılıklı olarak güvenliklerini sağlayan ve karşı taraftan gelebilecek bir saldırıyı bertaraf etmek amacına yönelik savunma sistemleri olarak kurulmuşlardır.[88]

Tarihi akış içerisindeki reel politik akım, 20. yüzyılın çatışma odaklı ve devlet merkezli güvenlik anlayışını teorik ve pratik çerçevede inşa etmiştir. Ancak reel politik anlayışın oluşturduğu güvenlik paradigmasının gerek düşünsel gerekse de

---

[82] Fikret Birdişli, ***a.g.m.***, s.152.
[83] Sait Yılmaz, ***a.g.e.***, s.211.
[84] David A. Baldwin, "Güvenlik Kavramı", ***a.g.m.***, s.8.
[85] Tarık Oğuzlu, ***a.g.m.***, s.13.
[86] Atilla Sandıklı ve Bilgehan Emeklier, ***a.g.m.***, s.5.
[87] Cihan Günyel, ***Avrupa'nın Güvenlik ve Savunma Politikalarının Oluşum ve Gelişim Süreci***, Sosyal Bilimler Enstitüsü, Kadir Has Üniversitesi, İstanbul, 2011, s.3.
[88] Muhittin Demiray ve İsmail Hakkı İşcan, ***a.g.m.***, s.149.

eylemsel boyutta güvenliği tesis etmedeki yetersizliği, 20. yüzyılın "buhranlar ve bunalımlar yüzyılı" olarak yorumlanmasında büyük rol oynamıştır.[89]

Ulusal güvenlik kavramının gelişmesinde harp silah araç ve gereçlerindeki teknolojik gelişmeler önemli rol oynamıştır. Özellikle taraf ülkelerde kitlesel tahriplere yol açan silahlar; cephe stratejilerinin topyekûn savaş stratejilerine dönüşmesine ve savaşların devletlerin tüm ulusal güç unsurlarına yöneltilmesine neden olmuştur. Dolayısıyla topyekûn savaş stratejisi; "Topyekûn Güvenlik" veya günümüz deyimiyle "Ulusal Güvenlik" kavramını ortaya çıkarmıştır. Ulusal güvenlik kavramındaki gelişmeler, beraberinde politik, sosyal, ekonomik ve askeri güçler arasında yeni dengeler oluşturmuş ve boyutları genişleyerek devlet yönetimlerinde vazgeçilmez bir yere sahip olmuştur. Böylece ulusal güvenlik, sadece silahlı kuvvetleri ilgilendiren bir kavram olmaktan da çıkmış, daha geniş bir yelpazede ele alınmaya başlanmıştır.[90] Devletin nerdeyse bütün organlarını ilgilendiren bir kavram haline dönüşmüştür.

Soğuk Savaş sonrasında, uluslararası ve ulusal güvenlik tanımlarının değişen doğası hiç şüphesiz uluslararası ve ulusal tehditlere yönelik ilgilenme yöntemlerini de değiştirmiştir. Üstelik, tehdit anlayışı da askeri tehditlerin yanı sıra ekonomik, siyasal, ekolojik ve sosyal tehditleri de kapsadığı için, bir anlamda geleneksel ulusal ve uluslararası güvenlik anlayışını ve güvenlik yaklaşımlarını da en başından etkilemiştir.[91] Devlet düzeyinde tehdit kavramı "bir kişi, grup veya devlet tarafından bir ülkenin hayati öneme sahip ulusal değerlerine yönelik; ekonomik, siyasi, sosyal, kültürel, psikolojik ve askeri olarak; niyet edilen, planlanan veya uygulanan, her türlü davranış ve eylemlerin bütünüdür." şeklinde tanımlanabilir.[92]

Beril Dedeoğlu'na göre, her ne biçimdeki tehdide göre olursa olsun, her devlet, üç halkalı bir güvenlik sistemi kurmaktadır;[93]

1. En iç halka, aktörün kendi iç güvenlik sistemidir. İçten gelebilecek ya da içte oluşabilecek tehlikeleri kapsamaktadır. Bu en sıkı halkadır. En iç halka, belirli bir rejimin, düzenin, siyasal iktidarın, sosyo-ekonomik sistemin devamının sağlandığı halka olarak tanımlanır.

[89] Atilla Sandıklı ve Bilgehan Emeklier, ***a.g.m.***, s.4.
[90] Sait Yılmaz, ***a.g.e.***, s.213.
[91] İsmail Dindar, ***21.Yüzyılda Teknoloji ve İstihbarat Savaşları***, IQ Kültürsanat Yayıncılık, İstanbul, 2004, s.56.
[92] Sait Yılmaz, ***a.g.e.***, s.221.
[93] Beril Dedeoğlu, ***a.g.e.***, s.63.

2. İkinci halka, yakın çevre tehlike ve güvenlik halkasıdır. Ülke sınırlarına komşu ya da yakın alanlar ve devletler, bu halka içinde yer alırlar. Bir devletin çıkarlarını genişletmesi için en elverişli coğrafya, yakın coğrafyasıdır ve bu nedenle de ikinci sıklıktaki güvenlik tehdit halkası burada oluşur.

3. Üçüncü ve en dıştaki halka gevşek bir halkadır ve küresel tehdit alanını oluşturur. İkinci halkanın dışındaki bölgesel savaş ve çatışmalar, küresel savaşlar, küresel ekonomik krizler, doğal çevrenin kirlenmesi, önemli uluslar arası ticaret yollarının risk altına girmesi gibi birçok alt başlık bu halkaya dâhildir.

20'inci yüzyılın sonlarına doğru önemi artan ve kapsamı da gittikçe genişleyen güvenliği, artık devlet ve bünyesindeki organlarca sağlamanın yeterli olmayacağı öngörülmüştür. Bu bağlamda devlete yardımcı olmak amacıyla özel askeri şirket ve güvenlik kuruluşları yapılanmasına gidilmiştir.

21. yüzyıla uluslararası sistemde kırılma yaratan ve küresel güven(siz)lik için bir dönüm noktası teşkil eden 11 Eylül saldırılarıyla adım atılırken, yeni güvenlik anlayışı ve yaklaşımlarının nasıl olacağına ilişkin kuramsal tartışmaların niceliği ve niteliğinde önemli bir değişim yaşanmaktadır.[94] 21'nci Yüzyılda güvenlik ihtiyaçları, savunma planlamasına; kabiliyete dayalı sistemler yanında sivil unsurlardan/kabiliyetlerden yararlanılma yöntem ve şekillerinin de dâhil edilmesini gerekli kılmaktadır. Savunma planlaması kapsamında sivil imkân ve kaynaklara olan ihtiyaç genellikle;[95]

- Bilgi yönetimi, bilgi ve haberleşme güvenliği,
- Sivil ve askeri amaçlı uydu ve uzayı kullanma teknolojisi,
- Kritik silah, karşı silah ve korunma teknolojileri,
- Harekât alanı (istihbarat, komuta-kontrol, harekât, lojistik vb.) desteği alanlarında toplanmaktadır.

[94] Atilla Sandıklı ve Bilgehan Emeklier, ***a.g.m.***, s.4.
[95] Sait Yılmaz, "21'inci Yüzyılda Güvenlik Alanının Yeni Sivil Aktörleri: Özel Askeri Şirketler Ve Kontratçı Firmalar", ***Güvenlik Stratejileri Dergisi,*** 2007, Yıl: 3, Sayı: 6, 43-70, s.59.

Günümüzde güvenlik kavramı devlet bağlamından ayrı düşünülmemiş ancak kapsam olarak genişleyerek çok boyutlu bir hale gelmiştir. Demokratik toplum kavramının gittikçe önem kazanması kişi hak ve özgürlüklerini ön plana çıkarmıştır. Önem kazanan bu kavramlar güvenlik kavramının içinde de yer etmiş ve artık güvenlik, devlet güvenliğinin yanı sıra bireysel değerleri de önemseyen bir şekil almıştır.

1.2.2. Küreselleşme ve Ulusal Güvenlik

Bazı düşünürler küreselleşmeyi; ekonomik, siyasal, sosyal ve kültürel alanlarda ortak değerlerden bazılarının yerel ve ulusal sınırları aşarak dünya çapında yayılması olarak kabul etmektedirler. Küreselleşme; dünya toplumlarının ekonomik, kültürel ve siyasal düzeyde iç içe girmesi, sermayenin dünya üzerindeki dolaşımının artık tek tek ülkeler düzeyinde değil, küresel düzeyde gerçekleşmesi şeklinde açıklanmaktadır.[96] Küreselleşme çok boyutlu bir olgudur. Ticaret potansiyelinin genişlemesiyle beraber özel sermaye ve yatırımların küresel dünyada olağanüstü hızla yayılışından, teknoloji ve iletişim olanaklarının gelişmesi sayesinde tüm yaşam alanlarının karşılıklı bağımlı hale gelmesine kadar küreselleşme, tüm standartları ve sınırları zorlar görünmektedir.[97] Genel olarak bir süreci, durumu, sistemi ve dönemi açıklamaya yönelik olarak kullanılmaya başlanan küreselleşme kelimesi, ulusal sınırları aşan karşılıklı ekonomik, politik ve toplumsal bağlantıların yoğunlaşmasını tanımlayan bir kavramdır.[98]

Küreselleşmenin tam olarak tanımı yapılamamaktadır. Küreselleşmenin en önemli öğesinin değişim olduğu değerlendirilmektedir. Küreselleşme durağan bir olay ya da olgu şeklinde olmayıp, dinamik bir olgu veya olay şeklindeki bir süreç olarak ifade edilebilmektedir. Bu süreçte döngüye dâhil olan faktörler hem etkilenerek hem de etkileyerek, dinamik döngüsel bir küreselleşme oluşturmaktadırlar.

Küreselleşme, sanayi toplumundan bilgi toplumuna, işgücü ağırlıklı teknolojiden yüksek teknolojiye, ulusal ekonomiden dünya ekonomisine, merkezi

[96] Sait Yılmaz, ***a.g.e.***, s.33-36.
[97] Şamil Ünsal, "Milli Güvenliğimizin Milletlerarası ve Küresel Boyutları", ***Türk Dünyası Araştırmaları***, 2013, Sayı: 207, 1-12, s.10.
[98] Abdullah Torun, ***Ulusal Güvenlik ve Küreselleşme: Türkiye'nin Ulusal Güvenlik Politikasının Dönüşümünde Küreselleşmenin Rolü,*** Sosyal Bilimler Enstitüsü, Ankara Üniversitesi, Ankara, 2012, s.20-21.

yönetimden yerel yönetime, temsili demokrasiden katılımcı demokrasiye geçiş gibi sosyal, siyasal, ekonomik ve yönetim faaliyetleri açısından çeşitli değişim ve dönüşümler yaşanmasına neden olmaktadır.[99]

Geleneksel güvenlik konuları büyük ölçüde dış tehditlerle meşgul olmuşken, küreselleşmenin gelişmesiyle güvenlik konuları ve sorunları artan bir şekilde uluslar ötesi/ uluslar-altı ve çok boyutlu olmuştur.[100] Dünyanın küçülmesi, ulaşım ve iletişim imkânlarının artması ve zamanın hızlı akıyor olması, diğer bütün sorunları olduğu gibi güvenlik sorunlarını da küreselleştirmektedir. Çevre kirliliği, ekonomik istikrarsızlıklar, uluslararası göç, ulus-ötesi organize suç şebekeleri, ulus-ötesi terörist faaliyetler, kitle imha silahlarının çoğalması gibi güvenlik sorunları küreseldir ve herkesi etkilemektedir. Güvenlik sorunlarıyla yerel ölçekte mücadele etmek neredeyse imkânsız hale gelmektedir.[101] Dolayısıyla bir devlette olan bir olay kısa sürede diğer devletleri etkileyebilmektedir. Diğer bir deyişle ulusal güvenlik için uluslararası güvenlik gerekmektedir.

Küreselleşme fiziki olmayan güvenlik kavramını da ortaya çıkarmıştır. Güvenliğin geleneksel tanımlamaları toprağın ve egemenliğin korunması üzerine gelişmiştir. Ancak küreselleşme ile birlikte ülke ve egemenlik yerini bilgi ve teknolojik değerlere bırakmaya başlamıştır. Nye ve Owens "bilgi gücü" nün uluslararası ilişkilerde gücün dağılımında giderek daha fazla kullanılmaya başladığını ifade etmektedirler. Benzer şekilde, askeri alanda devrim ile ifade edilmeye çalışılan olgu artık daha yüksek ateş gücü değil bilgi teknolojileri ve silahların zekâsındaki gelişmelerdir. Küreselleşmiş bir dünyada bilgi ve teknoloji artık fiziki olmayan güvenliğin temel unsurlarıdır.[102]

Küreselleşme ile yeni istihbarat görevleri ulusal güvenlikten, ekonomi, uzay, siber-uzay, medya operasyonları ve yurt dışında diplomasinin örtülü faaliyetler ile desteklenmesine kadar geniş bir yelpazede değişmektedir.[103] Yeni stratejik güvenlik ortamında artık ulusal çıkarların askeri olmayan yollarla elde edilme ihtiyacı ve askeri seçeneklerin en son başvurulacak yöntemler olması; çeşitli

[99] Armağan KULOĞLU, "Türkiye'ye Müteveccih Tehditler ve Güvenlik Anlayışı", http://www.beykent.edu.tr/WebProjects/Uploads/T%FCrkiyeye%20m%FCteveccih%20tehditler%20ve%20g%FCvenlik%20anlay%FD%FE%FD.pdf, (Erişim tarihi: 11.01.2014).
[100] Ersel Aydınlı, ***a.g.m.***, s.39.
[101] Tarık Oğuzlu, ***a.g.m.***, s.17.
[102] Haşim Türker, ***a.g.e.***, s.25.
[103] Deborah G. BARGER, ***Toward A Revolution in Intelligence Affairs***, RAND National Security Research Division Yayınları, 2005, s.3.

istihbarat fonksiyonları ile desteklenen yeni ulusal güvenlik politikalarına olan gerekliliğin temel nedenidir.[104]

Küreselleşme ekonomik refahın arttırılması ve barışın sağlanmasında yeni olanakları insanlığa sunarken aynı zamanda sosyal dağılma sürecine, ekonomik krizlerin ulus-devlet sınırlarını aşmasına ve küresel ekonomik sıkıntılara dönüşmesine ve şiddet ve çatışmanın tohumlarının ekilmesine de neden olabilmektedir.[105] Soğuk Savaş'ın sona ermesinin ardından sosyo-kültürel, etnik, demografik ve düşük yoğunluklu çatışmalarda artış meydana gelmiştir. Küreselleşme ile oluşan yeni tehditler arasında bölgesel çatışmalar, örgütlü suçlar, terörizm, siber saldırılar, kitle imha silahlarının yayılması, küresel ısınma, din, mezhep ve ırk farklılıkları yer alacaktır.

21. yüzyıl teknolojinin getirdiği imkânlar vasıtası ile gözetleme, izleme ve dinleme çağı olacaktır. İstihbarat artık büyük ölçüde istihbarat servislerinin işi olmaktan çıktığından siyasi, ekonomik ve teknik istihbarat kabiliyetlerini artırmak için akademik çevreler, özel sektör ve araştırma kurumları ile daha çok işbirliği yapmak zorundadırlar.[106] Ülkeler, 21. Yüzyıldaki hedeflerine karşı başarılı olmak istiyorsa teknolojisinde esaslı bir başkalaşım geçirmek zorundadır.[107] Çağımızda modern istihbarat kurumlarında casus uydular, internet ve teknolojinin diğer imkânları yoğun bir şekilde kullanılmaktadır.[108]

21. Yüzyılda gerçekleşen küreselleşmenin bir sonucu olarak, propaganda ve psikolojik harekât devlet güvenliğini tehdit edebilecek etkili birer silah olacaklardır. 21'inci Yüzyılın ilk çeyreği, güvenlik alanında yüzyıl boyunca önemli değişimlere yol açacak parametrelerin gelişmekte olduğu bir dönemi işaret etmektedir. 21. Yüzyılın güvenlik ortamı, teknoloji ve iletişimin ulaştığı boyutlar, uluslararası ortamın ve ilişkilerin küreselleşme olgusu altında giderek iç içe geçmesi devletlerin birbirlerine karşı bakış açılarını etkilemiştir. Artık devletlerarası müdahaleler gizli ve örtülü bir nitelik taşımaktadır.[109]

---

[104] Sait Yılmaz, ***a.g.e.***, s.216.
[105] Şamil Ünsal, "Milli Güvenliğimizin Milletlerarası ve Küresel Boyutları", ***Türk Dünyası Araştırmaları***, 2013, Sayı: 207, 1-12, s.10.
[106] Sait Yılmaz, "ABD İstihbaratında Yaşanan Değişimler", ***TURAN Stratejik Araştırmalar Merkezi Dergisi***, 2012, Cilt: 4, Sayı: 13, 10-15, s.15.
[107] James Bamford, ***Sırlar Evreni: ABD Ulusal Güvenlik Dairesi'nin Dinleme ve İstihbarat Ağı***, Dost Kitabevi Yayınları, Ankara, 2009, s.702.
[108] Gültekin Avcı, ***İstihbarat Teknikleri: Aktörleri - Örgütleri ve Açmazları,*** Timaş Yayınları, İstanbul, 2004, s.24.
[109] Sait YILMAZ, ***a.g.e.***, s.301.

Örtülü operasyonlar devletlerin güvenlik algılamalarında önemli bir yer teşkil etmeye devam edecektir. Bunun dört temel sebebi vardır:[110]

1. Hala güvenlik ortamında pek çok düşman, tehdit ve çözülmeyi bekleyen sorun bulunmaktadır.
2. Kurulan örtülü bürokrasiler kendilerine yeni roller bularak var olmaya devam edeceklerdir.
3. Örtülü operasyonlar geçmişteki nedenlerden dolayı yönetimlere çekici bir seçenek oluşturmaya devam edecektir.
4. Soğuk Savaş sonrası güvenlik ortamı örtülü operasyonlar için yeni olanaklar ve hedefler sunmaktadır.

Geleneksel olarak güvenliğin sağlanması devletin temel fonksiyonlarından biri kabul edilirken, 20'nci Yüzyılın son çeyreğinde, geniş bir alana yayılan ve her geçen gün önem kazanan bu hizmetin sadece devlet organları ve görevlileri tarafından karşılanamayacağı anlaşılmıştır. Bu yeni durum karşısında, devlet görevlilerinin hizmetlerine yardımcı olacak bir biçimde özel askeri şirket ve güvenlik kuruluşlarının oluşturulması yaygınlık kazanmıştır.[111] İlk bakışta özel askeri şirketlerin ortaya çıkışı ve bu kadar çabuk çoğalması devletin devlet gücü ve egemenliğinin erozyona uğradığı gibi bir endişe ile karşılansa da, bu aynı zamanda devlet ve özel aktörlerin yönetişim, dış politik baskı ve kontrol teknolojilerinin birbirine eklendiği yeni bir güvenlik ağı ortaya çıkarmaktadır.[112]

Sonuç olarak, küreselleşmenin ulusal güvenliğe etkilerini aşağıdaki şekilde özetleyebiliriz;[113]

- Uluslararası ve ulusüstü yapıların gelişmesi ulusal egemenliğin kaybına yol açmakta, ulusal çıkarları sağlamaya yönelik güç politikalarının uygulanmasını güçleştirmektedir.
- Küresel ekonomik bütünleşme ekonominin ulusal denetimini ve hükümetlerin etkinliğini sınırlamakta, devleti güçsüzleştirmektedir.
- Ekonomi ulusal gücün lokomotifi olarak ortaya çıkarken uluslararası ekonomik aktörlerin (çokuluslu şirketler, IMF, Dünya Bankası vb.) ulusal

[110] John Jacob NUTTER, ***CIA'nın Örtülü Operasyonları***, Güncel Yayıncılık, İstanbul, 2005, s.497.
[111] Mehmet Ali Bal, ***Modern Devlet ve Güvenlik***, IQ Kültür Sanat ve Yayıncılık, İstanbul, 2003, s.206.
[112] Sait Yılmaz, "21'inci Yüzyılda Güvenlik Alanının…", ***a.g.m.***, s.58.
[113] Sait Yılmaz, ***a.g.e.***, s.54

ekonominin gelişmesindeki belirleyici rolü ekonomik güvenliği ulusal güvenliğin en önemli güvenlik parametresi haline getirmektedir.

- Ulus ötesi sosyal ve dini hareketler ulusal güvenliğe meydan okumaktadır.
- Küresel iletişim ve ulaşım devletin sınırlarının kontrolünü daha da güçleştirmiştir.
- Ulusal birlik; etnik ve dinsel çeşitlilik ve devletten özerklik taleplerinin tehdidi altındadır.
- Ulus-devletin yeniden yapılanmaya ve rollerini yeniden belirlemeye, ulusal güvenlik konusunda yeni yöntem ve vasıtalara ihtiyacı vardır.

İKİNCİ BÖLÜM
İSTİHBARAT KAVRAMI VE SİBER İSTİHBARAT UNSURLARI

2.1. İSTİHBARAT KAVRAMI

2.1.1. İstihbaratın Tarihi

İstihbarat, insanlar arasındaki ilk ilişkinin kurulmasından itibaren var olan bir kavram olduğunu söyleyebiliriz. İnsanların ilişkide olduğu ya da her ne sebeple olursa olsun iletişim kurmak istediği veya iletişimde bulunduğu kişiler hakkında bilgi edinerek (ekonomik, siyasi, insani vb.), önceden hazırlanılması işi de bir nevi istihbarat çalışmasıdır. Devletler için ise istihbarat "hayatta kalmak" anlamını taşır. Bu nedenle etkin bir istihbarat servisine sahip olmayan devletler için kör, sağır ve dilsizdir demek mümkündür.[114]

İlk istihbarat faaliyetlerinin av peşinde iz sürmeden hareket ederek düşman peşinde iz sürmek şeklinde gerçekleştiği belirtilmektedir. Tufandan sonra Hz. Nuh'un güvercin yollayarak suların çekilip çekilmediğini araştırması dahi bazı araştırmacılar tarafından modern anlamda istihbarat olarak yorumlanmaktadır.[115]

İstihbarat tarihi çok eski yıllara dayanmaktadır. M.Ö. 500 yıllarında yaşamış meşhur Çinli komutan ve filozof Sun Tzu' ya göre, düşmanın durumu hakkında sürekli bilgi almadıkça ve doğru zamanda vurmaya hazırlıklı olmadıkça, savaş yıllarca sürebilir. Bu bilgiyi elde etmenin tek yolu casusluk faaliyetleridir.[116]

Dünya tarihinde bir devre mührünü basan askeri liderlerden Napolyon Bonapart'ın "iyi bir mevkide konuşlandırılmış bir casusun temin edebildiği bilgi ve haberlerin, bazen birkaç tümen askerden daha fazla önem arz ettiği" şeklindeki sözleri istihbaratın ne derece önemli bir faaliyet ve hayat sahası olduğunu göstermektedir.[117]

---

[114] Yavuz Özalp, "Siber İstihbarat ve Güvenlik Politikaları", http://bilgikultur.org/wp-content/uploads/S%C4%B0BER-%C4%B0ST%C4%B0HBARAT-ve-G%C3%9CVENL%C4%B0K-POL%C4%B0T%C4%B0KALARI.pdf, (Erişim tarihi: 21.01.2014).
[115] Ümit Özdağ, ***İstihbarat Teorisi***, Kripto Yayınları, Ankara, 2010, s.41.
[116] Sun Tzu, ***Savaş Sanatı,*** Çev. Şule Kılıçarslan, Form Yayınları, İstanbul, 1992, s.113.
[117] Gültekin Avcı, ***a.g.e.***, s.12.

Birinci Dünya Savaşı'nda, istihbarat örgütleri savaşın gerektirdiği istihbaratı üretememişlerdir. Bunun en önemli nedeni o dönem istihbaratın sadece gazete, kitap ve ateşe raporlarına dayanıyor olmasıydı. Ayrıca savaş, o dönemin karakteristiğinden farklı olarak sadece askeri istihbarat ile başarı sağlanabilecek bir savaş değildi. Ekonomik, sosyal ve moral faktörlerin de etkileşimde bulunduğu topyekûn bir savaş oluşu, istihbarat örgütlerini çaresiz bırakmıştır.[118]

İkinci Dünya Savaşı sürecinde istihbarat alanında önemli değişimler yaşanmıştır. Teknolojinin gelişmesine paralel olarak, insan istihbaratının yanında sinyal istihbaratı, görüntü istihbaratı gibi konularda önemli gelişmeler kaydedilmiştir. İkinci Dünya Savaşı sırasındaki istihbaratın bu hızlı yükselişi, savaşta yer alan komutanlar tarafından da istihbaratın öneminin kabul edilmiş olmasıyla; istihbaratın savaşın kazanılmasındaki hayati derecedeki önemi anlaşılmıştır.

Uluslararası ilişkiler gibi istihbarat bilimi de yaklaşık yarım yüzyıldır bir akademik disiplin olarak kabul edilmiştir. İkinci Dünya Savaşı'nın sonuna kadar olan dönemde askeri liderler barış zamanında bir istihbarat teşkilatına ihtiyaç olduğunu düşünmüyorlardı. Onlar için istihbarat sadece savaşları kazanmak için gerekli idi. ABD'de 1947 yılında Truman'ın barışı korumak için de istihbarat gereklidir teorisi CIA kanunu ile hayata geçti.[119] Bu aşamadan sonra diğer devletler istihbarat örgütlerine çok büyük yatırımlar yaparak, menfaatlerini korumak ve geleceklerini garanti altına almak amacıyla çalışmışlardır. Bu çalışmalar neticesinde istihbaratta özellikle teknolojik gelişimlere paralel olarak büyük gelişmeler yaşanmıştır.

20. yüzyılda ulaşılan istihbarat teknolojileri sonucunda ortaya çıkan modern istihbaratı modern öncesi istihbarat ile kıyasladığımızda ortaya çıkan tablo şöyledir:

[118] Michael Herman, ***Intelligence Power in Peace and War,*** Cambridge University Press, Cambridge, 1999, s.21.
[119] Sait Yılmaz, ***a.g.e.***, s.79.

Tablo-3: Modern Öncesi İstihbarat/Modern İstihbarat Karşılaştırma Tablosu[120]

	Modern Öncesi İstihbarat	**Modern İstihbarat**
Bilgi Kaynağı	Tamamen insani istihbarat	-Bütün yeni istihbarat türleri -Açık kaynaklar -İnsani istihbarat
Güvenirlik	Güvenirlik düşük; doğrulamalar zor; aldatma için kullanmaya eğilimli	Görece yüksek, doğrulanabilir; değişik istihbarat kaynakları tarafından desteklenebilir
Elde Edilebilir	Yavaş; önemli olmak için çok geç, olaylar tarafından aşılıyor	Çabuk; gerektiğinde elde edilebilir
İstihbarata Verilen Önem ve Talep	Ilımlı talep, önemli görülmekle birlikte yaşamsal değil; genelde istihbaratın kötümser ve negatif değerlendirilmesi	-Çok yüksek talep; savaş ve barışta -Önemli; yaşamsal görünüyor. İstihbaratın olumlu/pozitif değerlendirilmesi
Örgüt	Genellikle geçici, ayrı bir meslek değil, az sayıda üye	-Büyük ve profesyonel örgüt, sürekli -Örgüt, karışık istihbarat toplama sürekli örgüt, karışık istihbarat toplama
İstihbarat Döngüsü	Temel dört aşama; tespit, toplama, işleme, dağıtım	Temel dört aşama: tespit, toplama, işleme, dağıtım
Analiz	Sınırlı enformasyon, yoğun insan gücü	Sürekli artan enformasyon ortam bilgisayar desteği

2.1.2. İstihbaratın Tanımı ve Kapsamı

İstihbarat, kelime manası itibariyle Arapça istihbar kelimesinin çoğulu olarak; haberler veya yeni öğrenilen bilgiler, haber alma demektir.[121] İngilizcede istihbarat

[120] Ümit Özdağ, ***a.g.e.***, s.52.
[121] Gültekin Avcı, ***a.g.e.***, s.11.

kelimesinin karşılığı olan "intelligence"; akıl, zekâ, anlayış, haber, bilgi ve istihbarat anlamına gelmektedir. Buradaki vurgu, haberin toplanmasında değil, toplananların birleştirilmesi ve analiz edilmesindedir. Özdağ'a göre bu durum; istihbaratın ABD ve İngiliz toplumlarında "malumatın değerlendirilmesi" olarak, ülkemizde ise "malumatın derlenmesi" olarak algılandığının bir göstergesidir.[122] İstihbarat için Almancada "haberler" anlamına gelen "nachrichten", Fransızcada "işaret, aydınlanma, öğrenme ve öğretme" anlamlarına gelen "renseignement", kelimeleri kullanılırken, Rusçada ise anahtar kelime olarak "güvenlik" karşımıza çıkmaktadır.[123] Her dilde istihbaratın farklı anlamlandırılması o dildeki insanların istihbaratı algılamalarıyla doğrudan ilişkilidir.

İstihbarat ile ilgili net bir tanım yapmak oldukça zordur. Hemen hemen herkesin kabul edebileceği çok farklı tanımlamalar yapılabilir. Ümit Özdağ'ın tanımına göre; istihbarat ulaşılabilen bütün açık, yarı açık ve/veya gizli kaynaklardan her türlü aracın kullanılması sonucunda elde edilen her türlü veri, malumat ve bilginin ulusal genel veya ulusal özel plandaki politikaların gerçekleştirilmesi ve ulusal politikalara zarar verilmesinin engellenmesi amacı ile toplandıktan sonra önemine ve doğruluğuna göre sınıflandırılması, karşılaştırılması, analiz edilerek değerlendirilmesiyle ulaşılan bilgidir.[124]

İstihbarat, Türk Dil Kurumunun Türkçe Sözlüğüne göre; "Yeni öğrenilen bilgiler, haberler, duyumlar ve bilgi toplama, haber alma" olarak tanımlanmaktadır.[125] Gültekin Avcı ise istihbarata şu şekilde bir tanım getirmektedir: "İstihbarat, muhtelif imkân ve vasıtaları kullanarak, herhangi bir konuda enformatik materyal temini ve temin edilen bilgilerin ham halden kurtarılarak işlenmesi, kıymetlendirilmesi ve yorumlanarak bunlardan bir netice çıkarılmasıyla ilgili faaliyettir."[126] Warner'a göre ise istihbarat; faaliyetleri yönlendirmek üzere önceden bilinmesi gereken her türlü konu ile ilgilenmektedir.[127] Bu tanımlamalardan da anlaşılacağı üzere, istihbarat faaliyeti; sadece devletlerin değil, şirketler, reklam

---

[122] Ümit Özdağ, ***a.g.e.***, s.17.
[123] Niyazi Tılısbık ve Özdemir Akbal, ***İstihbarat ve Türkiye***, Nüve Kültür Merkezi Yayınları, Konya, 2006, s.11.
[124] Ümit Özdağ, ***a.g.e.***, s.30.
[125] Türk Dil Kurumu Resmi İnternet Sayfası, http://www.tdk.gov.tr/index.php?option=com_gts&arama=gts&guid=TDK.GTS.52e817f4c5ef32.41851431, (Erişim tarihi: 29.01.2014).
[126] Gültekin Avcı, ***a.g.e.***, s.12.
[127] Michael Warner, Wanted: A Definition of "Intelligence" Understanding Our Craft, https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol46no3/article02.html, (Erişim tarihi: 29.01.2014).

ajansları, kişiler vb. rakipleri ile ilgili bilgi edinmek veya farklı amaçlarla bilgi toplamakta ve bu bilgileri değerlendirip, analiz ederek gelecekle ilgili çıkarsamalar yapmaktadır.

İstihbaratın sadece haber, bilgi ya da istihbarat üretimi ile sınırlı olmadığının kavranması gereklidir. İstihbarat servisleri dışında da; özel kuvvetler veya çeşitli gerilla tipi unsurlar tarafından yapılan militer örtülü operasyonlar, çokuluslu şirketler veya finans kurumları tarafından ekonomik güvenliğe yönelik sinsi uygulamalar, yönlendirilmiş medya unsurları tarafından veya etki ajanları tarafından uygulanan propaganda faaliyetleri de birer istihbarat fonksiyonudur.[128] Küreselleşme beraberinde istihbaratın aktörlerini ve kapsamını da büyütmektedir. Küreselleşme ve teknoloji, istihbarat toplama vasıtalarının etkinliğini artıracak, özellikle uzaya dayalı istihbarat vasıtaları alanındaki teknolojik üstünlük, güvenlik alanında önemli bir kuvvet çarpanı olacaktır.

Yukarıda verilen tanımlardan yola çıkarak devlet açısından istihbaratın amacı, mevcut ve potansiyel devletlerin kısa ve uzun vadeli niyetlerinin, kısa ve uzun vadeli niyetlerini gerçekleştirmek için ne tedbirler aldıklarının, bu tedbirleri uygulama güç/yeteneklerinin olup olmadığının tespiti ile yeteneklerin kabul ihtimal derecesinin ne olduğunun belirlenmesidir.[129] Kısaca istihbarat, devletlerin başındaki karar vericilerin ülkelerinin güvenliklerini sağlama, bekalarını koruma, belirsizlikleri azaltma ve çıkarlarının arttırılmasını sağlamada önemli bir role sahiptir.

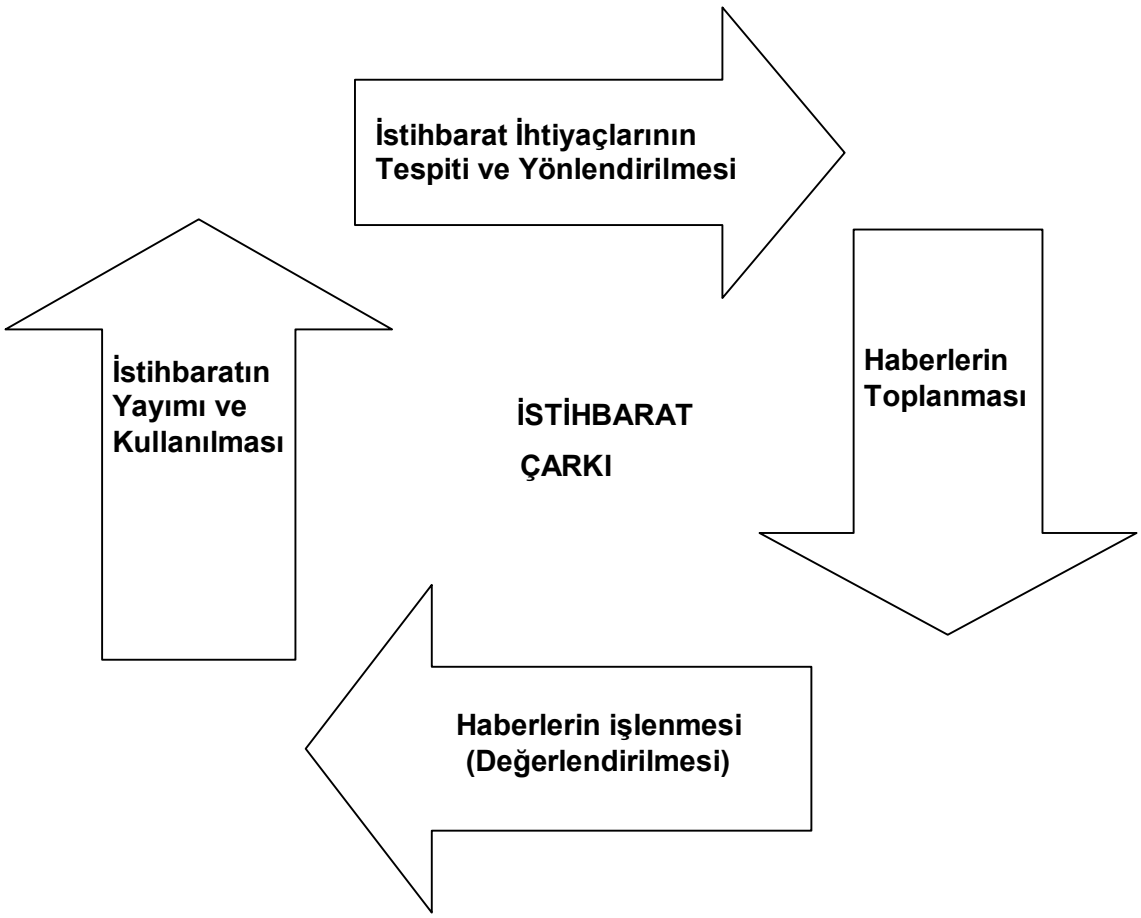
İstihbaratı dikkate almayan bir devlet yönetiminin, gözleri bağlı şekilde maraton koşmaya çalışan bir sporcudan hiçbir farkı yoktur. Böyle bir sporcu nereye gittiğini, rakiplerini, önünde mi arkasında mı olduğunu, ne kadar koştuğunu, özetle hiçbir şeyi bilmeden koşar. Oysa karar alıcılar uluslarının karşı karşıya olduğu fırsatları ve tehditleri öngörmekle yükümlüdür.[130]

2.1.3. İstihbarat Çarkı

İstihbaratın işleyiş mekanizması döngüsel olduğu kabul edilen ve ham bilginin/verinin istihbarata dönüştürülmesi sürecini gösteren "İstihbarat Çarkı" ile

[128] Sait Yılmaz, ***a.g.e.***, s.196.
[129] Muazzez Şenel ve Turhan Şenel, ***İstihbarat ve Genel Güvenlik Konularımız***, Emniyet Genel Müdürlüğü Yayınları, Ankara, 1997, s.32.
[130] Ümit Özdağ, ***a.g.e.***, s.20.

ifade edilir. Millî İstihbarat Teşkilatı'nın (MİT) resmî internet sitesinde bu çarkın safhaları şu şekildedir:



Şekil-1: İstihbarat Çarkı[131]

Daha ayrıntılı bir istihbarat çarkını Özdağ şu şekilde ifade etmektedir:[132]

- İstek veya sorunun tespiti.
- İhtiyaçların tespiti ve çalışma planının yapılması.
- Veri, malumat ve bilgi toplama sürecinin başlaması.
- Toplanan veri ve bilginin karşılaştırılarak güvenilirliğinin test edilmesi ve doğrulanarak düzenlenmesi.
- Yeterli bilgi olup olmadığının kontrolü; yoksa yeterli bilgi için aramaya ve tasnife devam edilmesi, yeterli bilgi olması durumunda,

[131] Millî İstihbarat Teşkilatı Resmî İnternet Sayfası, "İstihbarat Oluşumu", http://www.mit.gov.tr/isth-olusum.html, (Erişim tarihi: 03.01.2014).
[132] Ümit Özdağ, ***a.g.e.***, s.371.

- Veri ve bilginin entegrasyon, analiz ve sentezinin yapılarak yorumlanması.
- Ortaya çıkan istihbaratın üste aktarılması ve gözden geçirilmesi.
- İstihbaratın siyasal karar alıcıya verilmesi.

Genel olarak istihbarat bir süreçtir. Bu süreç; istihbarat ihtiyacının belirlenmesi, gerekli bilgi ve haberlerin toplanması, toplanan bu bilgi ve haberlerin tasnif edilerek analizinin yapılması kısaca işlenmesi, istihbaratın gerekli kurum ve kişilere dağıtılarak kullanılmasını kapsamaktadır. Bunlar;

- İstihbarat İhtiyaçlarının Tespiti ve Yönlendirilmesi: Bu aşamada, devletteki yetkili kişilerin ihtiyaç duydukları istihbarat taleplerine karşı, istihbarat birimleri bu istek ve ihtiyaçlar doğrultusunda haber toplama çalışmalarını yönlendirmektedir.

- Haberlerin Toplanması: Diğer bir aşama olan haber toplama işlevi, ‘’açık’’ ve ‘’kapalı’’ kaynaklar kullanılarak yerine getirilmektedir. Kitap, radyo, televizyon, gazete, dergi, internet siteleri gibi herkesin ulaşabileceği haber kaynakları açık kaynaklardır. Kapalı kaynaklar ise, çeşitli haber toplama yollarıyla, belirli bir istihbarat ihtiyacı konusunda sadece ilgili kişilerin habere ulaşabilmesidir. Yani kapalı kaynaklara herkes ulaşamamaktadır.

- Haberlerin İşlenmesi (Değerlendirilmesi): Bu aşamada toplanan haberler tasnif edilmekte, kıymetlendirilmekte, yorum ve analizi yapılmaktadır. Tasnif sırasında benzer bulgular bir araya getirilmektedir. Kıymetlendirme sürecinde haberin istihbarat değeri, doğruluğu ve güvenilirliği tespit edilmektedir. Yorum ve analizi sürecinde de, elde edilen bilgiler doğrultusunda olayların anlamı ve önemi ortaya konmaktadır.

- İstihbaratın Yayımı ve Kullanılması: Yorum ve analizi yapılan ve istihbarata dönüşmüş raporlar ilgili kurumlara iletilmektedir. İlgili kurumlar bu istihbaratı kullanmanın yanında geri beslemeler yaparak yeni istihbarat ihtiyaçlarını belirlemektedirler. Böylece, birbirini izleyen dört aşamadan oluşan ve dördüncü aşamadan sonra yeniden ilk aşamaya dönen ‘’İstihbarat Çarkı’’ tamamlanmış olmaktadır.

2.1.4. Elde Edilişi Bakımından İstihbarat Türleri

2.1.4.1.Açık Kaynak İstihbaratı

Açık kaynak ile kastedilen gazete, dergi, kitap, broşür, veri tabanları, internet vb. dâhil olmak üzere halkın kullanımına açık olan her türlü veri, haber, bilgidir.[133] Özellikle internet bu alanda önemli bir açık kaynak istihbaratı imkânı sağlamaktadır. Günümüzde istihbaratı oluşturan bilginin %85'ten fazlasının açık kaynaklardan temin edildiği değerlendirilmektedir.[134] Bu oran net bir şekilde açık kaynak istihbaratının önemini ortaya koymaktadır.

Açık kaynakların bileşenleri analiz edildiğinde diğer istihbarat toplama yöntemlerine nazaran birçok üstün tarafının olduğu görülmektedir. Maliyet açısından bakıldığında açık kaynak istihbaratı ucuzdur. Kaynak açısından ise olağanüstü bir zenginlik söz konusudur. Metot açısından bakıldığında açık kaynak istihbaratı uygulaması en kolay olan toplama yoludur.[135] Genel olarak bakıldığında açık kaynak istihbaratının etkin bir şekilde kullanıldığında en verimli istihbarat elde etme yöntemi olabilecek kapasitede olduğu değerlendirilmektedir.

Küreselleşen dünyada haber alma özgürlüğünün gittikçe yaygınlaşması, sosyal medya uygulamalarının gelişmesi, internet ve iletişim teknolojilerindeki hız, açık kaynaklar vasıtasıyla elde edilen istihbarı değeri olan bilgiye ulaşma imkânlarını arttırmıştır. Açık kaynaklarda yer alan veri, haber, görüntü ve bilgilerin istihbarata dönüştürülebilmesi faaliyetinin her geçen gün artarak devam ettiği, bu noktadan hareketle açık kaynak istihbaratının öneminin daha da çok artacağı değerlendirilmektedir.[136] Gelecekte istihbaratı oluşturan bilginin oranında açık kaynaklardan elde edilen bilginin daha da artacağı öngörülmektedir.

Gerçekte, istihbarat değerini taşıyan önemli miktardaki bilgi, açık kaynak istihbarat bilgileri sınıfındadır. Bu açık kaynak istihbarat bilgilerinin arasına pek ender olarak ulusal sırlar sızabilir. Açık kaynak istihbarat bilgileri nispeten kolay ve ucuz elde edilirler. Açık kaynaklardan normal şartlar altında politika, endüstri, tarım, ulaştırma, hava şartları gibi konular hakkında bilgi edinilir. Ayrıca, hedef ülkenin istemediği halde meydana gelen olaylar dikkatli izleyiciler tarafından izlenerek çeşitli bilgiler kolayca elde edilebilir.[137] Bu bilgilerden hareketle hedef ülkede meydana

[133] Ümit Özdağ, ***a.g.e.***, s.337.
[134] Sait Yılmaz, ***a.g.e.***, s.126.
[135] Ümit Özdağ, ***a.g.e.***, s.338-339.
[136] Hasan Ateş, ***Kamu Güvenliğinde İstihbarat Sisteminin Değerlendirilmesi***, Sosyal Bilimler Enstitüsü, Atılım Üniversitesi, Ankara, 2012, s.11.
[137] Sait Yılmaz, ***a.g.e.***, s.126.

gelebilecek gelişmeler kolaylıkla öngörülebilir ve gerekli önlemler alınabilir. Maliyet açısından duruma bakıldığında en masrafsız istihbarat elde etme yöntemidir.

Açık kaynak istihbaratındaki büyümenin çeşitli sebepleri vardır. Sebeplerden birincisi internet başta olmak üzere bilgi teknolojilerinde yaşanan büyük gelişmelerdir. Diğer bir sebep istihbarat ihtiyaçlarının Soğuk Savaş sonrası çok farklı alanlara yayılmasıdır. Soğuk Savaş öncesi tek bir noktaya odaklanan istihbarat çalışmaları, sonrasında ise tehdit algılamalarındaki değişmeyle beraber çok farklı sahalarda ortaya çıkmıştır.

Açık kaynakların bütün avantajlarına rağmen sınırlılıkları vardır. Bu noktada ne tür bilgilerin açık kaynaklarda tam anlamı ile bulunamayacağını hatırlatmak gerekmektedir. Bunlar;[138]

- Sürpriz saldırı hazırlıkları,
- Nükleer silahlanma,
- Silah kontrolü,
- Terörizm,
- Rüşvet ve şantaj,
- Uyuşturucu kaçakçılığı.

2.1.4.2. İnsan İstihbaratı

İnsan istihbaratı bilinen en eski istihbarat toplama yöntemidir. Yazılı metinlere bakıldığında da M.Ö. 5000'lerde Mısır Kralı 3' üncü Tutmosis, kuşatma altındaki Yafa kentine ajanlarını gizlice göndermiş ve bu ajanlardan gelen istihbarat raporları doğrultusunda savaş stratejisini belirlemiştir. Bu sayede şehri daha az bir maliyetle ele geçirmiştir.[139]

İnsan istihbaratı, insan unsuru kullanarak, yabancı karar alma sistemine sızma yöntemiyle yabancı sistemin güç ve zayıflıkları, amaç ve niyetleri konusunda bilgi toplamaktır.[140] Diğer bir tanıma göre ise insan istihbaratı; eğitilmiş insan kaynakları vasıtasıyla, insanlardan, görsel ve işitsel kaynaklardan, ilgi duyulan unsurların,

[138] Ümit Özdağ, ***a.g.e.***, s.342.
[139] Erdal Şimşek ve İlhan Bahar, ***Türkiye'de İstihbaratçılık ve Mit***, İstanbul, Kum Saati Yayınları, 2004, s.12.
[140] Ümit Özdağ, ***a.g.e.***, s.129.

niyetlerin, mahiyetlerin, kapasitelerin, güçlerin, takdirlerin, mevcut ekipmanların, personelin öğrenilebilmesi için toplanan bilgilerin analizinden elde edilen istihbarattır.[141] Kısaca insan istihbaratı hem açık hem de gizli bilgi toplama yöntemleriyle, insan kaynaklarından istihbarı bilgi elde edilmesidir.

Halk içinde, insan istihbaratı denilince; casuslar, gizli faaliyet gösteren ajanlar veya yabancı ülkede görev yapan Dışişleri Bakanlığı elemanları ve askeri ataşeler gibi açık istihbarat toplayıcıları akla gelmektedir. Günümüzde eski soğuk savaş dönemi ajan tipleri kaybolmakta, yeni ajan tipleri daha farklı fonksiyonlar ile bilim adamı, iş adamı gibi görüntüler altında artık kendilerine daha çok iş dünyası, araştırma merkezleri, sivil toplum örgütleri gibi kurumlar içerisinde yer bulmaktadır.[142]

Hedefle ilişkili sadece yetiştirilmiş ajanlar değil, hedefle iletişimdeki her kişi insan istihbaratı kaynağıdır. Turist olarak dış ülkelere giden kişiler, politikacılar, sporcular, gazeteciler, akademisyenler, yabancılarla temasta bulunabilecek her şahıs bir istihbarat kaynağı olabilir.[143] Bürokratların, uluslar arası organizasyonların temsilcilerinin, akademisyenlerin dış ülkeleri çeşitli maksatlarla ziyaretleri ve iletişimleri insan istihbaratı toplama vasıtaları arasında sayılabilir.

İnsan istihbaratının sağladığı avantaj ve dezavantajlar bulunmaktadır. Kullanılan istihbarat toplama yönteminin avantajlarının ve sınırlılıklarının bilinmesi istihbarat analizcisinin doğru değerlendirme yapmasına katkı sağlamaktadır. İnsan istihbaratının avantajları aşağıdaki gibi sıralanabilir:[144]

1. Her türlü harekâtta kullanılabilir,
2. Düşmanın niyetini ve planlarını ortaya çıkarmada yardımcı olur,
3. Diğer toplama yöntemleri ile elde edilen istihbaratın doğrulanması ve açıklanmasına imkân verir,
4. Teknoloji gerektirmez,
5. Her türlü hava ve arazi şartlarında etkindir,
6. Elle tutulmayan ve görülemeyen konularda haber toplamayı sağlar,
7. Toplanması ve analizi kısa sürede mümkündür,

---

[141] ***FM 2-22.3 (FM 34-52) Human Intelligence Collector Operations*****,** Department of the Army, Washington, 2006, s.1-4.
[142] Sait Yılmaz, ***a.g.e.***, s.124-125.
[143] Sait Yılmaz, ***a.g.e.***, s.124.
[144] USAF Intelligence Targeting Guide Airforce Pamphlet, www.fas.org.pdf, (Erişim tarihi: 10.01.2014).

8. Yüksek maliyet gerektirmez,
9. Elde edilen haber ve bilgi diğer toplama yöntemlerinin sağladıklarına kıyasla daha güncel ve eş zamanlıdır,
10. Biyografik istihbarat elde etmede en etkin yöntemlerden biridir,
11. Erken ikaz sağlar,
12. Esneklik sağlar, kişi değişken durumlara kolayca uyum sağlayabilir,
13. Hedefin imkân ve kabiliyetlerinin ortaya çıkarılmasını sağlar.

İnsan istihbaratının sınırlılıkları ise aşağıdaki gibi sıralanabilir:[145]

1. Haber kaynağı sayısı sınırlıdır,
2. İnsan zaaflarına karşı hassastır,
3. Haber kaynağı üzerinde asgari kontrol sağlar,
4. Haber kaynağının bulunması ve kaynaktan bilgi alınacak ortamı sağlayacak iş ilişkisinin geliştirilmesi zaman alabilir,
5. Yabancı dil bilgisi önemlidir,
6. İstihbarat planlandığı şekilde zamanında elde edilmeyebilir,
7. Görev yerine erişebilme veya hedefe sızma zor olabilir,
8. İnsan istihbaratını yapan vasıtanın güvenirliliğinin tespiti diğer toplama vasıtalarına nazaran daha zordur,
9. Yasal mevzuat faaliyetleri kısıtlar.

2.1.4.3. Teknik İstihbarat

Teknik istihbarat bir dizi teknik yöntemin kullanılarak istihbarı bilginin elde edilmesidir. Teknik istihbarat, 19. Yüzyılın üçüncü çeyreğinde telefonların dinlenmesini içeren sinyal istihbaratı ile başlamış, 1960'ların başında ilk casus uyduların yörüngeye oturmasına kadar geçen yaklaşık 100 yıl içinde büyük gelişme kaydetmiştir. Teknik istihbarat ile elde edilen bilgi, insan istihbaratı ile elde edilen bilgiyle mukayese edilemeyecek kadar çoktur.[146] Teknolojik gelişmelere paralel olarak teknik istihbarat kapsamı genişlemiştir. Teknolojik gelişmeler teknik istihbarata yeni kapılar açarak bu yolla elde edilen istihbarı bilginin boyutları artmıştır.

[145] ***FM 2-22.3 (FM 34-52) Human Intelligence Collector Operations***, Department of the Army, Washington, 2006, p.1-14.
[146] Ümit Özdağ***, a.g.e.***, s.134.

Teknik istihbaratta bilgi farklı yöntemler kullanılarak elde edilmektedir. Özdağ'a göre bu yöntemlerin en önemlileri;

- Sinyal İstihbaratı,
- Fotoğraf İstihbaratı,
- Uydu istihbaratı,
- Nükleer İstihbarat,
- Radar İstihbaratı,
- Akustik İstihbarat,
- Elektronik İstihbarat,
- Elektromanyetik İstihbarat,
- Tıbbi İstihbarat.

Bunlara farklı teknik istihbarat yöntemleri de eklenebilir. Özellikle iletişim teknolojilerindeki gelişmelere paralel olarak ve bu kapsamda internetin gelişimiyle siber istihbarat faaliyetleri de, teknik istihbaratın önemli yöntemleri arasına dâhil edilebilir.

Siber istihbarat, istihbarat literatüründe yoğun olarak internet ve bilgisayarın kullanımını kapsayan ancak teknik ve elektronik istihbarat toplama faaliyetleri içinde uydular, hava ve uzay araçları ile yapılan istihbarat ile birlikte anılmaktadır.[147] 21. yüzyıl teknolojinin getirdiği imkânlar vasıtası ile gözetleme, izleme ve dinleme çağı olacaktır[148].Bu çerçevede siber istihbarat, diğer istihbarat elde etme yöntemlerine nazaran daha kolay, daha ucuz ve ortaya çıkmasıyla doğacak kötü sonuçlar açısından daha az tehlikelidir.

Sinyal istihbaratı, orijinal olarak hedef tarafından gönderilen sinyal şeklindeki mesajların, elektromanyetik yayma vasıtaları ve sensörler tarafından tespit edilmesidir. Bu mesajlar, elektro-manyetik yayma vasıtaları ve sensörler vasıtası ile tespit edilebilir.[149] Çeşitli sinyal istihbarat türleri bulunmaktadır. Bunlardan bazıları; iletişim istihbaratı, elektronik istihbarat, lazer istihbaratı, radar istihbaratıdır. Bu istihbarat türleri ile sinyaller tespit edilebilmekte ve hedefle ilgili bilgilere ulaşılabilmektedir.

---

[147] Sait Yılmaz ve Olay Salcan, ***Siber Uzay'da Güvenlik ve Türkiye***, Milenyum Yayınları, İstanbul, 2008, s.17.
[148] Sait Yılmaz, "ABD İstihbaratında…", ***a.g.m.***, s.18.
[149] Sait Yılmaz, ***a.g.e.***, s.126.

Daha çok savunma amaçlı bir istihbarat türü olan fotoğraf istihbaratı, en basit uçaklara takılan fotoğraf makineleri ile başlayıp uzaydaki uydulardaki gelişmiş fotoğraf makineleri ile çekilen fotoğraflarla devam etmiştir.[150] Günümüz teknolojileri vasıtasıyla özellikle uydulardan faydalanarak çözünürlüğü çok yüksek fotoğraflar elde edilebilmekte ve istihbarat açısından kullanılabilmektedir.

Teknik istihbaratın da insan istihbaratında olduğu gibi avantajlı olduğu yönler ile sınırlılıkları mevcuttur. Avantajlı olan yönleri şunlardır;[151]

1. Anlık bilgi sağlayabilir,
2. Hedef hakkında çok belirgin bilgileri açığa çıkarabilir,
3. Hedefin hareketlerindeki ve faaliyetlerindeki değişiklikler anında fark edilebilir,
4. Diğer istihbarat disiplinlerini uyarabilir,
5. Hedefin yerini tespit ve anlık olarak takip imkanı sağlar,
6. Yüksek doğrulukta bilgi sağlar,
7. Kaynak üzerinde azami kontrol imkanı sağlar,
8. Elde edilen veriler en kısa sürede kullanıcılara iletilebilir.

Teknik istihbaratın sınırlılıkları ise şunlardır;

1. Hava şartlarından etkilenebilir,
2. Hedef tarafından aldatılmaya karşı hassastır,
3. Özel olarak hazırlanmış platformlara ihtiyaç duyar,
4. Maliyeti yüksektir,
5. Anlık bilgiyi verir, gelişecek durumla ilgili değerlendirme yapamaz,
6. Toplama süresi kısadır fakat değerlendirme uzun sürebilir,
7. Özel bir eğitim gerektirir.

2.2. SİBER İSTİHBARAT UNSURLARI

2.2.1. İnternet Kavramı

[150] Ümit Özdağ***, a.g.e.***, s.139.
[151] USAF Intelligence Targeting Guide Airforce Pamphlet, www.fas.org.pdf, (Erişim tarihi: 07.03.2014).

İnternetin ortaya çıkışı askeri amaçlıdır. Askeri ve sivil teknoloji; amaçlar, çok farklı olsa da, tıpatıp aynı doğrultuda gelişir. Bu, ilgili bütün ülkelerde, böyle olmuştur.[152] Sovyetler Birliği'nin 1957'de Sputnik uydusunu uzaya göndermesinden sonra Amerika Birleşik Devletleri hükümeti savaş sırasında veya savaştan önce klasik haberleşme kanallarının kullanılmayacak derecede tahrip edilmesi halinde tek bir merkezden yönetilmeyen veya diğer bir ifadeyle tek bir ana bilgisayar ünitesinden bağımsız olarak çalışabilen bir bilgisayar ağı kurulabilmesi için harekete geçmiştir. Bu amaçla İleri Araştırma Projeleri Ajansı'nın (ARPA) kurulmasına karar verilmiştir.[153]

İnternet'in temeli, Amerikan Savunma Bakanlığı İleri Araştırma Projeleri Ajansı (Advanced Research Project Agency-ARPA) tarafından yürütülen ARPANET projesiyle atılmıştır. Projenin öncelikli amacı, askeri herhangi bir saldırı durumunda dahi bilgi akışını devam ettirebilecek bir ağ sistemi yaratmaktı. Ancak 1971 yılında bu projeye, yaklaşık 24 kadar araştırma ve kamu sitesinin de bağlanmasıyla ARPANET, araştırmacıların da kullanımına sunulmuştur. 1989 yılında İNTERNET adını alan ARPANET artık araştırma projesi konumundan işletme durumuna gelmiş ve 1990'dan sonra hızla gelişerek bugünkü halini almıştır.[154] Dünya genelinde internet kullanıcı sayısı 2000 yılında 360 milyon iken, bu sayı Aralık 2013 tarihinde 2,75 milyar kullanıcıya ulaşmıştır. (Tablo-4)

Tablo-4: Dünya'da İnternet Kullanan Kişi Sayısı[155]

	Dünya'da İnternet Kullanan Kişi Sayısı								
	Milyon								
	2005	**2006**	**2007**	**2008**	**2009**	**2010**	**2011**	**2012***	**2013***
Gelişmiş Ülkelerde	616	649	719	750	773	830	875	913	958
Gelişmekte Olan Ülkelerde	408	502	645	807	974	1.193	1.398	1.584	1.791
Dünyada	1.024	1.151	1.365	1.556	1.747	2.023	2.273	2.497	2.749

[152] Tolga Yarman, ***Geçmişte ve Bugün Nükleer Enerji Tartışması***, Okan Üniversitesi Yayınları, İstanbul, 2011, s.26.
[153] Adem Peker, ***İnsani Değerler Yönelimli Psiko-Eğitim Programının Problemli İnternet Kullanımı ve Siber Zorbalık Üzerindeki Etkisi***, Eğitim Bilimleri Enstitüsü, Sakarya Üniversitesi, 2013, s.48.
[154] Sait Yılmaz ve Olay Salcan, ***a.g.e.***, s.35-37.
[155] Statistics, http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx, (Erişim: 14.02.2014).

Tablo-4'e göre gelişmiş ülkelerde 2005 ve 2013 yılları arasında internet kullanan kişi sayısındaki artış oranı %155 iken, gelişmekte olan ülkelerde ise bu oran %439'dur. Bu oranlarda gelişmekte olan ülkelerin potansiyelini ortaya koymaktadır.

İnternet, ilk başlarda gerçekte bir araştırma ve eğitim ağı olarak düşünülmüş ve tasarlanmış olmasına rağmen, bu günün dünyasında kullanma maksadı çok farklı boyutlara ulaşmıştır. Bugün internet, kamu, özel ve ticari iletişim için bir yapı haline gelmiştir ve süratle genişlemektedir.[156]

Günümüzde bilgiler, haberler, sinyaller tarihin hiçbir döneminde görülmemiş bir hızla tüm dünyaya yayılmaktadır.[157] Coğrafi olarak birbirinden ne kadar uzak olursa olsun dünyadaki bütün bilgisayarları birbirine bağlayan internet, 20. yüzyılın son çeyreğinin en önemli teknolojilerinden biridir. İnternet sayesinde mesafeler izafi olarak küçülmüş; dünyanın herhangi bir yerindeki bilgiye erişim hızı inanılmaz ölçüde artmıştır.[158]

Özellikle 1990 sonrası gelişen ağı sayesinde tüm dünyayı saran internet, devletlerin ulusal güvenliklerini her yönü ile tehdit etmeye başlamıştır. Uluslararası alışveriş şirketleri yüzünden gümrük sistemleri, "Hacker" ler yüzünden en gizli devlet sırları, her gün mantar gibi artan korsan siteler yüzünden gerçek hayatın sanal âleme de taşınması gereken hukuk sistemleri uygulanamamasından dolayı tehdit altındadır. Özellikle büyük kentlerin altyapı ve iletişim alanları büyük bir tehdit altındadır.[159]

İnternet kullanımının hızlı artışına rağmen siber uzayda güvenlik önlemleri yetersiz kalabilmektedir. Bunun en önemli nedenleri, internetin tasarlanışında ki beş önemli zafiyettir. Bunlar;[160]

---

[156] Sait Yılmaz ve Olay Salcan, ***a.g.e.***, s.37.
[157] Şamil Ünsal, "Milli Güç, Bileşenleri ve Vasıtaları", ***Türk Dünyası Araştırmaları***, 2010, Sayı: 187, 27-50, s.41.
[158] Sait Yılmaz, ***a.g.e.***, s.430.
[159] Mehmet Özcan, Siber Terörizm ve Ulusal Güvenliğe Tehdit Oluşturma Boyutu, http://bookre.org/reader?file=1183626&pg=2, (Erişim: 17.02.2014).
[160] Richard A. Clarke ve Robert K. Knake, ***Siber Savaş***, Çev. Murat Erduran, İkü Yayınevi, İstanbul, 2011, s.46.

1. Adresleme sistemidir. Kablosuz sistem kullanıyorsanız, hacker bu telsiz dalgalarını yakalar ve kullanır. Kablolu sistemde ise daha da çok fırsat vardır.
2. İnternette teknik organlar vardır ancak yetkili makam yoktur. Bir düzine devletlerarası ve sivil toplum kuruluşu internet yönetiminde rol oynuyor, ama tek başına tüm yetkiyi elinde toplayan bir kurum ortada henüz yoktur.
3. İnternetin üçüncü zayıf noktası da işletim sistemlerinin hepsinin açık ve şifresiz olmasıdır.
4. İnternetin diğer bir zafiyeti de "malware" adı verilen bilgisayarlara saldırmak üzere tasarlanmış kötü niyetli yazılımları dağıtma potansiyelidir.
5. Son olarak da internetin zayıf noktalarından biri de ademi merkeziyetçi bir tasarımı olan büyük bir ağ olmasıdır. İnternet öncelikle güvenlikten çok merkezi kontrolü yok etmek üzere kurulmuştur. Bunun nedeni, internet tek merkezden kontrol edilir ve bu merkez herhangi bir saldırı sonucu imha edilmesi durumunda bütün internetin kullanılamaz duruma gelme ihtimalidir. Bu riski ortadan kaldırmak amacıyla internetin merkezi kontrolü yoktur.

2.2.2 Siber Kavramı

Yalın olarak Türkçe sözlüklerde "siber" kelimesi yer almamaktadır. Aslında "sibernetik" kelimesinin bir öneki olan "siber" sözcüğü, aynı zamanda kelimeyi kısaltmak amacıyla da kullanılmaktadır. Sibernetik, Norbert Weiner isimli Amerikalı bir bilim adamı tarafından ilk kez 1948 yılında "hayvanlarda ve makinelerde iletişim ve kontrol bilimi" anlamında kullanılmıştır.[161] Sonrasında çok tartışılan ve üzerinde anlaşılan bir tanıma sahip olmasa da genel kabul görmüş "Süreçleri ve iletişimi kontrol etme ve yönetme, bilgisayar ve internetle ilgili" bir anlamı işaret ettiği değerlendirilmektedir. Türkçede bu kavramın karşılığında genellikle "bilişim" kelimesinin kullanıldığı görülmektedir. Bu kelime ise Fransızca "informatique" sözcüğünden gelen ve Türkçe "enformatik" olarak kullanılan kelimeden türetilmiştir.[162] Bilişim kelimesi, "İnsanoğlunun teknik, ekonomik ve toplumsal alanlardaki iletişiminde kullandığı ve bilimin dayanağı olan bilginin, özellikle elektronik makineler aracılığıyla düzenli ve akla uygun bir biçimde işlenmesi bilimi"

[161] Stafford Beer, What is Cybernetics?, http://www.nickgreen.pwp.blueyonder.co.uk/beerWhatisCybernetics.pdf, (Erişim tarihi: 11.02.2014).
[162] Ali Karagülmez, ***Bilişim suçları ve Soruşturma-Kovuşturma Evreleri***, Ankara, Seçkin Yayıncılık, 2005, s.34.

[163] anlamına gelmektedir. Bu tanımdan da anlaşılacağı üzere, "bilişim", "siber" kavramından daha kapsamlı bir anlamı ifade etmektedir.

Genel olarak "siber" ile bilgisayar ve buna bağlı elektronik sistemlerin bulunduğu ortam, "bilişim" ile de bu ortamdan etkin olarak faydalanma ve bu ortam aracılığıyla bilgi üretilmesi gibi anlamların çıkarılması mümkündür.[164] Siber kavramının hayatımıza girmesi daha çok internet ve bilgisayarın insanların, özel ve devlet kurumlarının bir parçası olması ile başlamıştır. Bu kavramın daha iyi anlaşılması için siber uzay, siber saldırı, siber savaş, siber suç, siber terör vb. kavramların da açıklanması gerektiği değerlendirilmektedir.

2.2.3 Siber Uzay Kavramı

Siber Uzay terimi ilk kez Amerikalı bilim-kurgu yazarı William Gibson tarafından, 1982 yılında basılan "Yanan Krom (Burning Chrome)" adlı hikâye kitabında kullanılmıştır.[165] ABD Savunma Bakanlığının tanımına göre siber uzay; internet iletişim ağları, bilgisayar sistemleri, gömülü işlemci ve kontrol birimlerini içeren, bilgi teknolojileri altyapılarından meydana gelen, birbirine bağımlı ağların oluşturduğu bilgi ortamındaki küresel bir alandır.[166] Diğer bir tanıma göre siber uzay, kritik altyapılarımızın çalışmasını sağlayan, birbirine bağlı yüz binlerce bilgisayar, sunucu, yönlendirici, anahtar (switch) ve fiber optik kablolardan oluşmaktadır.[167]

Siber uzaydan söz ederken sanki soyut bir beşinci boyutmuş gibi algılanmaktadır. Oysa siber uzay fiziksel bileşenlerden oluşmaktadır. Denizaltı kabloları, yüksek hızlı fiber optik kablo demetlerinden, her yönlendirici ve sunucuya kadar, bu fiziksel bileşenlerden her biri egemen ülkenin topraklarında yerleşiktir.[168]

Siber uzay enerji dağıtım ağları, kapalı askeri ağlar, iletişim ağları, cep telefonları, yazılım tabanlı telsizler, elektronik komuta sistemleri, Supervisory Control

---

[163] Türk Dil Kurumu Resmi İnternet Sayfası, http://www.tdk.gov.tr/index.php?option=com_gts&arama=gts&guid=TDK.GTS.515de6b7791330.26994092, (Erişim tarihi: 11.02.2014).
[164] Haydar Çakmak ve Cenker Korhan Demir, "Siber Dünyadaki Tehditler ve Kavramlar", ***Suç, Terör ve Savaş Üçgeninde Siber Dünya***, Barış Platin Kitabevi, Ankara, 2009, 23-54, s.26.
[165] Hasan Çifci, ***Her Yönüyle Siber Savaş***, TÜBİTAK Popüler Bilim Kitapları, Ankara, 2013, s.2.
[166] Department of Defense Dictionary of Military and Associated Terms, http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf, (Erişim tarihi: 21.01.2014).
[167] The National Strategy to Secure Cyberspace, https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf, (Erişim tarihi: 21.01.2014).
[168] Richard A. Clarke ve Robert K. Knake, ***a.g.e.***, s.137.

and Data Acquisition (SCADA) sistemleri, uydu sistemleri, insansız hava araçları, uçaklar (özellikle uçaktaki sistemleri kontrol eden temel yazılım ve donanımlar) gibi birçok sistem ve donanım siber uzayın elemanıdır.[169]

Siber uzay dünyadaki tüm bilgisayar ağları ve onların bağlı olduğu ve kontrol ettiği her şeyi kapsamaktadır. İnternet birbirine bağlı olan ağlardan oluşan açık bir ağdır ve siber uzay sadece internetten ibaret değildir. Siber uzay internet ve internete bağlı olmayan birçok bilgisayar ağını içermektedir.[170] Siber uzayın interneti de kapsayan ancak salt internetten ibaret olmayan bir sistem olduğu kabul edilmektedir. İnternet dışında, elektrik santrallerinin sahip olduğu bilgisayar ağları, barajların sahip olduğu bilgisayar ağları, ulaşım sisteminde kullanılan bilgisayar ağları vb. sistemlerde kullanılan bilgisayar ağları da siber uzayın bir parçasıdır.

İletişimin düşük maliyeti ve İnternet'e bağlanmadaki kolaylıktan dolayı, internet kullanımı, diğer elektronik iletişim çeşitlerinin yerini almaktadır. Bu geniş olanaklardan faydalanmak isteyen kritik altyapı işletmecileri, sistemlerini internete bağlamakta ve bu şekilde siber uzay ile fiziksel dünya birleşmektedir.[171] İnternet kullanımının inanılmaz büyüme hızı ve bilgisayarların hayatın bir parçası haline gelmesi "siber uzay" kavramının daha sık kullanılmasına ve ilerleyen dönemlerde de vazgeçilmez bir unsur olarak yer edineceği değerlendirilmektedir.

Siber uzay daha çok her gün kullanılan unsurlardan oluşmaktadır. Sizin işyerinize ya da çocuğunuzun okula götürdüğü dizüstü bilgisayar, masaüstü bilgisayarınız ve bunun gibi milyonlarca makine siber uzayı oluşturmaktadır. Şehir merkezindeki yer altındaki fiber optik kablolar, herhangi bir bilgisayarın, işlemcinin ya da bunları birbirine bağlayan kabloların olduğu her yer siber uzay sayılmaktadır.[172] Siber uzay akılda bıraktığı karmaşık kavram örüntüsünün aksine günlük hayatta kullandığımız akıllı telefonlar gibi aşina olduğumuz bilgi teknoloji unsurlarından oluşmaktadır.

Siber uzayda sınırların anlamı ortadan kalkmaktadır. Bilgisayarın başına geçen bir siber terörist için yolun diğer tarafındaki bir bilgisayar ile dünyanın her hangi bir yerindeki bilgisayar eşit uzaklıktadır. Yazılım ve donanım olarak siber uzayı oluşturan altyapının, tasarımı ve gelişimi de küreseldir. Siber uzayın bu küresel

[169] Hasan Çifci, ***a.g.e.***, s.5.
[170] Richard A. Clarke ve Robert K. Knake, ***a.g.e.***, s.44.
[171] Sait Yılmaz ve Olay Salcan, ***a.g.e.***, s.40.
[172] Richard A. Clarke ve Robert K. Knake, ***a.g.e.***, s.43.

karakteri nedeniyle mevcut açıklıklar herkes için vardır.[173] Mesafelerin önemini yitirmesini sağlayan siber uzay aynı zamanda sistemde oluşan fiziksel ya da yazılımsal açıkları sadece yakın çevreye karşı değil tüm dünyaya karşı vermektedir.

Gelişmiş ülkelerde bütün sektörlerin hizmetlerini siber uzaya taşımasıyla birlikte kritik öneme sahip bilgiler telefon hatlarından, fiber optik kablolardan ve elektro-manyetik dalgalar üzerinden iletilmeye başlamıştır. Kendilerine fayda sağlamak isteyen kişiler, gruplar ve organizasyonlar bu bilgilere erişerek güçlerini arttırmak istemektedirler.[174]

Siber uzaydaki kötü niyetliler, kişiler, suç örgütleri, teröristler veya ülkelerin bizzat kendileri olabilirler. Saldırganlar, hangi şekilde olursa olsunlar, tümü politik ve ekonomik olarak geniş çapta bir etki yaratabilmek için yazılım, donanım, ağ ve protokollerin tasarımı veya uygulanmasından kaynaklanan açıklıkları bulmak ve onları kullanma amacındadırlar.[175] Bu nedenle gün geçtikçe gelişen ve büyüyen siber uzay, beraberinde olası saldırılardan koruma yollarını da geliştirmekte, bu da yeni araştırma alanlarının oluşmasına olanak sağlamaktadır. Ülkeler ve organizasyonlar için gizliliği hayati önem taşıyan bilgilerin iletimi bu ortam üzerinden sağlanırken korunmaları içinde gerekli önlemler oluşturulmaktadır.

Savaşların kaderini değiştirmedeki kilit rolünden dolayı bilgi teknolojileri, kara, deniz hava ve uzaya ek olarak, yeni bir harekât alanı olan siber uzayın açılmasına sebep olmuştur. Yeni bir harekât alanı olan siber uzayın kendisine has özellikleri bulunmaktadır. Bu özelliklerin bilinmesi, bu ortamda nasıl harekât icra edileceği konusunda da ipuçları vermektedir. Siber uzayın temel özelliklerini sayacak olursak;[176]

- Diğer harekât alanlarının aksine, insan eliyle oluşturulmuş ve büyük bir kısmına özel sektörün sahip olduğu bir harekât alanıdır.
- Birbirine bağlı veya bağımsız bilgi sistemlerinden ve bu sistemlerde işlenen verilerden(metin, ses veya görüntü) meydana gelmektedir.
- Devletler, özel sektör veya şahıslar tarafından oluşturulan, sahip olunan, yönetilen, işletilen, dünyanın neredeyse tamamını saran bir alandır.

[173] Sait Yılmaz ve Olay Salcan, ***a.g.e.***, s.50.
[174] Salih Bıçakçı, ***21. Yüzyılda Siber Güvenlik***, İstanbul Bilgi üniversitesi Yayınları, İstanbul, 2013, s.3-4.
[175] Sait Yılmaz ve Olay Salcan, ***a.g.e.***, s.71.
[176] Hasan Çifci, ***a.g.e.***, s.8-9.

- Teknoloji; mimariler, stiller, işlemler, yeni kabiliyet ve yöntemler geliştikçe değişikliğe uğramaktadır.
- Siber uzaya, siber uzaydaki elemanlara erişim ve bu ortamda bir noktadan bir noktaya erişim neredeyse ışık hızında meydana gelmektedir.
- Işık hızına yaklaşan bir hızda harekât kabiliyetine imkân tanıdığından aynı hızda bir tehdit riskine yol açar.
- Kara, hava, deniz ve uzay ortamlarının tamamında harekât imkânı sağlar.
- Coğrafi veya siyasi olarak çizilen sınırlarla kısıtlı değildir. Coğrafyadan bağımsız erişim ve harekât imkânı sağlar.

Siber uzayın gelişmesiyle birlikte sosyal gerçekliğin en önemli iki katmanı olan mekân ve zaman bağıntısı değişmeye başlamıştır. Fiziksel uzaklıklar ve bilgi aktarımı için gereken zaman internetin oluşturduğu hızla kısalmıştır. Bu yetenek kısa sürede politik, askeri ve ekonomik alanlarda kullanılmaya başlanmıştır. Bankalar, borsalar ve her türlü ticari yapı faaliyetleri, yeni teknolojiyi kullanarak daha geniş alanda hizmet vermeye başlamıştır.[177] Askeri alanda da yoğun olarak bu alandan faydalanılmaktadır. Örneğin; Körfez Savaşında bilgisayarlar aşağıdaki maksatlarla kullanılmıştır;[178]

- Bilgisayarlar, Koalisyon Güçleri ordularının Suudi çölündeki hareketlerini organize etmiş ve yönlendirmiş,
- Binlerce uydu fotoğrafı ve elliden fazla uydu üzerinden gemilerin saatler süren elektronik haberleşme trafiğini ayarlamış,
- Uçaklar, pilotsuz uçaklar ve helikopterlerin uçuşuna yardımcı olmuş,
- Bombaları ve füzeleri, hatta top mermilerini yönlendirmiş,
- Iraklıların radarlarını karıştırıp hedef bilgisayarlarını bozmuş,
- Savunma bakanlığı adına olduğu kadar CNN TV için de uydu antenleri ve mesaj alışverişini idare etmiş,
- Silah platformları ve teçhizatlarının izini sürmüş,
- Bölgedeki silahların dökümünü çıkarmış,
- Can kayıplarını ev adreslerine kadar araştırmıştır.

2.2.4. Hacker Kavramı

[177] Salih Bıçakçı, ***a.g.e.***, s.3.
[178] Barış Gürsoy, "Uluslararası Güvenliğin Bir Boyutu Olarak Askeri Alanda Devrim Tartışması", ***Avrasya Dosyası Dergisi***, Cilt: 9, Sayı: 2, 2003, 127-141, s.140.

İngilizcesi “hacker” olan kelimenin, Türk Dil Kurumu tarafından Türkçe karşılığı “bilgisayar korsanı” olarak tanımlanmıştır. Bilgisayar korsanının anlamı ise; bilgisayar ve haberleşme teknolojileri konusundaki bilgisini gizli verilere ulaşmak, ağlar üzerinde yasal olmayan zarar verici işler yapmak için kullanan kimsedir.[179]

Bilgi hırsızlığı, başka bilgisayarlara sızma, “hack” etme işlemleri, gelişmiş bilgisayarlara ve modem – telefon hattı gibi erişim kanallarına sahip “uzmanlar” tarafından önce sızılacak bilgisayarın işletim sisteminde veya yazılımında bir açıklık, zayıf nokta bulunarak yapılmaktadır. Şayet sızılacak bilgisayar şifre ile korunuyorsa, şifreyi kendi geliştirdikleri programlarla kırarak ya da şifreyi bir şekilde öğrenerek, karşı tarafın bilgisayarına girilir. Ayrıca bilgi elde etmek isteyenler; dinleme istasyonları, telefonlara konulan çiplerden de faydalanmakta ve bu işlemler için bilgisayarın yardımına başvurmaktadır.[180]

Örneğin; Küçükçekmece'de, temin ettiği kimlik bilgileriyle sahte belgeler düzenleyerek bankaları 2 milyon TL dolandırdığı ileri sürülen bir hacker gözaltına alınmıştır. Yapılan araştırmada Sosyal Güvenlik Kurumu ve internetten vatandaşların kimlik bilgilerine ulaşarak sahte kimlikler çıkardığı tespit edilen Murat Ş.'nin, kredi talebiyle bankaları dolandırdığı iddia edilmiştir.[181] Hacker Murat Ş. İnterneti kullanarak birçok vatandaşın kimlik bilgilerine ulaşabilmiştir.

Yazılımları yazan veya donanımları tasarlayan elemanlar bazen hata yaparak, açık bir kapı bırakabilmekte veya hatalı bir program satırı yazabilmektedirler. Bundan yararlanan hacker da gizlice kapalı sistemlere sızabilmektedir. Örneğin; ABD’de şirketlerdeki fotokopi makineleri bile ağlarla birbirine bağlıdır. Şirketlerin içindeki fotokopi makinelerine şifre yerleştiren rakipleri kopyası çekilen tüm bilgilere anında ulaşabilir. Hatta uzaktan kumandayla makineye kısa devre yaptırıp ofisinizde kısa devre bile yaptırabilirler. Hackerlar böyle bir eylem yaptığı zaman, siber suçlu olmaktadırlar. [182]

Uluslararası alanda yukarıda örnekleri verilen siber suçlarla mücadelede çeşitli çalışmalar yapılmaktadır. Örneğin; Türkiye, 10 Kasım 2010 tarihinde Uluslararası

[179] Türk Dil Kurumu Resmi İnternet Sayfası, http://www.tdk.gov.tr/index.php?option=com_gts&arama=gts&guid=TDK.GTS.5305e5b5960b23.51272901, (Erişim tarihi: 11.02.2014).
[180] Sait Yılmaz, ***a.g.e.***, s.435.
[181] İki milyonluk vurgun yapan hacker yakalandı, http://www.sabah.com.tr/Yasam/2013/03/04/2-milyonluk-vurgun-yapan-hacker-yakalandi, (Erişim tarihi: 12.02.2014).
[182] Richard A. Clarke ve Robert K. Knake, ***a.g.e.***, s.44-45.

Siber Suç Sözleşmesi'ni imzalayarak anlaşmaya taraf olmuş ancak yürürlüğe girmesi 2 Mayıs 2014'te Resmi Gazete'de yayınlanmasıyla gerçekleşmiştir. Uluslararası Siber Suç Sözleşmesi'nin Türkiye'de yürürlüğe girmesi için yaklaşık 4 yıl beklenilmiştir.

Günümüzde siber alanda saldırı ya da bilgi hırsızlığı gerçekleştirmek isteyen bir bireyin yüksek oranda teknik bilgiye sahip olması gerekmemekte, bu tür araçlara birkaç fare tıklaması ile ulaşılabilmektedir. İnternet üzerinden indirilip kullanılabilen bu tür araçların artmasıyla birlikte güvenlik bariyerleri de yetersiz kalmaya başlamıştır.[183]

Windows 95 içinde 10 milyondan az kod satırı vardı. Windows XP içindekilerin sayısı 40 milyon, Windows Vista'da ki kod sayısı ise 50 milyondan fazladır. On yılda kod satırları sayısı beş katına çıkmıştır. Kod yanlışları da aynı oranda çoğalmıştır. O yanlışların çoğu hackerlara yazılımlara müdahale imkânı sağlamaktadır.[184]

Hacker'lar genel olarak üç gruba ayrılmaktadır;[185]

1. Siyah Şapkalılar: Her türlü programı, siteyi veya bilgisayarı güvenlik açıklarından yararlanarak kırabilen ve sistemleri kullanılamaz hale getiren, bilgileri değiştiren veya gizli bilgileri çalanlardır.
2. Beyaz Şapkalılar: Beyaz şapkalılar da her türlü programı, siteyi veya bilgisayarı güvenlik açıklarından yararlanarak kırabilen fakat kırdığı sistemin açıklarını sistem yöneticisine bildirerek o açıkların kapatılmasını ve zararlı kişilerden korunmasını sağlamaktadırlar.
3. Gri Şapkalılar: Yasallık sınırında saldırı yapan, iyi veya kötü olabilen hackerlardır.

2.2.5. Siber Saldırı Kavramı

Siber uzaydaki her türlü veri, programın değiştirilmesi, bozulması, sahtesinin üretilmesi, kesintiye uğratılması ya da yok edilmesi siber saldırı olarak adlandırılmaktadır. Siber saldırılar aşağıdaki gibi sınıflandırılabilir:[186]

---

[183] Adem Kaya, ***Siber Güvenliğin Milli Güvenlik Açısından Önemi, Savunma Bilimleri Enstitüsü***, Kara Harp Okulu, Ankara, 2012, s.16.
[184] Richard A. Clarke ve Robert K. Knake, ***a.g.e.***, s.50.
[185] Hasan Çifci, ***a.g.e.***, s.229-230.
[186] Lech J. Janczewski and Andrew Michael Colarik, ***Cyber warfare and cyber terrorism,*** IGI Global, London, 2008, p.13-25.

- Elektronik posta eklentileriyle virüs saldırıları,
- Kamu hizmetlerinin görülmesini sağlayan bilgisayar sistemlerinin aşırı yüklenmesini sağlayarak çalışamaz hale getirilmesi,
- Dezenformasyon ya da propaganda yapmak maksadıyla devletlerin veya ticari kuruluşların internet sayfalarının bozulması,
- Bilgisayar sistemlerine yetkisiz girişler yapılarak bilgilerin elde edilmesidir.

Siber saldırılar verilere ya da kontrol sistemlerine olan saldırılar olmak üzere iki temel şekilde meydana gelmektedir. Bilginin çalınması veya bozulması sıklıkla karşılaşılan verilere yönelik eylem türlerindendir. Kontrol sistemleriyle ilgili olanlar ise bir fiziksel altyapıyı kullanılmaz hale getirme ya da yanlış yönlendirmeyi amaçlamaktadır.[187]

Siber uzayda yapılan saldırılar, saldırıyı gerçekleştirenlerin motivasyonlarına, kimliklerine ve amaçlarına göre çeşitli adlar almaktadır. Bu konuda genel kabul görmüş tanımlamalar şunlardır; politik nedenlerle toplumda endişe yaratmak amacıyla terör örgütlerince ya da kimliği bilinmeyen kişilerce yapılan eylemler siber terör, kişisel kazanç sağlamak amacıyla toplumsal düzeni ve huzuru tehdit eden faaliyetlerde bulunmak ise siber suç, devletlerin aralarındaki mücadeleyi veya çatışmayı siber ortama taşımaları ise siber savaş olarak adlandırılmaktadır.

Siber saldırıda uygulanan yöntemlerden bazıları şunlardır;[188]

- Virüs,
- Truva atı,
- Hizmet Dışı Bırakma,
- Aldatma,
- Mahremiyet ve Gizlilik İhlali,
- Yetkisiz Giriş,
- Phishing,
- Spam.

Siber uzayda faaliyet gösteren istihbarat örgütleri de yukarıda sayılan yöntemlerin birçoğunu kullanarak faaliyetlerine devam etmektedir. Siber uzayda saldırı yapabilmek için öyle çok pahalı ve karmaşık silah sistemleri

[187] Haydar Çakmak ve Cenker Korhan Demir, ***a.g.m.***, s.30.
[188] Sait Yılmaz ve Olay Salcan, ***a.g.e.***, s.56-61.

gerekmemektedir. Bazen bir bilgisayar ve bir e-posta ile karşıdaki sisteme tahmin edilemeyecek kadar büyük boyutlarda zarar vermek mümkün olmaktadır.[189]

Bir ülkenin altyapısına karşı yapılacak siber saldırı güç şebekesini haftalarca devre dışı bırakabilir. Boru hatları petrol ürünlerini ve gazı iletemez hale gelir. Trenler kalkamaz, uçaklar da yerde kalır. Bankalardan para çekilemez, dağıtım sistemi çöker ve hastaneler kısıtlı kapasiteyle çalışmak zorunda kalır. Sivil nüfus karanlık ve soğuk evlerde, gıda, para ve tıbbi bakımdan yoksun, ne olup bittiği konusunda haber alamaz hale gelir. Bunun sonunda yağmalamalar ve bir suç dalgası da meydana gelebilir.[190] Siber saldırılardan bir kısmını aşağıda ayrıntılı olarak ele alalım.

2.2.5.1. Bilgisayar Virüsleri

Virüsler kullanıcının isteği dışında bilgisayara yüklenerek çalışan oldukça etkili bir programdır. Diğer bilgisayarlara bulaşma ve kendi kendine çoğalma özelliğinin biyolojik virüslere benzemeleri nedeniyle virüs olarak adlandırılmaktadırlar. Virüsler, internet sitelerinden indirilen dosyalardan, e-postalardan veya bir depolama aygıtından (CD, DVD, harici bellek vs.) bulaşabilirler. Veri kayıplarına ve hasarlara neden olabilirler.[191] Virüslerle diğer zararlı yazılımlar arasındaki en önemli fark, virüslerin başlatıcı unsur olarak insan etkileşimine ihtiyaç duymasıdır. Aktif hale gelebilmesi için virüslü program, dosya veya e-postanın kullanıcı tarafından çalıştırılması, okunması ya da indirilmesi gerekmektedir. Virüsler sistem bileşenlerine göre; dosya virüsleri, önyükleme (boot) virüsleri, makro virüsler ve betik (script) virüsler olarak sınıflandırılabilirler.[192]

Virüslerle ilgili yaşanmış birçok örnek bulunmaktadır. Örneğin; İran'ın nükleer tesislerini hedef aldığı iddia edilen Stuxnet virüsü Tahran'ı alarma geçirmiştir. İranlı yetkililer, enerji santralleri, barajlar ve sanayi birimleri gibi altyapı tesislerinin sistemlerini hedef alan ilk kötü amaçlı yazılım olan Stuxnet virüsünün ülke genelinde 30 bin sanayi bilgisayarını etkilediğini açıklamıştır. Iran Daily gazetesine göre, Sanayi Bakanlığı bilgi teknolojileri konseyi başkanı Mahmud Liayi, Stuxnet'in şu ana kadar İran'da 30 bin IP adresini etkilediğini belirtmiştir. Öte yandan, yazılımı analiz

[189] Hasan Çifci, ***a.g.e.***, s.23.
[190] Richard A. Clarke ve Robert K. Knake, ***a.g.e.***, s.131.
[191] Sait Yılmaz ve Olay Salcan, ***a.g.e.***, s.56.
[192] Gürol Canbek ve Şeref Sağıroğlu, ***Bilgi ve Bilgisayar Güvenliği: Casus Yazılımlar ve Korunma Yöntemleri***, Ankara, 2006, s.176-177.

eden Alman bilgisayar güvenliği araştırmacısı Ralph Langner, yazılımın belirsiz nedenlerden dolayı faaliyete geçmesi ertelenen Buşehr nükleer santralini hedef aldığını belirtmiştir.[193]

2.2.5.2. Truva Atı

Truva atı, direk bir saldırı veya bir virüs vasıtasıyla hedeflenen sistemlere yerleştirilen, kötü niyetli yazılım programıdır. Kendini zararsız bir program gibi gösterir. Çalıştığında verileri silebilir veya bozabilir. Şifreyi elde edebilir veya uzaktan kontrol imkânı veren erişimi sağlar.[194] Truva atlarının iki türü vardır. Birincisi, kullanışlı bir programın bir hacker tarafından tahribata uğratılıp içine zararlı kodlar yüklenip program açıldığında yayılan türüdür. Örnek olarak çeşitli hava durumu uyarı programları, bilgisayar saati ayarlama yazılımları ve paylaşım programları verilebilir. Diğer türü ise bağımsız bir program olup başka bir dosya gibi görünmektedir. Örnek olarak oyun dosyası gibi kullanıcıyı aldatmaya yönelik bir takım yönlendiricilerle programın harekete geçirilmesine ihtiyaç duyulmaktadır.[195]

Örneğin; Türkiye'de 2013 yılında iki ay süresince binlerce bilgisayar kullanıcısının e-posta adresine veya mobil cihazına gelen sahte telefon faturaları ve kredi kartı ekstrelerinde adeta patlama yaşanmıştır. Siber suçlular, fatura görünümündeki sahte e-postalarla "Hesperbot" adlı bankacılık truva atını bilgisayarlara yaymışlardır. Siber suçlular, bu uygulamada bilgisayar ve akıllı telefon kullanıcılarının merak ve şaşkınlıklarından faydalanmışlardır. E-postalara, mümkün olmayan bir borcun yazılı olduğu faturalar gelmiştir. Refleks olarak insanlar şaşırmış ve e-maillerini açmışlardır. İşte bunun yapıldığı an truva atı bilgisayara bulaşmakta ve sistem saldırılara açık hale gelmektedir.[196]

2.2.5.3. Hizmet Dışı Bırakma

[193] Dünya Stuxnet tehdidine karşı mücadele veriyor,
http://www.hurriyet.com.tr/planet/15876929.asp,
(Erişim tarihi: 08.04.2014).
[194] Sait Yılmaz ve Olay Salcan, ***a.g.e.***, s.57.
[195] Kötü Virüs,
http://tr.wikipedia.org/wiki/K%C3%B6t%C3%BC_vir%C3%BCs,
(Erişim tarihi: 03.04.2014).
[196] Türkiye'yi sahte fatura fırtınası vurdu,
http://www.dha.com.tr/turkiyeyi-sahte-fatura-firtinasi-vurdu_555315.html,
(Erişim tarihi: 08.04.2014).

Hizmet dışı bırakma bir bilgisayar sisteminin ya da web sitesinin işlemesini, hizmet vermesini engellemek amacıyla yapılan saldırılardır. Hizmet dışı bırakma saldırısı şöyle işler: Zombi adı da verilen casus programlarla sisteme sızan saldırganlar, sunuculara çok sayıda veri göndererek, sunucuların dolayısıyla web sitelerinin çökmesini sağlar. "Dağıtılmış Hizmet Dışı Bırakma"nın işleyişi "Hizmet Dışı Bırakma"nın benzeridir. Tek farkı saldırının birden fazla noktadan yapılmasıdır.[197]

Herhangi bir saldırgan ele geçirdiği bilgisayarlar vasıtasıyla bir siteye kolayca hizmet dışı bırakma saldırısı yapabilmektedir. Yapılan bu saldırı sitenin normal takipçilerine cevap verememesine yol açmaktadır. Bu saldırılar hem prestij kaybına hem de maddi kayıplara neden olmaktadır. Örneğin; 2009 yılında Twitter'ın, 2012 yılında Türk Hava Yolları'nın sitelerine yapılan ve saatlerce sistemlerin kapalı kalmasına yol açan saldırılar hizmet dışı bırakma saldırılarıdır. 2012 yılında Türkiye'de 10'dan fazla kamu kurumu da bu saldırılara maruz kalmış ve ciddi prestij kaybı yaşanmıştır.[198]

2.2.5.4. Solucanlar

Zararlı programlardan bir diğeri de solucanlardır. Aslında virüs olmakla birlikte hedefleri bakımından virüslerden ayrılırlar. Virüsler, bağlantı kurulan bilgisayarın dosyalarına süratle yayılırken, solucanlar ise ağ üzerindeki diğer bilgisayarlara hızla yayılma amacı taşımaktadırlar. Kısaca solucan bağımsız kendi kendine çoğalabilen, ağ üzerinde bir bilgisayardan diğerine yayılma yollarını araştıran ve yayılan bir programdır.

Solucanlar genel olarak kullanıcı müdahalesi olmadan yayılmakta ve kendilerinin birebir kopyalarını ağdan ağa dağıtmaktadırlar. Kurtçuklar yayılmak için bir taşıyıcı programa veya dosyaya ihtiyaçları olmadığı için sistemde bir tünel de açabilmekte ve başkasının, bilgisayarınızın denetimini uzaktan eline geçirmesine olanak sağlayabilmektedir.[199]

---

[197] Barış Baraz vd.,***Büro Teknolojileri***, Anadolu Üniversitesi Yayınları, Eskişehir, 2013, s.146-147.
[198] Siber Saldırılara Karşı Savunma Aracı Geliştirildi,
http://www.tubitak.gov.tr/tr/haber/siber-saldirilara-karsi-yerli-savunma-araci-gelistirildi,
(Erişim tarihi: 08.04.2014).
[199] Virüs, solucan ve Truva atı nedir?,
http://www.bilgiportal.com/zemin/yazi/1358/virus-solucan-ve-truva-ati-nedir,
(Erişim tarihi: 05.04.2014).

Solucan işletim sistemleri ve programların güvenlik açıklarını kullanarak önce bir bilgisayardan başlar, sonra ağdaki diğer bilgisayarlar ile iletişim kurduğu anda kendini o bilgisayara da transfer eder. Saniyeler içinde milyonlarca bilgisayara bulaşma kabiliyeti vardır. İnternet aracılığıyla dağılan ve o ana kadar en büyük hasara neden olan en eski solucan Morris İnternet Worm'dur.[200] Diğer bir büyük hasara sebep olan örnek ise; Dünyanın dört bir yanında etkili olan, "SQL slammer" adlı bilgisayar solucanıdır. Dünya'da internet erişimini güçleştirmiştir. Amerika, Asya ve Avrupa'da bilgisayarları etkileyen solucan nedeniyle, birçok ülkede internet erişiminde sorunlar yaşanmıştır. Solucan Amerika Birleşik Devletleri'nde otomatik para çekme makinelerini bile bozmuştur.[201] Diğer örnekte ise; 2000 yılında yayılan Love Bug solucanı ABD Massachusetts Eyaletinde e-posta hizmetinin kapatılmasına neden olmuştur. Milyonlarca bilgisayara zarar veren Love Bug'ın 8.7 Milyar dolar zarara neden olduğu hesaplanmaktadır.[202]

2.2.5.5. Klavye Kaydediciler

Klavye kaydedici programlar Truva atıyla var olurlar. Klavye kayıtçı basitçe klavyeden yapılan her dokunuşu kaydeden ve bu kayıtları kişisel bilgileri çalmak isteyen kişilere gönderen programlardır. Bu kişiler istedikleri zaman yazılan her türlü bilgiyi görebilirler. Bu yöntemle e-posta şifresi, kredi kartı numarası gibi önem taşıyan bilgiler çalınabilir.[203]

Klavye kaydediciler küçük programcıklardır ancak bunlar sadece yazılım olarak değil donanım olarak da var olabilmektedirler. Kullanıcılar ve sistemler klavye kaydedicilerin farkına varamamaktadırlar. Bu tür klavye hareketlerini kaydeden donanımlar fiziksel olarak klavye ile bilgisayar arasına monte edilmekte ve bilgisayar kasasının arka kısmına gizlenmektedir. Yapılan araştırmalarda ne kullanıcılar, ne de sistemler bu kaydedicileri fark etmiştir. Hazırlanmaları ve kurulumları çok basit olan bu tür cihaz ve yazılımların varlıklarına karşı dikkatli olunması gerekmektedir.[204]

---

[200] Hasan Çifci, ***a.g.e.***, s.151.
[201] Solucan virüs fena vurdu,
http://arsiv.ntvmsnbc.com/news/198871.asp,
(Erişim tarihi: 09.04.2014).
[202] Stephen Haag and Maeve Cummings, ***Management Information Systems For The Information,*** 6 th Edition, New York, 2007, p.393.
[203] Barış Baraz vd.,***a.g.e.***, s.146.
[204] Keyloggers: The Overlooked Threat to Computer Security,
http://www.keylogger.org/articles/kishore-subramanyam/keyloggers-the-overlooked-threat-to-computer-security-7.html,
(Erişim tarihi: 09.04.2014).

2.2.5.6. Arka Kapılar

Arka kapılar, bilgisayar korsanlarının hedef bilgisayar ya da ağ sistemlerine uzaktan yetkisiz erişim yapmalarını sağlayan zararlı yazılımlardır. Arka kapıların en önemli özelliği, sisteme ilk kez sızılırken eklenen program sayesinde aynı ortama kolaylıkla giriş imkânı sağlamasıdır. Bu tarz yazılımlarda en sık kullanılan yöntem, hedef sistemde dinleme ajanı yerleştirilmiş bir kapıyı açık tutmaktır.[205] Arka kapı, sadece saldırgan tarafından bilinen, normal kimlik kontrol mekanizmalarını kullanmadan karşıdaki sisteme gizli bir kanalla ulaşmayı sağlayan yöntem veya giriş noktasına verilen isimdir.[206]

Arka kapılar genellikle işletim sistemi ya da paylaşım yahut bedava yazılımlar içerisinde bulunurlar. Arka kapılar ayrıca elektronik posta veya diğer kötü amaçlı yazılımlar üzerinden de yayılabilir. Bazı arka kapılar, var olan ağları işletmek için haberci uygulamalarının dış görünüşüne benzetilerek tasarlanabilir. Bir sohbet programı olan IRC(Internet Relay Chat) ağı bu amaçla yaygın bir şekilde istismar edilmiştir.[207]

2.2.5.7. Casus Yazılımlar (Spyware)

Casus yazılımlar çeşitli amaçlarla kullanıcı bilgisini ve faaliyetlerini izleyen, toplayan ve nihayetinde bir kuruma/şirkete vb. ileten yazılımlardır.[208] Casus yazılımlar vasıtasıyla toplanan veriler oldukça geniş bir alana yayılmaktadır. Kullanıcının internette yaptıkları, kullanıcının e-postalarından kimlik bilgilerine kadar pek çok veri casus yazılımlar vasıtasıyla elde edilebilmektedir.

Casus yazılımların siber uzayda dağılmasında kullanılan yöntemler şunlardır:[209]

- İşletim sisteminde "arka kapı (backdoors)" gibi programların bulunması,

[205] Gürol Canbek ve Şeref Sağıroğlu, ***a.g.e.***, s.184.
[206] Hasan Çifci, ***a.g.e.***, s.154.
[207] Taner Altunok ve Filiz Katman, "Siber Tehdit Altyapısı ve Araçları", ***Suç, Terör ve Savaş Üçgeninde Siber Dünya***, Barış Platin Kitabevi, Ankara, 2009, 23-54, s.73.
[208] Taner Altunok ve Filiz Katman, ***a.g.m.***, s.73.
[209] Gürol Canbek ve Şeref Sağıroğlu, "Casus Yazılımlar: Bulaşma Yöntemleri ve Önlemler", ***Gazi Üniv. Müh. Mim. Fak. Dergisi***, Ankara, 2008, Cilt: 23, No: 1, 165-180, s.167.

- Genellikle ücretsiz dağıtılan ekran koruyucular, oyunlar ve dosya paylaşım programlarının içinde gizlenmesi,
- Kök kullanıcı takımları (rootkit) yardımıyla kendi işlem ve dosyalarını saklayarak sistemde çalışması,
- E-postaya ekli dosyanın açılması ya da e-postada önerilen bir web adresine girilmesi,
- Bilgisayarda giderilmemiş açıklıklardan yararlanmadır.

Casus yazılımlar geçmişte etkin olarak kullanılmış ve halende kullanıldıkları değerlendirilmektedir. Örneğin; Kasım 2009'da başlayan ve Şubat 2011 tarihinde açığa çıkarılan petrol ve enerji firmalarından veri çalmayı amaçlayan siber casusluk saldırılarıdır. Öncelikle, hedef alınan şirketin web sitesindeki açıklık kullanılarak içeri girilmekte, ele geçirilen bilgisayarlara casus yazılım yüklenmekte ve bu yolla şirketteki diğer bilgisayarlara da ulaşarak veri çalınmaktadır.[210] Burda casus yazılımı hedef bilgisayara ulaştırmak amacıyla web sitesi açıklığından faydalanılmıştır. Bu sadece yöntemlerden birisidir. Siber uzayda yapılabileceklerin limiti arttıkça yöntemlerde artmaktadır.

2.2.5.8. Bot Ağı (Botnet)

Botnetler organize edilmiş saldırıya ya da verilen emri yerine getirmeye planlanmış sistemlerdir. Botnet'ler bot master adı verilen kişiler tarafından kurulurlar. Bot masterlar yazdıkları program ya da web sayfaları aracılığıyla zararlı yazılımlarını siber uzayda farklı bilgisayarlara yayarlar. Bu yazılımları kullanmaya başlayan bilgisayarlar farkında olmadan botnet içine dahil olurlar. Bot master'ın emrini bekleyen bu bilgisayarlara "zombi" ismi verilir.[211]

Botnet saldırılarının temel özelliği, sadece tek bir saldırgan tarafından sayısı yüzleri, binleri hatta milyonları bulan bilgisayarların, kullanıcılarının haberi dahi olmadan istenilen eylem doğrultusunda yönlendirilebilmesidir. Bir milyon üyesi olan bir köle bilgisayar ağı, Fortune 500'deki tüm şirketleri internet üzerinde çalışamaz hale getirebilmekte, 10 milyon üyesi olan bir köle bilgisayar ağı ise, büyük bir batılı devletin tüm iletişim altyapısını felç edebilmektedir.[212]

---

[210] Hasan Çifci, ***a.g.e.***, s.176.
[211] Salih Bıçakçı, ***a.g.e.***, s.40.
[212] Hasan Çifci, ***a.g.e.***, s.155.

Botnet'in parçası olan bir bilgisayar suç unsuru olan dosya ve görüntülerin yayılmasında, istenmeyen elektronik posta olarak tanımlanan spam faaliyetlerinde, şahsi bilgilerinizin, internet ve banka hesaplarınıza ait bilgi ve şifrelerin ele geçirilmesinde kullanılabilmektedir. Ele geçirilen bu bilgiler de sizin adınız ve paranız kullanılarak çok ciddi suçların işlenmesine aracılık edebilmektedir.[213]

2.2.5.9. Aldatma (IP Snoofing)

Bilgisayarlar arasındaki bağlantı çeşitli protokoller aracılığıyla sağlanmaktadır. Bu protokoller aracılığıyla başka bir bilgisayara bağlanıldığında bağlanan bilgisayar kendi kimliğini karşı tarafa tanıtır. Bağlanılan bir bilgisayara gerçek IP adresinin gösterilmemesi yani asıl kimliğin gizlenmesine IP spoofing (Aldatma) denir.[214] İnternet Protokolü'nün kısaltması olarak kullanılan IP, bir bilgisayar adresini gösterir. İki bilgisayar birbirine güvendiğinde, diğer bilgisayar sistemlerinde bulunmayan hassas bilginin erişimine izin verirler. Hassas bilgilere erişim hakkını kazanan güvenilen bilgisayar gibi davranan saldırgan, bu güvenden faydalanır veya imtiyazlı programlar kullanarak saldırıya uğramış bilgisayarın kontrolünü ele geçirmektedir.[215]

2.2.5.10. Yemleme

Yemleme(phishing), internet üzerinde güvenilen elektronik iletişim kaynaklarından birinin yerine geçerek kullanıcıların o kaynakla irtibata geçmesini sağlama ve onlardan kullanıcı adı, parola, kredi kartı bilgileri ve diğer özel bilgileri çalma eylemidir.[216] Diğer bir ifadeyle, e-posta veya bunun gibi bilgi girilmesi gerektiren bir kuruluşun web sayfasının bir kopyasının yapılıp kullanıcının hesap bilgilerini çalmayı amaçlamaktadır.[217]

Phishing saldırısı çeşitli basamaklardan oluşmaktadır.

---

[213] Alana Maurushat, "Zombie Botnets", ***Scripted***, 2010, Volume 7, Issue 2, 370-383, p. 371.
[214] IP spoofing,
http://www.cclub.metu.edu.tr/nenedir/Ip+spoofing,
(Erişim tarihi: 09.04.2014).
[215] Sait Yılmaz ve Olay Salcan, ***a.g.e.***, s.56.
[216]How Phising Works,
http://computer.howstuffworks.com/phishing.htm,
(Erişim tarihi: 12.03.2014).
[217] Sait Yılmaz ve Olay Salcan, ***a.g.e.***, s.59.

- İlk olarak saldırgan, hedeflediği kurbanlara ait e-posta adreslerini çeşitli yöntemler (tahmin, açık kaynak araştırması, sızdırma vs.) kullanarak öğrenir.
- İkinci aşamada saldırgan gerçek web sitesine benzeyen sahte bir adresten müşteriye e-posta gönderir ve bazı işlemlerde bulunmasını ister. (Örneğin, müşterinin hesabının bulunduğu bankanın web sitesi görünümündeki sahte bir e-postayı müşteriye göndererek, kimlik bilgileri, şifre vb. bilgileri güncellemesini isteyebilir.)
- Gönderilen e-postanın içeriğine göre; alıcı istenen işlemi ya da güncellemeyi yapabilir, zararlı içerik bulunan dosyayı açabilir veya istenilen web sitesine bağlanabilir.

Başarıya ulaşan saldırgan hedeflediği alıcı ya da müşteriye ait kişisel bilgileri kullanarak dolandırıcılık işlemini gerçekleştirir.[218]

2.2.5.11. Koklayıcı (Sniffers)

Koklayıcılar, ağ üzerinde bulunan IP paketlerini taramak maksadıyla kullanılan donanım ve yazılımlardır. Tüm ağ trafiğini dinleyerek kaydedebilirler. En önemli özellikleri veri paketlerinde bulunan, kimlik, şifre vb. hassas bilgileri, paket içeriğini tarayarak bulabilmeleridir. Veri paketlerinin aktif ağ cihazları kullanılarak sadece istenilen adrese gönderilmeleri, koklayıcıların bu paketleri incelemesini engelleyebilir.[219] Bir sniffer programı, saldırgan tarafından daha sonra kullanılmak maksadıyla bilginin birçok çeşidini kaydedebilir. Saldırganların birçoğunun özel ilgi alanı, uzakta olan bilgisayarlara bağlantı için gerektiğinde kullanılan şifre ve kullanıcı adlarıdır. Bugün saldırganların ellerinde, dünya üzerindeki birçok şirket, kamu siteleri ile üniversitelerden yüz binlerce kullanıcı ad ve şifreler vardır.[220]

2.2.5.12. İstenmeyen E-posta (Spam)

İnternet üzerinde aynı e-postanın yüksek sayıdaki kopyasının, bu tip bir mesajı alma talebinde bulunmamış kişilere gönderilmesi Spam olarak adlandırılır. Spam

[218] Educating Your Customers on ID Theft, Phishing and eCrime, http://www.antiphishing.org/resources/Educate-Your-Customers/, (Erişim tarihi: 09.04.2014).
[219] Gürol Canbek ve Şeref Sağıroğlu, ***a.g.e.***, s.207.
[220] Sait Yılmaz ve Olay Salcan, ***a.g.e.***, s.59.

çoğunlukla ticari reklam şeklinde olup, bu reklamlar sıklıkla güvenilmeyen ürünlerin, çabuk zengin olma kampanyalarının, yarı yasal servislerin duyurulması amacına yöneliktir.[221]

Sayıları bazen milyonları bulabilen istenmeyen e-postalar yarattıkları yoğun mesaj trafiği sebebiyle ağ problemlerine neden olabilmektedirler. Örneğin, New York'ta yaşayan Anthony Greco spam mesajları gönderebilmek için Ekim-Kasım 2004 tarihinde MySpace.com'da yanıltıcı binlerce hesap yaratmıştır. Greco, bu hesapları kullanarak, mortgage kampanyaları ve yetişkin içerikli sitelerinin reklamlarını ihtiva eden 1,5 milyondan fazla spam mesajı göndermiştir. Gelen yoğun spam mesajlarını silmek ve gelecek saldırılara önlem için alınan koruyucu tedbirler MySpace şirketine 5.000 dolara mal olduğu belirtilmektedir.[222]

2.2.6. Siber Terörizm Kavramı

Siber terörizm, bilgisayar ağlarını bozmaya yönelik kasıtlı ve geniş kapsamlı eylemler dâhil olmak üzere, terör eylemlerinde internet tabanlı saldırıları ve internete bağlı kişisel bilgisayarları kullanmaktır.[223] Hasan Çifçi'ye göre geniş anlamda ise, can ve mal tehdidine ilave olarak, sosyal, dini, ideolojik, politik veya başka amaçlarla bilgisayar ağlarına yapılan saldırılar da siber terörizm kapsamına girmektedir.[224] Diğer bir tanıma göre siber terörizm; siyasi bir motivasyonla önceden planlanan, neticede toplumlarda korku ve endişe yaratmayı hedefleyen bilgisayar ve bilgisayar sistemleri ile internet teknoloji ve imkânlarına yönelik yapılan eylemlerdir.[225] Bu konuda genel kabul görmüş siber terör tanımlaması olarak ise; politik nedenlerle toplumda endişe yaratmak amacıyla terör örgütlerince ya da kimliği bilinmeyen kişilerce yapılan eylemlere siber terör denilmektedir.

Bilişim teknolojilerinde ortaya çıkmış olan her yenilik sıradan bilgisayar kullanıcılarına olduğu kadar terörist örgütlere de fayda sağlamaktadır. Komuta ve kontrolün geniş bir çevreye yayarak ve iletişimde sınırsız fırsatlar ile terör örgütleri

---

[221] Spam nedir?,
http://spam.nedir.com/,
(Erişim tarihi: 09.04.2014).
[222] Sait Yılmaz ve Olay Salcan, ***a.g.e.***, s.60-61.
[223] Cyberterrorism,
http://en.wikipedia.org/wiki/Cyberterrorism,
(Erişim tarihi: 12.02.2014).
[224] Hasan Çifci, ***a.g.e.***, s.6.
[225] Haydar Çakmak ve Cenker Korhan Demir, ***a.g.m.***, s.39.

interneti silah gibi kullanabilmektedirler.[226] Bu nedenle terör örgütleri de internet üzerinde kendi amaçları doğrultusunda çalışmalar yapmaktadır. İnternetin sahip olduğu potansiyel nedeniyle gelecekte birçok terör örgütü bu alanı aktif olarak kullanabilecektir.

Timothy L. Thomas "El Kaide ve İnternet: Siber Planlamanın Tehlikesi" isimli makalesinde terör örgütlerinin, interneti aşağıdaki özellikleri sebebiyle kullanmayı seçtiğini belirtmiştir. Bunlar;[227]

- Tüm militan profillerinin toplanmasını sağlaması,
- İnterneti gerçek bir ideolojik silah olarak kullanabilmesi,
- Yanlış bilgilendirme yaparak kamuoyunu yanıltma sağlanabilir,
- İnternet çok kolaylıkla para ve fon toplayarak örgüt için finansal kaynak sağlayabilmektedir,
- İnternet dışarıdan kontrol edilebilen ve emir verilebilen bir yapıya sahiptir,
- İnternet terör örgütlerine sempatizan kazanımını kolaylaştırır,
- İnternet potansiyel hedefler için bilgi toplanmasını sağlar,
- İnternet saldırının planlandığı yer ve hedef arasında uzaklık imkânı sağlar,
- İnternet verilerin değiştirilmesine imkân sağlar,
- İnternet gizli mesajların gönderimini kolaylaştırır,
- İnternet terör gruplarına az kaynakla dünyanın her yerinde propagandasını yapma imkânı sağlar,
- İnternet yasal kurallar ile avantaj sağlar,
- İnternet grup, diaspora veya hackerları bir eylem için organize edebilir.

Güvenlik uzmanları tarafından terör gruplarının basit, gelişmiş ve kompleks olarak üç düzeyde siber alanda faaliyette bulunabildikleri belirtilmiştir. Basit ve yapılandırılmamış düzeyde, terör örgütleri temel hacker becerilerine sahiptir. Başkalarından profesyonel yardım almaktadırlar. İleri düzeydekiler daha sistematik saldırılar yapabilmekte, hackerlama için araç oluşturabilmektedirler. En tehlikeli olarak görülenler kompleks ve koordineli yapıdaki üçüncü gruptur.[228] Geçmişe

[226] Taner Altunok ve Aşkın İnci Sökmen, "Dünya'da Siber Terör Örnekleri", ***Suç, Terör ve Savaş Üçgeninde Siber Dünya***, Barış Platin Kitabevi, Ankara, 2009, 85-110, s.85.
[227] Al Qaeda and the Internet:The Danger of "Cyberplanning" http://strategicstudiesinstitute.army.mil/pubs/parameters/articles/03spring/thomas.pdf (Erişim tarihi: 12.02.2014).
[228] Taner Altunok ve Aşkın İnci Sökmen, ***a.g.m.***, s.91.

bakıldığında her üç terör grubuna ait örnekler görülmektedir. Gelecekte de benzer durumların yaşanması ihtimal dâhilindedir.

Teröristler tarafından ilk siber terör saldırısı, Ağustos 1998 de Tamil Kaplanları ile bağlantılı ve kendilerine "Internet Siyah Kaplanlar" adı veren bir grup, Sri Lanka'nın, başta ABD dâhil olmak üzere dünyanın çeşitli yerlerinde bulunan diplomatik postalarına, günde ortalama 800 e-posta olmak üzere yaklaşık iki hafta e-posta göndermek yoluyla saldırılarını gerçekleştirmişlerdir. Saldırılar Sri Lanka dış temsilciklerinde örgütün amacı olan, korku ve endişeyi yaratmıştır.[229] Bu siber saldırının, siber terör olarak nitelenmesinin sebebi yapılma amacıdır ve bu örnektekinin yapılma amacı politiktir.

Terör örgütleri devlet kurumlarında kullanılan bilgisayarlara ulaşarak gizli veya kişisel bilgi ve belgelere ulaşabilirler. Örneğin Diyarbakır'da polisin hırsızlık yaptığı şüphesiyle yakaladığı ve elindeki dizüstü bilgisayarında Milli İstihbarat Teşkilatı (MİT) ve Genelkurmay Başkanlığı başta olmak üzere devlete ait gizli bilgiler yer alan 19 yaşındaki hacker R.C.'nin, PKK'nın 'hacker'i olduğu ve örgütün ele başlarından Murat Karayılan'a kuryelik yaptığı ortaya çıkmıştır. Ele geçen film ve müzik CD'lerinin içine sakladığı gizli bilgileri şifreleyen PKK'lı R.C. vicdan azabı çektiği için polisin çözemediği CD'lerdeki şifreleri kaldırınca gerçek ortaya çıkmıştır.[230]

2.2.7. Siber Savaş

Siber savaş bir devlet tarafından, bir devlet adına veya o devleti desteklemek üzere başka bir ülkenin bilgisayar veya bilişim ağlarına veri eklemek, değiştirmek ya da bozmak veya bilgisayarları, ağ üzerindeki cihazları ya da bilgisayar sisteminin kontrol ettiği nesneleri kesintiye uğratmak veya onlara hasar vermek amacıyla yetkisiz giriş yapılmasıdır.[231] Birleşmiş Milletler Terimler sözlüğünde, siber savaş, bilgi savaşı ile birlikte aynı anlamda "bilgisayar sistemlerinin düşman sistemlerine zarar vermek veya yok etmek maksadıyla kullanıldığı savaş tipidir"[232] şeklinde tanımlanmaktadır.

---

[229] Taner Altunok ve Aşkın İnci Sökmen, ***a.g.m.***, s.91.
[230] PKK'nın en önemli 'hacker'ı yakalandı,
http://www.hurriyet.com.tr/gundem/10393202.asp,
(Erişim: 14.02.2014).
[231] Richard A. Clarke ve Robert K. Knake, ***a.g.e.***, s.119.
[232] Cyberwar,
http://unterm.un.org/DGAACS/unterm.nsf/WebView/E996B25EA7D3B36E85256B090056D806?OpenDocument,
(Erişim: 14.02.2014).

Kamuoyu, siber saldırı ve siber suç terimleri ile oldukça aşina olmasına rağmen, son on yıllık zaman diliminde siber savaş terimi gündemi daha fazla meşgul etmeye başlamış ve devletler siber savaşı, taktiklerine ve doktrinlerine almaya başlamışlardır. Siber savaş için yapılmış uluslararası anlaşma olmadığı için bu terimin tanımlanması ve neyin siber savaş oluşturduğu tartışma konusudur.[233] Bu nedenle ülkeler ve uluslararası örgütler tarafından farklı tanımlamalar yapılmaktadır. Ancak günden güne siber savaş terimi medyada daha fazla ilgi görmektedir.

Siber savaş, siber terör ve siber suçların aynı sanal yapıyı kullanmaları bir benzerlik gibi gözükse de motivasyon kaynaklarında ve amaçlarında farklılık vardır. Ayrıca siber savaş, suç ve terörizmden göreceli olarak daha koordineli ve daha yoğun saldırıları içermektedir. Diğer taraftan siber suçlar ve siber terörizm bireyler ya da gruplar tarafından işlenirken siber savaşın tarafı devlet veya örgütlenmiş bir otorite olmaktadır. Bu sebeple kişisel boyutta yapılan faaliyetler siber savaş içerisinde değerlendirilmemektedir.[234]

Siber savaş ortamını hazırlayan çeşitli etmenler vardır. Siber savaşı olası kılan üç boyut vardır:[235]

1. İnternet'in tasarımında mevcut hatalar,
2. Donanım ve yazılımdaki hatalar,
3. Artarak devam etmekte olan kritik sistemlere online erişim olasılığı.

Siber savaşı olası kılan üç unsurun arasında, yazılım ve donanım hataları en önemlisidir. Her geçen gün devlet ve özel sektörün faaliyetlerini siber uzaya taşımaları da bir diğer siber savaşı olası kılan etmendir. Son olarak ise internetin ilk oluşturma felsefesinde güvenliğe yeterli önem verilememesi ve halen bunun devam etmesidir.

Geçmişe bakıldığında çeşitli yaşanmış siber saldırı veya siber savaş örnekleri mevcuttur. Örneğin; 2008 tarihinde Güney Osetya üzerindeki anlaşmazlık sebebiyle Rusya ve Gürcistan arasında yaşanan çatışmalarda görülmüştür. Gürcistan hükümetinin resmi sayfaları tahrif edilmiş, çevrim dışı bırakılmış, meclis ve dış işleri

[233] Mehmet Yayla, Hukuki Bir Terim Olarak "Siber Savaş", http://tbbdergisi.barobirlik.org.tr/m2013-104-1247, (Erişim: 14.02.2014).
[234] Haydar Çakmak ve Cenker Korhan Demir, ***a.g.m.***, s.44.
[235] Richard A. Clarke ve Robert K. Knake, ***a.g.e.***, s.45-48.

bakanlığı siteleri kullanılamaz hale getirilmiştir. Gürcistan Başkanı'nın kişisel internet sayfası ise onu günümüzün Hitler'i olarak tasvir eden başka bir internet sayfasına yönlendirilmiştir.[236]

Diğer örnek NATO'nun Kosova operasyonu sırasında yaşanmıştır. NATO'nun askeri operasyonu süresince Brüksel'deki ağ sunucusuna Sırbistan kaynaklı saldırılar yapılmıştır. Buna mukabil değişik kaynaklardan ana Yugoslav ağ sunucusu yaklaşık yarım milyon e-posta bombardımanına tutulmuştur. Bu savaşın siber uzaydaki başka bir yansıması da Sırbıstan'dan batılı ülkelerin internet sitelerine mesajlar gönderilerek NATO ve ABD'ye karşı propaganda yapılması olarak gerçekleşmiştir.[237]

Bu örnekler gelecekte siber uzayda neler yaşanabileceği ile ilgili ipuçları vermektedir. Yaşanmış olan siber saldırılardan çıkarılacak beş tane ders vardır:[238]

1. Siber savaş gerçektir,
2. Siber savaş ışık hızında gerçekleşmektedir,
3. Siber savaş küreseldir,
4. Siber savaş geleneksel savaş alanından önce yer almaktadır,
5. Siber savaş başlamıştır.

Yaşanmış örnek olaylarda göz önünde bulundurulduğun da, siber savaşta neler yapılabileceği aşağıda anlatılmıştır. Bunlar;[239]

- Rafinerilerde ve nükleer tesislerde yangın çıkıp patlama olabilir,
- Hava trafik kontrol sisteminde meydana gelen arıza ve hatalı çalışmalardan dolayı uçaklar havada çarpışabilir,
- Bankalar çalışamaz hale gelebilir ve müşteri verileri çalınabilir, silinebilir,
- Bankalardan ve ATM'lerden para çekemeyen vatandaşlar mağaza ve dükkânları yağmalayabilir,
- Trenler birbirleriyle çarpışabilir, raydan çıkabilir, hatalı yönlere sevk edilebilir,

[236] Caucasus Foes Fight Cyber War, http://news.bbc.co.uk/2/hi/europe/7559850.stm, (Erişim: 14.02.2014).
[237] Haydar Çakmak ve Cenker Korhan Demir, ***a.g.m.***, s.47.
[238] Richard A. Clarke ve Robert K. Knake, ***a.g.e.***, s.22-23.
[239] Hasan Çifci, ***a.g.e.***, s.12-14.

- Elektrikler kesilebilir ve elektrikle çalışan sistem ve ev aletleri bu süre boyunca kullanılamaz,
- Trafik ışıkları hatalı bir şekilde çalıştırılarak çarpışma ve tıkanmalar meydana gelebilir,
- Petrol ve doğalgaz boru hatlarında patlamalar meydana gelebilir,
- Uydu sistemleri ele geçirilip, meteoroloji, seyrüsefer, iletişim uyduları ve diğer uydular düşürülebilir veya yörüngesinden çıkarılıp rotasından saptırılabilir,
- İnternete erişim kesilebilir. Bilet ve otel rezervasyonları, banka işlemleri, e-ticaret gibi işlemler kesintiye uğrar.

Siber savaştaki en önemli unsurlardan biri istihbarattır. Hedef sistemin özellikleri, bağlantıları, donanım ve yazılım muhteviyatı hakkında ayrıntılı bilgilerin elde edilmesi ve daha sonra bunlardaki güvenlik açıklarının ortaya çıkarılması gerekir. İstihbarat, sadece saldırı açısından değil, savunma açısından da önemlidir. Örneğin; ABD'nin Milli Güvenlik Teşkilatı (NSA) ile ABD Siber Komutanlığı'nın başındaki kişinin aynı isim olması, siber ortamda istihbaratın ne kadar önemli olduğunun göstergesidir.[240]

Saldırılar siber ortamda gerçekleştirilse de sonuçlarının siber ortamda olduğu kadar fiziksel ortamda da görülebilecek olması siber savaşı, klasik savaş ile kıyaslar hale getirmektedir. Bu konuyla ilgili çeşitli görüşler mevcuttur. Bunun önemli sebeplerinden biri ülkelerin siber savaş ile ilgili sahip oldukları potansiyel gücü ortaya çıkartmamalarıdır. Klasik savaş ile siber savaş arasındaki farklar Tablo-5'de yer almaktadır.

Tablo-5: Klasik Savaş ve Siber Savaş Kıyaslaması[241]

[240] Hasan Çifci, ***a.g.e.***, s.19.

[241] Hasan Çifci, ***a.g.e.***, s.20.

Kriterler	Klasik Savaş	Siber Savaş
Saldırı Kaynağı	Saldırının nereden kaynaklandığının bulunması nispeten kolaydır.	Saldırının nereden geldiğini tespit etmek çok zordur, hatta bazen imkânsızdır.
Hızı	Bir füzenin, bir uçağın, tankın veya muharebeye dâhil olan başka bir silah/sistemin hızı kadardır	Işık hızındadır.
Etkisi	Çoğunlukla fiziksel alanda etkilidir.	Çoğunlukla bilgi ve iletişim sistemleri alanında etkilidir.
Savaşanlar	İki veya daha fazla ülkenin silahlı kuvvetleri savaşmaktadır.	Bir kişi, bir grup, bir örgüt veya bir devlet savaşabilir.
Maliyeti	Kullanılan silah/sistemlerin maliyetine bağlıdır. Pahalıdır.	Genelde ucuzdur. Bazen bir bilgisayarla etkili olmak mümkündür.
Silahlar	Tabanca, top, tüfek, bomba, uçak, gemi, tank, füze, radar vb.	Çipler, bilgisayarlar veya bilgi sistemlerinde kullanılan diğer donanımlar, yazılımlar.
Teknoloji İhtiyacı	Genelde ileri teknoloji gerektirmektedir.	Çoğunlukla çok yüksek teknik ve teknolojiye ihtiyaç duyulmamaktadır. Ancak etkili olabilmek için yüksek teknolojinin kullanılması da faydalıdır
Saldırı Belirtileri	Saldırının farkına varılır.	Saldırının farkına varılmayabilir.
Hasar Tespiti	Fiziksel etkilerinden dolayı, hasar tespiti nispeten kolaydır	Nerede ve ne kadar hasar oluştuğunu tespit etmek çok zordur; çoğu zaman imkânsızdır.

Siber savaşın ortaya çıkışıyla bu gücün nasıl hesaplanabileceği ile ilgili farklı görüşler ortaya çıkmıştır. Bu güç hesaplanırken sadece devlet kurumlarının sahip olduğu değil özel sektöründe gücü hesaplanmalıdır. Bunun sebebi özel sektöründe siber uzay da oldukça aktif olmasıdır. Bir ülkenin siber savaş kapasitesi aşağıda belirtilen kabiliyetlerin toplamı olarak ifade edilebilir;[242]

Devlet Kurumlarının kabiliyetleri:

[242] Cyber Warfare An Analysıs of The Means And Motıvatıons of Selected Natıon States, http://www.ists.dartmouth.edu/docs/cyberwarfare.pdf, (Erişim: 14.02.2014).

- Aktif siber savaş unsurları,
- Uygulanabilir siber savaş doktrini,
- Bilgisayar olayları müdahale ekipleri,
- Siber suç önleme ve araştırma ekipleri,
- Siber programlarla ilgili akademik çalışmalara devletin katılım durumu
- Devlet destekli bilgi teknolojileri projeleri,
- İstihbarat kabiliyeti
- Askeri Komuta, Kontrol, Muhabere, Bilgisayar ve İstihbarat kapasitesi,
- Askeri istihbarat unsurları,
- Bilgi teknolojilerinin kullanımı.

Özel sektörün kabiliyetleri:

- Bilgisayar bilimleri ve mühendisliği konusundaki akademik durum,
- İletişim ağlarının kullanım yaygınlığı,
- Bilgisayar güvenliği program ve projeleri,
- Teknolojik açıdan gelişen ülkelerde okuyan öğrenciler,
- Bilgi ve iletişim ağı altyapısı,
- Bilgisayar korsanları,
- Donanım üretme kapasitesi,
- Yazılım geliştirme kapasitesi,
- Bilgi ve iletişim teknolojileri,
- Bilgi güvenliği firmaları,
- İnternet servis sağlayıcı kapasite ve sayısı,
- Uydu sayısı,
- Denetleme kontrol ve veri toplama, sistem geliştirme, kullanma kapasitesi.

Siber Savaş konusundaki uzmanlardan olan Richard Clarke'a göre siber savaş gücü sadece siber saldırı kabiliyetinden ibaret değildir. Siber savaş gücüne siber bağımlılık ve siber savunma da dâhildir. Bu çerçevede bazı ülkelerin siber savaş kabiliyetleri aşağıda ki tabloda yer almaktadır. (Tablo-6)

Tablo-6: Ülkelerin Siber Savaş Kabiliyetleri[243]

[243] Richard A. Clarke ve Robert K. Knake, ***a.g.e.***, s.75.

Ülke	Siber Saldırı	Siber Bağımlılık	Siber Savunma	Toplam
ABD	8	2	1	11
Rusya	7	5	4	16
Çin	5	4	6	15
İran	4	5	3	12
Kuzey Kore	2	9	7	18

Tablo-6'ya göre ABD siber uzay faaliyetlerinde çok etkin olduğu için "Siber saldırı" puanı en yüksektir. ABD siber uzaya en çok bağımlı ülke olduğu için "Siber bağımlılık" puanı en düşük olan ülkedir. Çin kendi siber uzayını istediğinde tüm dış siber dünyadan izole edebileceğinden "Siber savunma" puanı yüksektir.

Verisign firması tarafından yapılan çalışmaya göre ülkeler, siber kabiliyetlerine göre dört gruba ayrılmıştır. Daha sonrada bu gruplarda yer alan ülkelerin özellikleri belirtilmiştir. Aşağıda bu tablo yer almaktadır;

Tablo-7: Ülkelerin Siber Savaş Kabiliyetlerinin Sınıflandırması[244]

[244] Hasan Çifci, ***a.g.e.***, s.26.

	Ülkeler	Özellikleri
Birinci Grup	ABD Çin Rusya	Siber güvenlik ve savunma geliştirme çabaları üzerine uluslararası politika koyma kabiliyetine sahip ülkelerdir.
İkinci Grup	İngiltere Fransa İsrail	Birinci gruptaki ülkeleri yakından takip etmektedirler. Ancak, daha az personel ve daha kısıtlı altyapıya sahiplerdir.
Üçüncü Grup	Türkiye Hindistan Güney Kore Tayvan Almanya Kuzey Kore	Siber güvenlik politikası ve savunma kabiliyetleri geliştirilmesi için önemli ölçüde kaynak tahsis eden ülkelerdir. Ancak, bu alanda lider ülke değillerdir. Birçok durumda, birinci gruptaki ülkeleri taklit etmektedirler.
Dördüncü Grup	İsveç Japonya Avustralya Hollanda İran Pakistan Finlandiya	Siber güvenlik ve savunma kabiliyetlerine yönelik kısıtlı kaynak tahsis eden ülkeler.

Türkiye'de bu gruplar arasında üçüncü grupta yer alarak, siber güvenlik politikası ve savunma kabiliyetleri geliştirilmesi için önemli ölçüde kaynak tahsis eden ülkelerden biridir.

ÜÇÜNCÜ BÖLÜM

SİBER İSTİHBARAT KAVRAMI VE ULUSAL GÜVENLİK-SİBER İSTİHBARAT İLİŞKİSİ

3.1. SİBER İSTİHBARAT KAVRAMI

21. yüzyıla girerken internet tabanlı bilişim teknolojilerinin neredeyse bütün endüstri dallarının altyapısını oluşturduğu görülmektedir. İnternette mesaj gönderme için kullanılan e-postanın ardından, e-reklam, e-ticaret, e-devlet, e-oylama vb. pek çok kavram yeni teknoloji ile birlikte gittikçe gelişerek gündelik yaşamımızın birer parçası haline gelmiştir. Bunun yanında internet bağlantılı cep telefonları, diz üstü, kişisel ve tablet bilgisayarlar gibi üretilen her yeni sistem de bilgisayar tanımının sınırlarını zorlamaktadır.[245]

Teknolojik gelişmeler bilgi depolamayı kolaylaştırırken aynı zamanda istihbarat faaliyetlerini de kolaylaştırmaktadır. Günlük yaşamın internet ile iç içe geçtiği günümüzde, internet üzerinden kişilerin, özel sektör ve devlet kurumlarına ait bilgilerin, kullanıcı hesaplarının ele geçirilmesi sıkça yaşanmaktadır.

Siber istihbarat'ın tanımı ile ilgili kesinlik mevcut değildir. Siber istihbaratı farklı yapan ve diğer istihbarat elde etme yöntemlerinden daha avantajlı konuma getiren kullandığı materyallerdir. Bu araçlar yüksek teknolojiye sahiptirler; böylece gerekli ve nitelikli stratejik bilgiyi elde ederken, zaman ve ekonomik avantaj sağlarlar. Aynı zamanda, bu araçlar daha az emek ve sermaye ile daha net bilgi getirdiğinden dolayı klasik istihbarat anlayışını değiştirmektedirler. Birçok uzmana göre siber istihbarat; düşmanın kendimiz hakkında bilgi edinmesini önlerken, onun hakkındaki her şeyi öğrenmektir.[246]

Siber istihbarat kişisel, ekonomik, politik veya askeri avantaj sağlamak için, iletişim ağları veya bilgisayarlara yasa dışı sızarak, şahıslardan, rakiplerden, gruplardan, ülkelerden veya düşmanlardan, onların izni olmadan sırlarını elde etme eylemidir.[247]

---

[245] Moses Dlamini, Mariki Eloff and Jan Eloff, " Information Security: The Moving Target", ***Computers & Security*****,** 2009, vol.28, issues 3-4, 189-198, p.191.
[246] Nedret Ersanel, ***Siber İstihbarat: Siber ve Dijital Casusluğun Anatomisi***, Asam Yayınları, Ankara, 2001, s.10.
[247] Hasan Çifci, ***a.g.e.***, s.6.

Siber ortamı kullanarak siber uzayda yer alan bilgileri elde edip istihbarat oluşturmak için muhtelif yöntemler kullanılmaktadır. Bu yöntemleri aşağıdaki şekilde gruplandırmak mümkündür;[248]

- Sosyal Mühendislik,
- Sosyal Medya,
- Casus Yazılımlar,
- Ücretsiz Web Hizmetleri,
- Arama motorları,
- Yemleme,
- İletişimin Dinlenmesi.

3.1.1. Sosyal Mühendislik

Sosyal mühendislik temel olarak insan ilişkilerini veya insanların dikkatsizliklerini kullanarak hedef kişi veya kurum hakkında bilgi toplamak olarak tanımlanabilir. Bu olayda amaç hedef alınan kurum veya kişi yapısı, kurumsal ağın yapısı, çalışanların/yöneticilerin kişisel bilgileri, şifreler ve saldırıda kullanılabilecek her türlü materyalin toplanmasıdır.[249]

Sosyal mühendislik, teknolojiyi kullanarak ya da kullanmadan bilgi edinmek için insanlardan faydalanıp, etkileme ve ikna yöntemlerinin kullanılmasıdır. Sosyal mühendisliği normalde insanların tanımadıkları biri için yapmayacakları şeyleri yapmalarını sağlama sanatı olarak tanımlayabiliriz.[250]

The Washington Times gazetesinde 18 Temmuz 2010 günü yayınlanan bir haber, teknolojinin ve özellikle internetin sunduğu imkânların, istihbarat ve daha geniş bir çerçevede ulusal güvenlik alanında ne derece önemli bir silah haline geldiğinin göstergesi olmuştur. Robin Sage, 25 yaşında, Massachusetts Teknoloji Enstitüsü mezunu ve ABD Deniz Kuvvetleri'ne bağlı Donanma Ağ Muharebe Komutanlığı'nda "siber tehdit uzmanı" olarak çalışan bir bilgisayar korsanıdır. ABD

---

[248] Hasan Çifci, ***a.g.e.***, s.292.
[249] Sosyal Mühendislik Nedir?, http://www.cyber-warrior.org/dokuman/Default.Asp?Data_id=4442, (Erişim: 14.03.2014).
[250] Türkiye'deki Kamu Kurumlarında Sosyal Mühendislik Uygulamaları, http://www.bilgiguvenligi.gov.tr/sosyal-muhendislik/turkiyedeki-kamu-kurumlarinda-sosyal-muhendislik-uygulamalari.html, (Erişim: 14.03.2014).

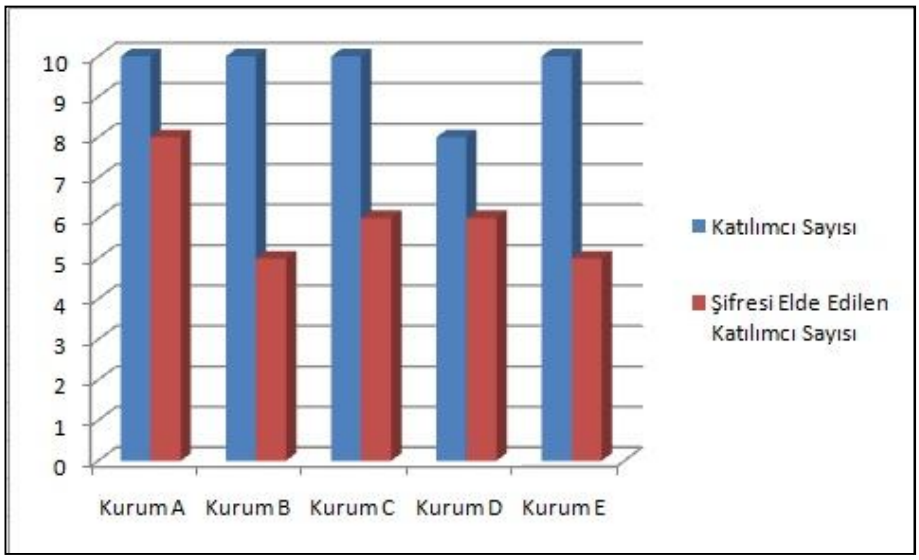
Silahlı Kuvvetleri, istihbarat ve güvenlik teşkilatlarına mensup çok sayıda (300'den fazla) kişi ile Facebook, Twitter, LinkedIn gibi sosyal ağ siteleri üzerinden arkadaşlık kurarak çok sayıda gizli bilgiyi ele geçirmiş ya da bu bilgileri edinecek kadar yeterli ipucu ve veri elde etmiştir. Ancak Robin Sage aslında gerçek bir kişi değildir. Thomas Ryan adlı, New Yorklu bir yazılım uzmanının yarattığı sanal bir karakterdir. İnternet ortamındaki yegâne profil resmi de bir porno sitesinden alınmıştır.[251]

Robin Sage testi Aralık 2009 ile Ocak 2010 tarihleri arasında, iki ay süren test sonucuna göre;[252]

- Gerçek bir şahsiyet olmamasına ve detaylı bilgileri yer almamasına rağmen, Google ve Lockheed Martin gibi önemli firmalardan iş teklifi, erkeklerden de akşam yemeği teklifi almış,
- FBI ve CIA hariç, birçok istihbaratçı ve askeri personel kendisi ile siber ortamda arkadaş olmuş,
- Kendisine sunulan bilgilerin birçoğuyla harekât güvenliği ve personel güvenliği kuralları ihlal edilmiş,
- Gerçek bir kişilik olup olmadığını test edenler ve sahte olduğunu ortaya çıkaranlarda olmuştur.

Diğer bir örnek TÜBİTAK'ın yaptığı sosyal mühendislik çalışmasıdır. TÜBİTAK Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü (UEKAE) Bilişim Sistemleri Güvenliği Bölümü yaklaşık 1,5 yıl süresince kamu kurumlarına sosyal mühendislik saldırıları gerçekleştirmiştir. Bu kapsamda toplam 5 kamu kurumunda test icra edilmiştir. Bu testte toplam 48 kullanıcı ile telefon görüşmesi yapılmış ve 30'una ait şifre elde edilmiştir. Aslında burada kurum bazında başarı oranına bakmak pek de doğru olmayabilir. Çünkü saldırgan olarak kurumdan sadece bir kişinin bile şifresi ele geçirildiğinde, bu şifreyle pek çok bilgiye ulaşabilmek mümkün olmaktadır.[253] Sonuçlar analiz edildiğinde aşağıdaki Grafik-1 ortaya çıkmaktadır.

[251] İnsan İstihbaratı ve Robin Sage Deneyi, http://www.siyahgribeyaz.com/2010/08/insan-istihbarat-ve-robin-sage-deneyi.html, (Erişim: 14.03.2014).
[252] Hasan Çifci, ***a.g.e.***, s.292-293.
[253] Türkiye'deki Kamu Kurumlarında Sosyal Mühendislik Uygulamaları, http://www.bilgiguvenligi.gov.tr/sosyal-muhendislik/turkiyedeki-kamu-kurumlarinda-sosyal-muhendislik-uygulamalari.html, (Erişim: 14.03.2014).



Grafik-1: Kamuda Bilgi Güvenliği Bilinci Analizi[254]

Grafik-1'e göre bütün kurumlardan belirli sayıdaki personelle telefon irtibatı kurulmuş ve her kurumdan belirli sayıdaki kişiden şifre elde edilmiştir. Sonuçta kamu kurumlarındaki personelde bilgi güvenliği bilincinin yetersiz olduğu değerlendirilmektedir.

3.1.2. Casus Yazılımlar

Casus yazılımlar, Truva atı, rootkit, klavye dinleyici gibi, kullanıcıdan habersiz olarak bilgisayarlarda çalışan ve bilgisayarlardaki verileri belirli sunuculara gönderen yazılımlardır. Bu yazılımlar aracılığıyla bilgisayardaki tüm veriler, kullanıcıya hissettirilmeden çalınabilir. Bu yazılımların kabiliyeti ve kullanılan yöntemler, insanın hayallerinin sınırlarını zorlamaktadır.[255]

Siber istihbarattan önce, bir casusun çalabileceği bilgi miktarı üzerinde fiziksel kısıtlamalar vardı. Ancak siber etkinliklerin hızı, hacmi ve küresel erişimi, siber istihbaratı daha önceden yapılan istihbarat faaliyetlerinin yanında nitelik ve kapsam bakımından çok farklı kılmaktadır. Örneğin; 2009 yılında F-35 savaş uçağı geliştirme projesiyle ile ilgili veri depolama sistemlerine yetkisiz giriş yapılmış ve F-35 savaş uçağının geliştirilmesiyle ilgili terabitler dolusu bilgi, bilinmeyen kişilerce ele geçirilmiştir. Soğuk Savaş döneminde bir casusun bu kadar bilgiyi, gizli ve korunan

[254] Türkiye'deki Kamu Kurumlarında Sosyal Mühendislik Uygulamaları, http://www.bilgiguvenligi.gov.tr/sosyal-muhendislik/turkiyedeki-kamu-kurumlarinda-sosyal-muhendislik-uygulamalari.html, (Erişim: 14.03.2014).
[255] Hasan Çifci, ***a.g.e.***, s.294.

bir tesisten çıkarması için bir kamyonet ve forklifte ihtiyacı vardı.[256] F-35 savaş uçağı projesi geliştirme maliyetinin için 395,7 milyar dolar[257] olarak hesaplandığı göz önünde bulundurulduğunda elde edilen bilgilerin öneminin ve ekonomik değerinin daha net anlaşılacağı değerlendirilmektedir.

Hiçbir istihbarat amaçlı yazılım programı ya da kullanımı Savcılık Yönetim Bilgi Sistemi (PROMIS) programı kadar istihbarat örgütleri içinde sansasyon yaratmamıştır. PROMIS programının temel özelliği, farklı veri tabanlarından bilgileri toplayıp bunları birbirleriyle bağlantılı hale getirilebilmesidir. Bu program sayesinde o zamana kadar emsali görülmemiş bir hizmet kullanıcılara sunulmuştur. Örneğin; sadece bir evde normalden fazla su tüketimi yapılıyorsa veya herhangi bir evde telefon görüşmelerinde önemli bir artma başladıysa kullanıcısını uyarmaktadır.[258] Bu program 1990'lı yılların başlarında, programı üreten Inslaw Şirketi'nin bilgisi dışında, "Truva Atı" olarak bilinen virüs yerleştirilerek el altından birçok ülkeye satılmıştır.[259] Bu programın Mısır, Suriye, Pakistan, Kuveyt, İsrail, Ürdün, İran ve Irak'ın da bulunduğu birçok ülkenin emniyet veya askeri kurumları tarafından satın alındığı tespit edilmiştir. Promis programı Türkiye'ye de satılmıştır.[260] Programın içine yerleştirilen "Truva Atı" yazılımı sayesinde, Promis yazılımını satın alıp kullanan ülkeler, bilgisayar sistemlerindeki gizli bilgileri otomatik olarak ABD ve İsrail istihbarat örgütlerine de açmış olmaktadır.[261] Bu yöntemle bir devletin sahip olduğu en kritik bilgilere, başka ülkelerin ulaşması mümkün kılınmıştır. Bu şekilde elde edilebilecek bilgiyle, harcanan emek ve maliyet kıyaslandığında siber istihbaratın önemini bir kez daha ortaya çıkartacağı değerlendirilmektedir.

Dünyadaki birçok ülke siber uzayda neler yapılabileceği ve sonuçları ile ilgili kendi sistemleri üzerinde testler yapmaktadır. Örneğin; The Washington Post'da ki bir değerlendirmeye göre; 1994 yılında internete bağlı (istihbarat ve güvenlik açısından açık sayılabilecek) ABD ordusuna ait 150 binden fazla askeri bilgisayar bulunmaktadır. ABD istihbarat kurumları ve ordu bu bilgisayarlara saldırı yapılması adına bir grubu serbest bırakmış, bu bilgisayarların yüzde 90'ına yakınına giriş

[256] Richard A. Clarke ve Robert K. Knake, ***a.g.e.,*** s.124.
[257] How the F-35 Nearly Doubled In Price,
http://nation.time.com/2012/07/09/f-35-nearly-doubles-in-cost-but-you-dont-know-thanks-to-its-rubber-baseline/
(Erişim Tarihi: 12.03.2014)
[258] Nedret Ersanel, ***a.g.e.***, s.34-35.
[259] Ömer Özkaya, **Zihin Kontrolü,** BSR Yayın Grubu, İstanbul, 2011, s.238.
[260] Gültekin Avcı, ***a.g.e.***, s.70-71.
[261] Ömer Özkaya, ***a.g.e.***, s.238.

yapılmış ve ancak yüzde 4'ü fark edilebilmiştir.[262] Sonuçta siber saldırının kimler tarafından ve ne zaman başladığı, hangi sistem ve bilgilerin zarar gördüğü, bu bilgilerle saldırıyı yapanların hangi kazançları sağladığının tespit edilmesinin zordur. Hatta çoğu zaman da saldırıyı yapanların tespitinin mümkün olmaması ülkeleri siber istihbarat alanında yatırım yapmaya yönlendirmektedir. Bu gelişmeler ışığında, siber uzayda ulusal güvenliklerini sağlamak amacıyla siber istihbarata yatırım yapacak ülkelerin ilerleyen yıllarda sayısının ve bu konuya ayrılan ekonomik kaynakların daha da artacağı öngörülebilir.

3.1.3. Sosyal Medya

Sosyal medya, kurumlar, topluluklar ve bireyler arasında etkileşimli bir iletişim imkânı sağlayan, kullanıcı veya müşterilerin ürettiği içeriğin yer aldığı web tabanlı uygulamalara verilen isimdir.[263]

İnternet forumları, internet günlükleri, video, resim ve dosya paylaşım siteleri, kişisel sayfa ve bilgi paylaşım siteleri, arkadaşlık siteleri, haber paylaşım siteleri vb. internet hizmetleri sosyal medya gurubunda sayılabilir. Örneğin; facebook, twitter, youtube, flickr, mylife, myspace, raptr, linkedln. Sosyal medya, istihbarat toplayan kişi veya gruplar ve istihbarat örgütleri için büyük fırsatlar sunmaktadır. Sosyal medyayı kullanarak kişiler, ülkeler, kurumlar hakkında bilgi elde edilebilir.[264]

Genel bir değerlendirme yapıldığında Sosyal Medya sayesinde istihbarat örgütleri şu bilgileri elde edebilmektedir;

- Sizin, arkadaşlarınızın ile neler yaptığınızın bilgisi,
- Yaş gününüzün gün, ay ve yıl olarak bilgileri,
- Sizin ve arkadaşlarınızın eğitim bilgileri,
- Nerelere hangi etkinliklere davet edildiğinizin bilgileri,
- Hangi gruplara davet edildiğiniz,
- Oturduğunuz şehir,
- Arkadaşlarınızın ve sizin ilgi duyduğu şeyler,
- Neleri beğendiğiniz,

[262] Nedret Ersanel, ***a.g.e***., s.19-20.
[263] Social media, http://en.wikipedia.org/wiki/Social_media, (Erişim Tarihi: 12.03.2014).
[264] Hasan Çifci, ***a.g.e.***, s.293.

- Siz ve arkadaşlarınızın bulunduğu yerin detay bilgileri,
- Siz ve arkadaşlarınızın yazdığı notlar,
- Siz ve arkadaşlarınızın size ait veya etiketlendiğiniz fotoğraf ve videolarınız,
- Facebook'a yazdığınız sizin ve arkadaşlarınızın ilişki durumu,
- Sizin ve arkadaşlarınızın politik ve dini görüşleri,
- Sizin ve arkadaşlarınızın yazdığı durum mesajları,
- Siz ve arkadaşlarınızın web adresleri,
- Sizin elektronik postanız,
- Belki de en önemlisi; başka istihbarat örgütleri için veri olabilecek önemli kurum ve kuruluşlara ait fotoğraf, resim, doküman ve belgeler.

Wikileaks kurucusu Julian Assange, Russia Today'e verdiği röportajında Facebook'un insanların isim ve bilgileri hakkında dev bir veritabanı olduğunu ve kullanıcıları tarafından gönüllü olarak kullanılsa da, ABD istihbaratının kullanması için geliştirildiğini iddia etti. Facebook'u "şimdiye kadar icat edilmiş en dehşet verici casus makinesi" olarak tanımlayan Assange, "Herkes şunu anlamalı ki, arkadaşlarını Facebook'a ekleyerek ABD istihbarat servisleri için bedavaya çalışıyorlar ve onlar için bu veritabanını oluşturuyorlar." demiştir.[265] Assange'ın bu iddiası da sosyal paylaşım siteleri ile istihbarat örgütlerinin ne kadar çok iç içe geçtiğini göstermektedir. İstihbarat örgütleri bu ağları kullanarak ulusal güvenliği tehdit edecek konuma gelebilmektedir. Bunun en yakın örneği olan Arap Baharı sürecinde internet üzerinden haberleşerek örgütlenen on binlerce insanın organize olduğu hatırlandığında sosyal paylaşım ağlarının gücü daha iyi anlaşılabilecektir.

Facebook'un bugün elindeki veriler bütün istihbarat örgütlerinin iştahını kabartmaktadır. Gerek Google'ın, gerek Twitter'ın, gerek Facebook'un Amerika'da bağlı olduğu yasalar sebebiyle aslında bu ülkenin yerel istihbaratı veya CIA'in, istediği verileri bu şirketlerden alabilecekleri anlamına gelmektedir. Resmi olarak olmasa da gayri resmi olarak bunun yapıldığını birçok forumlarda ya da Amerika'daki tartışma gruplarında görülmektedir. Echelon ses tarama sisteminin benzeri bir sistemin bugün Twitter ve Facebook'ta paylaşılan anlık verileri metinsel olarak gerçekleştirdiği yönünde iddialar mevcuttur.

[265] Assange: Facebook en büyük ajan,
http://www.sabah.com.tr/Teknoloji/Haber/2011/05/04/assange-facebook-dunyanin-en-buyuk-ajani-597582296690,
(Erişim tarihi: 10.03.2014).

3.1.4. Ücretsiz Web Hizmetleri

Günümüzde Gmail, herkese mesajlarını saklaması için 10 giga bayt alan veriyor ve bu boyut sürekli artmaktadır. Yahoo, Hotmail gibi çok sayıda ücretsiz e-posta hizmeti veren siteler vardır. Bu siteler aracılığıyla kim kiminle yazışıyor, neler yazılıyor, gönderiliyor ve hangi dosyalar paylaşılıyor başta olmak üzere daha birçok sorunun cevabını bu sistemlerde bulmak mümkündür. Bu açıdan bakıldığında dünyanın en yaygın ve etkili istihbarat araçlarından birinin sahibinin Google olduğunu söylesek yanlış olmayacaktır.[266]

Örneğin; ABD'nin internet izleme ve telefon dinlemeye yönelik gizli programlarını basına sızdıran NSA eski sistem analisti Edward Snowden'den elde edilen belgelere ve yetkililerle yapılan görüşmelere dayandırılan haberde NSA'nın, Yahoo ve Google iç ağlarından, kurumun Washington'un bir banliyösündeki merkezinde bulunan veri deposuna her yıl milyonlarca veri aktarımı yaptığının ortaya çıktığı belirtilmiştir. Verileri elde etmede kullanılan en önemli aracın NSA ve İngiliz istihbarat örgütü Hükümet İletişimler Merkezi (GCHQ) ile ortak yürütülen MUSCULAR projesi olduğu belirtilen haberde, NSA ve GCHQ'nun, Google ve Yahoo'nun veri merkezleri arasındaki bilgileri ileten fiber optik kablolardaki tüm veri akışını kopyaladıklarının ortaya çıktığı aktarılmıştır.[267]

İnternet üzerinden verilen çeşitli hizmetlerin ücretsiz olması, kullanıcı açısından cazip olmasına karşılık, bu hizmetlerin neden ve ne amaçla ücretsiz oldukları düşündürücüdür. Ücretsiz dosya saklama ve web alanı siteleri, ücretsiz programlar ve ücretsiz web tabanlı virüs tarama siteleri de siber istihbarat elde etmede kullanılan araçlardandır.

3.1.5. İletişimin Dinlenmesi Yoluyla İstihbarat Toplanması

Bilgisayarlar, iletişim ağı aracılığıyla birbirleriyle iletişim kurarlar. İletişim ağı, kablolu ve kablosuz veri aktarma cihazlarından oluşmaktadır. Veriler bilgisayarlar arasında akarken, iletişim ağındaki verilerin yasal veya yasa dışı yollarla dinlenmesi ve ele geçirilmesi mümkündür. Şifresiz iletişim ağı protokolleri ile veri alışverişi

[266] Hasan Çifci, ***a.g.e.***, s.295.
[267] ABD İstihbaratı Google ve Yahoo'ya Sızmış, http://www.hurriyet.com.tr/avrupa/25015721.asp, (Erişim tarihi: 10.03.2014).

yapıldığında, akan trafiği aradaki herhangi bir bağlantı veya düğüm noktasında ele geçirmek mümkündür. Şifreli protokollerin kullanılmasında ise, trafik ele geçirilse bile, şifrenin çözülmesi gerekecektir.[268]

Dünya üzerindeki iletişimin dinlenmesi ile ilgili bilinen en yaygın örnek ECHELON sistemidir. ECHELON sistemi 1948 yılında ABD, Avustralya, İngiltere, Kanada ve Yeni Zelanda arasında imzalanan bir anlaşmayla kurulmuştur. Günümüzde ECHELON dünyanın çeşitli yerlerindeki dev kulakları ve uyduları aracılığıyla sınır aşan, her telefon görüşmesini, faks, teleks ve elektronik posta mesajıyla, radyo dalgalarını, havacılık ve denizcilik frekanslarını dinleyebiliyor.[269]

3.1.6. Yemleme Yoluyla İstihbarat Toplanması

Yemleme(phishing), internet üzerinde güvenilen elektronik iletişim kaynaklarından birinin yerine geçerek kullanıcıların o kaynakla irtibata geçmesini sağlama ve onlardan kullanıcı adı, parola, kredi kartı bilgileri ve diğer özel bilgileri çalma eylemidir.[270] Diğer bir ifadeyle, e-posta veya bunun gibi bilgi girilmesi gerektiren bir kuruluşun web sayfasının bir kopyasının yapılıp kullanıcının hesap bilgilerini çalmayı amaçlamaktadır.[271]

Örneğin, öncelikle hedefteki kişiye e-posta gönderilir. Hedefteki kişiye ses, video, resim veya yazılı dosya (pdf, ppt,doc, xls vb. dosyalar) gibi e-posta sistemlerince engellenmeyen dosyalar gönderilir. Hedefteki kişi, kendisine gönderilen dosyayı açtığında, dosyayı açmayı sağlayan program (Adobe Acrobat Reader, Paint, Real Player, Office vb.) çalışır. Dosyayı açmaya çalışan programdaki güvenlik açığını kullanan kod parçası da çalışır. Bu zararlı kod parçası, saldırganın hedefteki kişinin bilgisayarına uzaktan bağlanmasını sağlayan bir kapı açar. Bu aşamadan sonra saldırgan her şeyi yapabilir; bilgisayardan veri çalabilir, hedefteki kişinin bastığı tüm tuşları kaydederek onun şifrelerini ele geçirebilir, kredi kartı bilgilerini ele geçirebilir, istediği dosyaları bilgisayara yerleştirebilir, bilgisayardaki sistemi bozabilir, başka bilgisayarlara saldırmak için kullanabilir.[272]

---

[268] Hasan Çifci, ***a.g.e.***, s.301-302.
[269] Ömer Özkaya, ***a.g.e.***, s.260.
[270] How Phising Works, http://computer.howstuffworks.com/phishing.htm, (Erişim tarihi: 12.03.2014).
[271] Sait Yılmaz ve Olay Salcan, ***a.g.e.***, s.59.
[272] Hasan Çifci, ***a.g.e.***, s.300-301.

3.1.7. Arama Motorları Aracılığıyla İstihbarat Toplanması

Arama motorlarının ortaya çıkması ile beraber istihbarat elde etmek amacıyla kullanılması sorgulanmaya başlanmış ve sonuçta arama motorlarından faydalanılarak birçok farklı yöntemle istihbarat elde edilmeye başlanmıştır.

Arama motorları birkaç açıdan önemli istihbarat kaynağıdır;[273]

- Bunlardan bir tanesi, arama motorlarının, dünyadaki sunuculardaki verileri toplaması ve kaydetmesidir. Dünyanın her yerinden, çok değişik konularda bilgiler bir araya getirilerek veri tabanlarına kaydedilmektedir. Veri madenciliği adı verilen yöntemle çok değerli bilgileri elde etmek mümkündür.
- Bir diğer istihbarat elde etme yöntemi ise, kimlerin neyi aradığı bilgisidir. Arama motoru firmaları (Google, yandex vb.) hangi ülkenin, hangi şehrinin, hangi bilgileri aradığını bilmektedir. Örneğin; google firması hangi IP adresinden hangi aramaların yapıldığını bilmektedir. Hangi IP adresini hangi şirketin veya devlet kurumunun kullandığını bulmak çok basittir. Bu şekilde hangi firmanın neleri araştırdığı veya hangi devlet kurumunun nelere ilgi duyduğu bilinebilir.
- Arama motorları kullanarak veri toplamak mümkündür. Örneğin; google arama sayfasında gelişmiş arama seçenekleri yazarak, önemli bilgilere ulaşılabilmektedir.

Örneğin; Gazi Üniversitesi Mühendislik Fakültesi Bilgisayar Mühendisliği Bölümü Öğretim Üyesi ve Fen Bilimleri Enstitüsü Müdürü Prof. Dr. Şeref Sağıroğlu arama motorları ile ilgili görüşleri şunlardır; "Arama motorları her şeyimizi biliyor, ellerinde müthiş bir veri tabanı var. Ülkenin gidişatını bile biliyorlar. Ülkenin gidişatını aranılan kelimelerin istatistiklerinden biliyorlar, ona göre strateji geliştiriyorlar. Arama motorları bizi, bizden iyi tanıyor, analiz ediyor. Aradığınız kelime, nelere bakıp, nelerle ilgilendiğiniz sizi ele veriyor."[274]

Sonuçta, Prof. Dr. Şeref Sağıroğlu'nun değerlendirmeleri arama motorlarının önemini ve gelecekte de hangi amaçlarlarla kullanılabileceğini net bir şekilde ortaya

[273] Hasan Çifci, ***a.g.e.***, s.299.
[274] Google, Elindeki Müthiş Veri Tabanı Sayesinde Hakkımızdaki Herşeyi Biliyor!, http://yorumcahaber.com/haber_detay.asp?haberID=5167, (Erişim tarihi: 15.03.2014).

koymaktadır. Gelecekte istihbarat amacıyla çok daha yoğun bir şekilde arama motorları kullanılacaktır.

3.2. ULUSAL GÜVENLİK VE SİBER İSTİHBARAT İLİŞKİSİ

3.2.1. Siber İstihbaratın Ulusal Güvenlik İçerisindeki Yeri

Soğuk Savaş sonrası güvenlik kavramının içeriği önemli oranda değişmiştir. 20. Yüzyıl ve öncesinde güvenlik denilince çoğu zaman akla gelen ülke sınırlarının güvenliği idi. Oysaki günümüzde ekonomi, çevre, enerji vs. güvenliğinden de ciddi manada söz edilmekte ve tedbirler alınmaktadır. Örneğin; bir ülke geçmişte silahlı güçleriyle ülke sınırlarını rahatça korurken günümüzde silahlı güçler yeterli olmamaktadır. Nano-Teknoloji, bilgisayar vs. gibi yeni tehlikelere karşı yeni uzmanlara ve uzmanlık kuruluşlarına ihtiyaç vardır.[275] Günümüzde bu alanlardan biri de siber saldırı, siber istihbarat vb. gibi siber tehlikelere karşı oluşturulan siber güvenlik kuruluşlarıdır.

Özellikle 1990 sonrası gelişen ağı sayesinde tüm dünyayı saran internetin, son dönemde adaptasyonu o kadar hızlı olmuştur ki, fiziki ortamda yer alan hemen her şey siber uzay ortamına taşınmıştır. İnsanlar sohbet etmek, alışveriş yapmak, müzik dinlemek, film seyretmek veya bilgi aramak vb. amaçlar için internet kullanmaktadır. Ayrıca dünyada birçok ülkede çok sayıda işletme ve tüketici internet ortamında boy göstermektedir. İnternetin kullanıcıları açısından diğer bir parçası da devlet kurumlarıdır. İnternetin büyümesine paralel olarak, ülkelerde faaliyetlerini siber uzaya taşıyarak sistemlerini entegre etmişlerdir. Böylece ülkelerin ulusal güvenliklerinin bir parçası da siber uzay olmuştur.

Siber uzayın genişlemesi ve bilgi iletim süresinin kısalmasıyla ekonomik, politik ve askeri alanlarda internet kullanılmaya başlanmıştır. Devletler de küçük ölçekte altyapı hizmetlerinin dağıtımında, makro ölçekte ise dış temsilcilikleriyle iletişimden diplomasiye, istihbarati bilgi toplamadan savunma teknolojilerine kadar geniş bir çerçevede bilgi teknolojisi ve siber uzayın imkânlarından yararlanmaya başlamışlardır.[276] Siber uzay devletlere birçok imkân ve fırsat sağlamasının yanında beraberinde çeşitli siber riskleri de getirmektedir.

[275] Sait Yılmaz, ***a.g.e.***, s.ıx.
[276] Salih Bıçakçı, ***a.g.e.***, s.3.

Günümüzde bilgi teknolojisindeki baş döndürücü gelişmeler, kamu ve özel sektör alanlarındaki çalışma yöntemlerine büyük etki yapmaktadır. Bugünkü gelişmelere bakarak yakın bir zamanda ülkelerdeki kamu faaliyetleri, ekonomik faaliyetler ve günlük yaşam bilgi teknolojilerine ve bilgi altyapılarına tamamen bağımlı hale gelecektir.[277] Bilgisayarın günlük yaşamda aktif bir rol almaya başlaması beraberinde internet kullanımının yaygınlaşması ile bilgi teknolojilerinin gerek zamandan gerek işgücünden sağladığı tasarruf insanlık için büyük fayda sağlamaktadır. Ancak gelişmiş ülkeler, büyük şirket ve kuruluşlara bakıldığında örgütsel yapıları tamamen bilgi teknolojilerine dayanmaktadır. Bu da onları yaşanabilecek herhangi bir siber saldırı karşısında özellikle ülkelerin ulusal güvenlikleri açısından telafisi mümkün olmayan kayıplar yaşama ihtimaliyle karşı karşıya bırakmaktadır.

Hızla gelişen bilgi teknolojileri, bu alanı yoğun olarak kullanan ülkelere birçok avantaj sağladığı gibi beraberinde getirdiği olumsuzluklar da mevcuttur. Bilgi teknolojilerini yoğun olarak kullanan ülkeler bütün sistemlerini bu alana endeksleyerek zaman ve emek gerektiren faaliyetleri basit hale getirmiş, ancak bu da onları siber uzaya bağımlı hale getirmiştir. Bu durumda ortaya çıkabilecek çıkar çatışması, siber saldırı, siber istihbarat faaliyetlerinin yaşanması durumunda bilgi teknolojileri konusunda daha donanımlı olan ülke, kendi menfaatleri ve amaçları doğrultusunda hareket ederek ulusal güvenliğini sağlamada avantajlı konumda olacaktır. Gelişen bilgi teknolojileri beraberinde ülkelerin siber savunma sistemlerini de gelişime zorlamış ve köklü değişimler yaşanmasına neden olmuştur.

Günümüzde devletlerin bekasını devam ettirebilmeleri için ulusal güvenliğin korunması gerekmektedir. Bu nedenle hayati alt yapıların korunmasının önemi ve gerekliliği tartışılmazdır. Devletin ekonomik, özel ve askeri yapılarının korunması için ülkenin siber uzay ağlar sisteminin güvenliğinin sağlanması gerekmektedir. Örneğin; Fransa'da şifreli yazılım ve donanım "mühimmat" olarak kabul edilmektedir. Ülke dışından getirilmesi ve kullanımı devletin onayına bağlıdır. Bu çerçevede ülkenin düşmanlarının (ülkeler, ülke içi gruplar, bireyler vb.) yapacakları siber saldırıların önlenmesi şarttır.[278] Bu siber saldırılardan biriside siber istihbarat faaliyetleridir. Yaşanmış siber istihbarat örneklerine bakıldığında ulusal güvenliğe en fazla zarar veren siber saldırılardan birinin siber istihbarat çalışmaları olduğu görülmektedir.

[277] Sait Yılmaz ve Olay Salcan, ***a.g.e.***, s.11.
[278] Nedret Ersanel, ***a.g.e.***, s.157-158.

Siber uzayda güvenlik alanında ki mücadele farenin hep bir adım önde olduğu kedi-fare savaşına benzetilmektedir. Bakanlıklar, kamu kurumları, üniversiteler, laboratuarlar yani internete bağlı ne kadar kuruluş varsa hedef halindedir. Hacker'lar teknoloji, istihbarat, entelektüel bilgi, askeri silahlar ve stratejiler peşindedir. Bu nedenle sahip olunan her veri ya da bilgi ele geçirilmeye çalışılmaktadır.[279] Siber uzayda kritik bilgi bulunduranlar, her zaman siber saldırılara karşı dikkatli olmak zorundadır. Bu nedenle siber istihbarata karşı, siber uzayda yer alan kurumların, şirketlerin, bireylerin vb. sürekli bir gelişim içerisinde bulunmasının gerektiği değerlendirilmektedir. Bu çerçevede devletinde ulusal güvenliğini sağlayabilmesi için özellikle siber istihbarat faaliyetlerine karşı siber uzayının güvenliğini sağlaması gerektiği değerlendirilmektedir.

Devlet kurumları siber uzayda faaliyetlerini yaparken, sahip oldukları kritik bilgiler de saldırılara açık hale gelebilmektedir. Bilgisayar kullanıcıları sahip oldukları yazılımlar ile bilgilerinin korunduğunu düşünürken, sürekli farklı yöntem ve yazılımlar deneyen hackerlar bilgisayarların kontrolünü ele geçirebilmekte ve bilgileri istediği bilgisayara kopyalayabilmektedir. Bu şekilde çok kritik bilgiler kullanıcıların farkında olmadan el değiştirebilmektedir. Bununla ilgili yaşanmış devletler çapında onlarca örnek bulunmaktadır. Ülkelerin ulusal güvenlikleri ile ilgili kritik bilgiler siber istihbarat yöntemiyle kopyalanmıştır.

3.2.2. Siber İstihbarat Uygulamaları

Günümüzde küresel iletişim ağlarından yararlanan istihbarat örgütleri, neredeyse istedikleri bütün kapalı veri bankalarına girerek gizli ve özel bilgilere ulaşabilmektedirler.[280] Savunma ve güvenlik sektöründe, güvenlik kameralarından ateşleme sistemlerine çok geniş bir alanda; enerji sektöründe, elektrik santralleri, petrol ve gaz nakil hatlarında; ulaşım sektöründe demiryolu ve havayolu ulaşımında sistemlerin işleyişi elektronik kontrol edilmektedir. Ayrıca yine finans ve bankacılık alanlarında; bilgi ve telekomünikasyon alanlarında; halk sağlığı, su, tarım ve burada sayılmayan pek çok sektörde sistemlerin işleyişi elektronik olarak kontrol edilmektedir.[281] Bu alanlardan herhangi birinin siber saldırılara uğraması ulusal güvenlik için ciddi tehdit oluşturmaktadır.

---

[279] Sait Yılmaz, ***ABD İstihbaratı 1947-2013***, Kripto Yayınevi, Ankara, 2013, s.242-243.
[280] Egmont R. Koch ve Jochen Sperber, ***Bilgi mafyası: Gizli Servisler, Bilgisayar Casusluğu ve Yeni Bilgi Karteli***, Çev. Kaan Ökten, Sarmal Yayınevi, İstanbul, 1996, s.145.
[281] Haydar Çakmak ve Cenker Korhan Demir, ***a.g.m.***, s.28.

Ülkelerde yukarıda sayılan alanlarda ve bunların dışındaki birçok sahada güvenliklerini sağlamak maksadıyla yazılım ve donanım güvenliği şirketleri ile beraber çalışmaktadır. Örneğin, RSA Security firması, kriptoloji alanında ürettiği yazılım ve donanımlar ile ABD'nin en saygın güvenlik firmalarından biridir. Buna rağmen siber saldırıya uğramış ve sahip olduğu verilerin bir kısmı çalınmıştır. Siber saldırganlar bunu yaparken öncelikle firma çalışanları hakkında sosyal medya üzerinden araştırma yapılarak onların adları ve e-posta hesapları ele geçirilmiştir. Daha sonra şirketteki bir grup çalışana, onların ilgisini çekecek olan "2011 Recruitment plan.xls" (2011 işe alım planı) isimli bir Excel dosyası gönderilmiştir. Excel dosyası, Adobe Flash yazılımının güvenlik açığının kod parçalarını içermektedir. Çalışanlardan biri, e-postasındaki bu Excel dosyasını açtığında zararlı yazılım aktif hale gelmekte ve yazılım bilgisayara kurularak, şirket dışındaki bir bilgisayarla irtibata geçmektedir. Böylece siber saldırıyı yapanlar, kendi bilgisayarından firma bilgisayarını yönetebilmektedir. Daha sonra ise sistem yöneticisinin hesabını ele geçirerek sunuculara erişim hakkı kazanmıştır. Kritik verileri, kendi belirlediği ara sunuculara kopyalayarak şifrelemiş ve orijinallerini silmiştir. Son olarak ise şifrelediği şirket verilerini kendi bilgisayarına kopyalamıştır.[282]

Başka bir örnekte ise, 1999 yılında ABD Hava Kuvvetleri hedef alınmıştır. Yapılan siber saldırı sonucunda ABD'de ki bir hava üssünden büyük miktarda veri çalınmıştır. Hava Kuvvetleri veri çalınma esnasında FBI ve NSA'den yardım çağrısında bulunmuşlardır. Sonuçta Savunma ağlarından ve Enerji Bakanlığı'nın nükleer laboratuarlarından verilerin çalınmasına engel olunamamıştır.[283] Çoğu zaman yapılan siber saldırılar fark edilememektedir. Ancak bu olayda fark edilebilmesine rağmen büyük miktardaki verinin çalınmasına engel olunamamıştır. Çalınan veriler doğrudan ulusal güvenliği tehdit edebilecek bilgiler içermektedir. Veri çalınmasına engel olunamamasının en büyük sebeplerinden birinin de siber saldırıyı gerçekleştirenlerin oldukça profesyonel olmalarıdır.

Ülkeler de siber uzayda sahip oldukları bu kritik altyapıları ve sahip oldukları bilgileri korumak amacıyla çeşitli çalışmalar yapmaktadır. Bu çalışmalar neticesinde ülkeler stratejik kararlar almaktadır. Örneğin; Fransız Savunma Bakanlığı'na bağlı istihbarat örgütü olan Stratejik İşler Delegasyonu bir araştırma yapmış ve şöyle bir

[282] Anatomy of an attack, https://blogs.rsa.com/anatomy-of-an-attack/, (Erişim tarihi: 11.04.2014).
[283] Richard A. Clarke ve Robert K. Knake, ***a.g.e.***, s.60.

iddiada bulunmuştur; CIA ve NSA ajanları ile Microsoft yetkilileri arasında gizli bir ortaklık kurulmuş ve Windows İşletim Sistemi'nin içerisine "casus program" yerleştirilerek, bu işletim sistemini kullanan bilgisayarlardaki bilgiler farklı yerlere aktarabilmektedir.[284] Çin, Almanya, Fransa ve birçok ülke "Microsoft ürünlerini" kamu kurumlarında kullanmamaktadır. Bunun yerine kaynak kodları açık ve millileştirilmeye yatkın Linux İşletim Sistemlerini kullanmaktadırlar.[285] Bu şekilde bilgi altyapılarını dış tehditlere karşı koruma konusunda çok önemli bir adım atmışlardır. İşletim sistemleri içerisine yerleştirilebilecek arka kapı vb. yazılımları ile ülkelerin kamu kurumlarının sahip olduğu kritik bilgilerin başkaları tarafından ele geçirilmesi ve siber saldırıların bir kısmının önüne geçilerek, ulusal güvenliklerini sağlama adına büyük mesafe almışlardır. 21. yüzyılın bilgi çağı olduğu kabul edildiğinde sahip olunan kritik bilgilerin muhafazası ve siber saldırılara karşı korunmasının önemi bir kez daha ortaya çıkmaktadır.

Günümüzde bir devletin ulusal güvenliğine zarar vermek, bir kişinin evinden bile yapabileceği bir eylem haline gelebilmektedir. Örneğin, 2000 yılında ABD ordusuna ait uzay gemileri, roketler ve uyduları yönlendirmek için kullanılan çok gizli bilgisayar sistem kodları bilgisayar korsanları tarafından çalınabilmiştir.[286] Her geçen gün siber saldırı yapmak için bireylerin sahip olması gereken bilgi birikimi azalmaktadır. Böylece gelecekte çok az siber korsanlık bilgisine sahip olan bireyler siber uzayda önemli bilgi kaynaklarına ulaşabileceklerdir. Bu durum teknoloji bağımlılığı artışına paralel olarak ortaya asimetrik hasım ve asimetrik tehditler ortaya çıkaracaktır.

Bir başka olay ise, 2002 yılından itibaren ABD Savunma Bakanlığına karşı Çin tarafından yapılan siber istihbarat faaliyetlerinin gayri resmi adı olan Titan Rain'dir. ABD Hava Kuvvetlerinden General William Lord'a göre, Çin, ABD'nin gizlilik dereceli olmayan askeri iletişim ağından 10 ila 20 terabayt boyutunda veri çalmıştır. Bu verilerin ABD Kara Kuvvetleri Bilgi Sistemleri Mühendislik Komutanlığı, Deniz Okyanus Sistemleri Merkezi, Füze Savunma Ajansı ve Sandia Milli Laboratuvarlarından ele geçirildiği belirtilmiştir. 2008 yılında, ABD Savunma Bakanlığı iletişim ağına bağlı bilgisayarlarda 43880 adet zararlı faaliyet (siber

[284] Ömer Özkaya, ***a.g.e.***, s.280.
[285] Gültekin Avcı, ***a.g.e.***, s.39.
[286] Hacker Gets Hold of Top Secret U.S. Space Codes, http://membrane.com/security/secure/Top_Secrets.html, (Erişim tarihi: 15.04.2014).

istihbarat girişimi, saldırı girişimi, virüs vb.) tespit edildiği ifade edilmiştir.[287] Bu saldırılarda sadece ABD kamu sektörü siteleri değil, devletle işbirliğindeki önemli özel sektör de hedef alınmıştır. Bunlar arasında Lockheed Martin, Boeing, Raytheon vb. bulunmaktadır.

Başka bir yaşanmış olay ise, 12 Ocak 2010 tarihinde Google firması tarafından duyurulan, McAfee firması tarafından ismi konulan ve Microsoft Internet Explorer yazılımındaki açıklığı kullanarak bilgisayarlardan veri çalmayı amaçlayan siber casusluk eylemidir. Internet Explorer'daki güvenlik açığı yüzünden, zararlı bir web sitesine bağlanan kullanıcıların bilgisayarına otomatik olarak casus yazılım yüklenmekte ve bilgisayarın kontrolünü ele geçirerek bilgisayardaki verileri çalmaktadır. Google ve aralarında ABD'li savunma sanayi firmalarının da olduğu 20 civarında şirketten çok miktarda kişisel ve kurumsal verinin çalındığı ileri sürülmüştür. Bu olay üzerine Google firması, Çin kaynaklı siber saldırılara maruz kaldığını belirtmiş ve eş zamanlı olarak dönemin ABD Dışişleri Bakanı Hillary Clinton, Çin'i kınamış ve bu konuda bilgi talep etmiştir.[288]

Diğer çarpıcı bir olay ise, Kanadalı araştırmacılar tarafından 2009 yılı Mart ayında yayımlanan bir raporla öğrenilmiştir. Tibet'in ruhani lideri Dalay Lama'nın bürosunun bilgisayarında herhangi zararlı bir yazılım olup olmadığını öğrenmek amacıyla başlatılan bu araştırma bir "siber istihbarat" ağını ortaya çıkarmıştır. Elde edilen sonuçlara göre, yaklaşık iki yıllık süre içerisinde 103 ülkede 1295 bilgisayara sızılmıştır. Sızılan bu bilgisayarlar içerisinde elçilikler, bakanlıklar ve diğer devlet kuruluşları bulunmaktadır. Ayrıca sızılan bu bilgisayarlardan ortam dinlemesinin ve görüntü alınmasının mümkün olduğu anlaşılmıştır. Eylemi gerçekleştirenleri tespit etmek mümkün olmamakla beraber şüpheli dört kontrol servis sağlayıcının üçünün Çin'de olduğu tespit edilmiştir.[289] Çin'in, siber istihbarat alanında Dünya'da ki önde gelen ülkelerden biri olduğu kabul edilmektedir. Dünya'da siber istihbarat alanında en fazla yatırım yapan ülkelere bakıldığında ABD, Çin, Rusya ve İsrail'in ön plana çıktığı ve özellikle bu alanda ABD ve Çin arasında çok büyük çekişmeler yaşandığı değerlendirilmektedir.

---

[287] Jeffrey Carr, ***Inside Cyber Warfare***, Published by O'Reilly Media, USA, 2012, p.4.
[288] Operation Aurora,
http://en.wikipedia.org/wiki/Operation_Aurora,
(Erişim tarihi: 15.04.2014).
[289] Haydar Çakmak ve Cenker Korhan Demir, ***a.g.m.***, s.47-48.

Kaspersky Lab'in 2014 yılındaki son keşfi "Maske", karmaşık yapısı ile şimdiye kadar karşılaşılan en gelişmiş siber casusluk operasyonudur. Arkasında bir devletin olduğu düşünülen bu tehdit Türkiye'yi de etkilemiştir. "Maske"yi özel kılan, saldırganlar tarafından kullanılan araçların karmaşıklığıdır. Maske'nin öncelikli hedefleri arasında, devlet kurumları, diplomatik ofisler ve elçilikler, enerji, petrol ve gaz şirketleri, araştırma kuruluşları yer almaktadır. Bu hedefli saldırının Ortadoğu ve Avrupa'dan Afrika ve Amerika'ya kadar uzanan 31 farklı ülkede tespit edildiği belirtilmektedir. Saldırganların temel amacı ise, virüs bulaşmış sistemlerdeki hassas verileri toplamak olarak açıklanmıştır.[290]

Yukarda anlatılan örnek olaylardan da anlaşılacağı gibi gelecekte siber uzayda kendine yaşam sahası bulabilen ve bunu koruyabilen devletlerin, ulusal güvenliklerini sağlayarak, bağımsız olarak varlıklarını devam ettirebilecekleri öngörülmektedir. Gelecekte siber saldırılara hazır olmayan ülkeler, siber istihbarata önem veren ülkeler karşısında çok zor durumda kalacaklardır. Bu çerçevede istihbarat örgütleri 21. yüzyıldaki hedeflerine karşı başarılı olmak istiyorsa teknolojisinde esaslı bir başkalaşım geçirmek zorundadır.[291] Bu değişimin içerisinde siber istihbarat faaliyetlerine önem verilmesi gerektiği değerlendirilmektedir.

3.3. ABD, RUSYA VE ÇİN'İN SİBER İSTİHBARAT SİSTEMLERİ

Ülkerler yıllardan beri casusluk yapma ve istihbarat toplama faaliyetleri yapmakta ve buna devam etmektedirler. Teknolojik gelişmelerin ortaya çıkması ile siber istihbarat bu alana yeni bir soluk getirmiştir. Siber istihbarat, geleneksel istihbarattan çok daha kolay ve tehlikesizdir. Siber istihbarat için kullanılan yöntemler de karşıdaki sisteme hasar veren ve sabotaja yol açabilecek etkiler doğurabilmektedir.[292]

Siber istihbarat ile ilgili birçok ülke çalışmalar yürütmektedir. Özellikle bir kısım ülkeler bundan çok büyük avantajlar elde etmektedir. Ancak hiçbir ülke siber istihbarat sistemini ve bu alanda sahip olduğu imkân ve kabiliyetleri açıklamamaktadır. Bu nedenle elde edilen bilgiler kısıtlı kalmaktadır.

---

[290] Dünya'nın en büyük siber casusluk operasyonu!, http://www.aksam.com.tr/ekonomi/teknoloji/dunyanin-en-buyuk-siber-casusluk-operasyonu/haber-284207, (Erişim tarihi: 15.04.2014).

[291] James Bamford, **Sırlar *Evreni: ABD Ulusal Güvenlik Dairesi'nin Dinleme ve İstihbarat Ağı***, Çev. Suat Kemal Angı, Dost Kitabevi Yayınları, Ankara, 2009, s.702.

[292] Richard A. Clarke and Robert K. Knake, ***Cyber War: The Next Threat To National Security and What To Do About It,*** HarperCollins Publishers, 2010, p.150-153.

Bu bölümde devletlerden öne çıkanlarının siber istihbarat sistemleri açıklanmaktadır. Bu sebeple ABD, Çin ve Rusya ele alınacaktır.

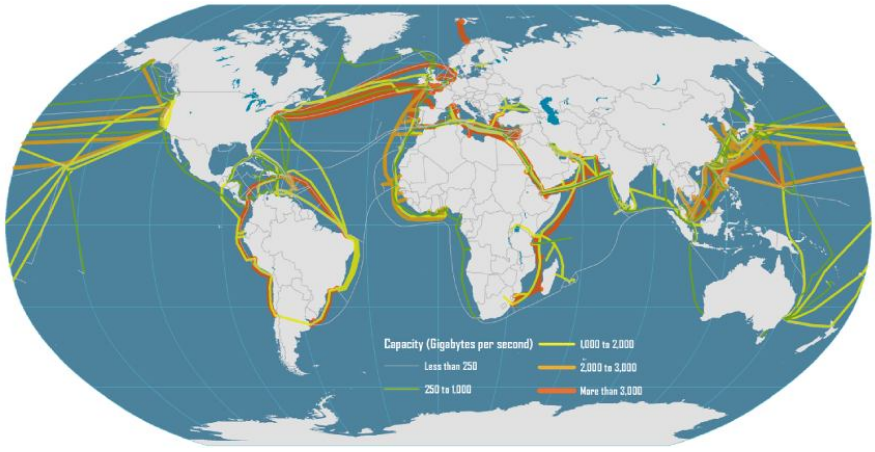
3.3.1. Amerika Birleşik Devletleri Siber İstihbarat Sistemi

ABD siber uzayı yeni bir harekât ortamı olarak kabul etmiştir. Bu atılan adımla birlikte kara, hava, deniz, uzaydan sonra beşinci harekât ortamı siber uzay olmuştur. Bu sebeple ABD ordusu, diğer harekât ortamlarında olduğu gibi siber uzayda da faaliyetlerini planlamakta ve icra etmektedir.

ABD ordusu, herhangi bir savaşı sadece video ekranı, klavye ve fare (Mouse) ile kazanmayı hedeflemektedir. Pentagon yetkilileri, bilgisayar savaşlarının en büyük zaafının, kendi sistemlerinin de başka ülkeler tarafından yok edilebilmesi ihtimali olduğunu belirtmektedir.[293]

Kıtasal bazda ki LAN (Yerel bölge ağı)'lar küresel olarak dünyayı paylaşan daha büyük WAN (Geniş bölge ağı)'lara bağlanmıştır. Bunların ana ağ protokolü İnternet Protokolü (IP)dür. Bu küresel ağ NSA'nın ana bilgisayar haberleşme ağı olan Pathway'i içerir. Avrupa ile Asya, Okyanusya, Afrika ve Güney Amerika haberleşmeleri normalde ABD yoluyla yapıldığı için iletişim istihbarat ağı büyük önem kazanmıştır.[294] Aşağıdaki haritada kıtaları birbirine bağlayan küresel denizaltı kablo ağı yer almaktadır.

Harita-1: Küresel Denizaltı Kablo Ağı[295]



[293] Sait Yılmaz, ***21. Yüzyılda…a.g.e.***, s.436.
[294] Sait Yılmaz, ***21. Yüzyılda…a.g.e.***, s.80.
[295]Global Submarine Cable Network, http://people. hofstra.edu/geotrans/eng/ch2en/conc2en/global_submarine_cable_network.html, (Erişim tarihi: 11.04.2014).

Temelinde ABD siber güvenliğini sağlamak amacıyla üç ana sektörde yoğunlaşacaktır. Bunlardan ilki internet omurgasıdır. Binlerce millik fiber optik kabloya sahip ana şirketler, denizaltı kabloları ile de dünyanın geri kalanına bağlanarak omurgayı oluşturmaktadır. Bu internetin omurgası korunduğu takdirde ABD altyapısının çoğu da korunmuş olacaktır. İkincisi ise elektrik şebekesinin güvence altına alınmasıdır. Son olarak ise savunma bakanlığının korunmasıdır.[296]

ABD siber savaşı yürütebilmek amacıyla 2009 yılında bir generalin komutası altında ABD Siber Kurmay Başkanlığı kurulmuş ve bilişim ile interneti silah gibi kullanma vazifesi ile görevlendirilmiştir. Benzer yapılar Rusya, Çin ve bir dizi başka ülkede de mevcuttur. Bu askeri ve istihbarat toplama yapıları "lojik bombalar" ve "tuzak kapılar" kullanarak siber çarpışma alanları oluşturmaktadırlar.[297]

2011 tarihli ABD Savunma Bakanlığının Siber Uzayda Harekât Stratejisi(Department of Defence Strategy for Operating in Cyberspace) belgesi genel olarak verilerin çalınması, bilgilerin değiştirilmesi ve verilerin imha edilmesi girişimlerine karşı odaklandığı değerlendirilmektedir. Bu strateji belgesinde üzerinde durulan beş stratejik girişim aşağıdadır;[298]

- ABD Savunma Bakanlığı'nın siber uzayın tüm imkânlarından faydalanabilecek şekilde organize edilmesi, eğitimi ve donanımı için tüm siber uzayın harekât alanı olarak kullanılması,
- ABD Savunma Bakanlığı ağ ve sistemlerinin korunması için yeni savunma konseptlerinin uygulanması,
- Devletin hep beraber siber güvenlik stratejisinin etkinleştirilmesi için, ABD'deki diğer bakanlıklar, kamu kurumları ve özel sektör ile ortak çalışmalar yapılması,
- Siber güvenliğin güçlendirilmesi için ABD'nin müttefikleri ve uluslar arası ortakları ile güçlü ilişkiler kurulması,
- Yetenekli siber işgücü ve hızlı bir şekilde elde edilecek teknolojik yenilikler vasıtasıyla milli yeteneklerin geliştirilmesi.

[296] Richard A. Clarke ve Robert K. Knake, ***Siber Savaş…a.g.e.***, s.84-89.
[297] Richard A. Clarke ve Robert K. Knake, ***Siber Savaş…a.g.e.***, s.IX - X.
[298] ***Department of Defense Strategy for Operatıng in Cyberspace***, Department of Defense, USA, 2011, p.5-10.

Yukarıda sayılan stratejik girişimler vasıtasıyla ABD Savunma Bakanlığı, ABD'nin kritik altyapılarına (Enerji, iletişim, finans, ulaşım vb.) ve Savunma Bakanlığı sistemlerine ülke içerisinden veya dışarısından yapılabilecek siber saldırıların önüne geçebilmeyi öngörmektedir.

ABD siber uzayda çeşitli faaliyetler yürütmekte ve belirli bir stratejinin yanında birde gizli siber strateji takip etmektedir. Çifci'ye göre ABD gizli siber stratejisinin bir bölümü aşağıdaki unsurlardan oluşmaktadır;[299]

- Barış zamanında, müttefikler dâhil tüm ülkelerin sistemlerine sızmak için siber saldırılar düzenlemek. Saldırıların temel amacı sistemleri çökertmek değil, sistemlerden bilgi çalmak ve sistemler hakkında bilgi toplamaktır.
- Barış zamanında yazılım ve donanımlara tuzak kapılar yerleştirmektir. Bu maksadı gerçekleştirmek amacıyla işletim sistemi geliştiren, yazılım ve donanım geliştiren özel firmalar ile NSA aracılığıyla gizli anlaşmalar yaparak, barış zamanında veri çalmak, savaş zamanında ise hedefi etkisiz hale getirmek kolay olacaktır.
- Google, Gmail, Facebook, Twitter gibi kişisel bilgilerin girildiği, insanlarla iletişime geçilen siteleri desteklemek. Buradaki verileri otomatik olarak, ülke bazında, dil bazında, kelime bazında gruplamak ve arşivleyerek, zamanı geldiğinde, herhangi bir kişinin lehinde veya aleyhinde kullanmak. Bu çerçevede, bu sitelere erişimde tüm trafik şifreli olmalı ki, başka ülke veya gruplar dinleyemesin.

Yukarıdaki bilgiler ışığında ABD'nin siber uzaydaki ağırlığı net bir şekilde görülebilmektedir. ABD, gelecekte bu alanda yapılabilecekleri öngörerek kendi siber çalışmalarını yapmaktadır. Bu çerçevede siber istihbarat, ABD'nin vazgeçemeyeceği unsurlardan biridir. Bu alanda büyük yatırımlar yapmış, yapmakta ve gelecekte de bu doğrultuda hareket edecektir.

3.3.2. Çin Siber İstihbarat Sistemi

Birinci Körfez Harekâtı'nda, ABD'nin savaş tekniklerini gören Çinliler, ABD'ye göre on yıllarca geri olduklarının farkına vardılar. ABD, Saddam'ın Rus ve Çin malı tanklarını, toplarını ve tüm askeri teçhizatını kolaylıkla imha etti. 1990'lı yılların ortalarında Çin, Birinci Körfez Harekâtı'ndan çıkarttığı dersler doğrultusunda, kendi

[299] Hasan Çifci, ***a.g.e.***, s.79-80.

stratejisini değiştirdi. Eski stratejileri, sayısal üstünlükleri ile savaş çıktığı takdirde ABD'yi yenmek şeklinde açıklanmıştı. Bu strateji artık işe yarayamayacaktı. Bu nedenle 1990'lı yılların sonlarında, Çin de aynı ABD gibi siber savaş birlikleri kurmuştur.[300] Çin bu süreçte siber alanda büyük adımlar atmıştır. Teknolojik altyapısını ve yetişmiş insan gücünü oluşturmayı başarmıştır.

2010 yılında, dünyadaki birçok devlete ve özel teşebbüse ait bilgisayar sistemlerine girilmiş, bu girişlerin bir kısmının başlangıç noktasının Çin olduğu belirlenmiştir. Bu girişlerin temelde bilgisayarlardan veri çalma (siber istihbarat) amaçlı olduğu ortaya çıkarılmıştır. Ancak, veri çalmak için kullanılan karmaşık ve yüksek teknik beceri isteyen yöntemlerin, sistemlere saldırmak için de kullanılabilmesi, tehdidin boyutunu daha da büyütmektedir.[301]

Great Firewall of China, Çin devleti tarafından, internet erişiminin filtrelenmesi ve zararlı olan sitelere erişimin engellenmesi ve bazı sitelere erişimin kısıtlanmasına ilişkin internet sansürü projesidir.[302] Bu projenin en önemli özelliği, Çin istediği zaman siber uzayını dış dünyaya kapatabilmesidir. Herhangi bir siber saldırı durumunda ki buna siber istihbarat saldırıları da dâhil olmak üzere, bu proje çok etkin bir şekilde kullanılabilecektir.

ABD'deki bir siber güvenlik şirketi olan Mandiant, 2013 yılında yayınladığı raporda, Çin ordusunun içindeki gizli bir birimin, "dünyanın en yayılmacı casusluk grubu" olduğunu öne sürmüştür. Mandiant şirketine göre, "61398" adlı birlik, dünya genelinde en az 141 kuruluştan "sistematik olarak yüzlerce terabaytlık veri" çalmıştır. Mandiant şirketi 2004'ten bu yana veri güvenliğinin ihlal edilmesiyle ilgili raporunda, "bu faaliyetleri yürütenlerin esas olarak Çin'de üslendiğini ve Çin hükümetinin onlardan haberdar olduğunu" vurgulanmaktadır. Hack'leme faaliyetlerinin izi sürüldüğünde, Şangay'ın Pudong bölgesindeki 12 katlı bir binaya ulaşıldığını aktaran Mandiant Şirketi, Çin Halk Kurtuluş Ordusu'nun 61398 numaralı birliğinin de aynı yerde olduğuna dikkat çekmektedir.[303]

---

[300] Richard A. Clarke ve Robert K. Knake, ***Siber Savaş…a.g.e.***, s.81.
[301] Hasan Çifci, ***a.g.e.***, s.299.
[302] Internet censorship in the People's Republic of China, http://en.wikipedia.org/wiki/Internet_censorship_in_the_People%27s_Republic_of_China, (Erişim tarihi: 13.04.2014).
[303] 61398: Çin'in siber birliği en büyük 'casusluk grubu', http://www.bbc.co.uk/turkce/haberler/2013/02/130219_china_cyber_espionage.shtml, (Erişim tarihi: 11.04.2014).

Mandiant Raporuna göre, adı geçen siber casusluk grubunun özellikleri şöyledir:[304]

- Grubun yüzlerce, belki binlerce üyesi iyi derecede İngilizce ve ileri bilgisayar ağ güvenliği bilgisine sahiptir.
- Hack'lenen 20 farklı sektörden, 141 şirketin %87'si İngilizce konuşulan ülkelerde kuruludur.
- Grup, aynı anda düzinelerce ağdan veri sızdırabilmektedir.
- Yüzlerce terabaytlık iş planı, fiyatlama belgesi, kullanıcı bilgisi, e-posta adresi ve iletişim listesi grup tarafından çalınabilmektedir.
- İçine sızılan bir ağda ortalama 356 gün kalınmaktadır. En uzun süre bir ağ içerisinde kalınma süresi 1764 gündür.
- Hedef alınan sektörler, Çin'in Beş Yıllık Plan kapsamında stratejik olarak tanımladığı sektörlerle örtüşmektedir.

Çin'in bu ve benzeri casusluk gruplarının olduğu öngörülmektedir. Bu casusluk gurupları vasıtasıyla, klasik istihbarat yöntemleriyle elde edemeyeceği, kritik verileri elde etmiştir. Geçmişte yaşanan örneklere ve Çin'in çalışmalarına bakıldığında gelecekte de siber istihbaratta ileri düzeydeki ülkeler arasında yer alacaktır.

3.3.3. Rusya Siber İstihbarat Sistemi

Rusya'da 2000 yılı sonrasında ulusal güvenlik politikaları gözden geçirilmiş ve bilgi harekâtı stratejilerine ağırlık verilmiştir. Çevresinde bulunan ülkeleri kendi çıkarları doğrultusunda hareket etmeleri için siber saldırıları da kullanmıştır.

Kişisel verilerle ilgili Rus 152 numaralı Federal Kanun'da, belirtilen çok kısıtlı durumlar haricinde, Rusya'daki internet servis sağlayıcıların yabancı bir ülkenin yetkili birimlerine bilgi vermesi yasaklanmıştır. Bu yasakla birlikte, yabancı bir ülkeye yapılan siber saldırılarla ilgili bir araştırma çerçevesinde, saldırıların Rusya üzerinden gelmesi durumunda, saldırı kaynağına ilişkin bilgilere ulaşılmasının önü kapanmıştır.[305] Buda önemli avantajlar sağlayabilmektedir. İyi Rus siber hackerları ağlara girmekte asla zorlanmamaktadırlar. Ağ operatörleri internet bağlantılarını kestikleri zaman dahi ağdan içeri sızabilmektedirler. Bu gerçekleştiği takdirde bile

[304] APT1 Exposing One of China's Cyber Espionage Units Report, Mandiant Company, USA, 2013, p. 20-26.
[305] Hasan Çifci, ***a.g.e.***, s.86.

sızıntıyı tespit eden ülke Rusya'dan bilgi talebinde bulunsa bile cevap alamamaktadır.

ABD'li uzmanlara göre, Rusya sahip olduğu siber saldırı araçları ile Çin'den daha tehlikelidir. Moskova'da FAPSI(Devlet İletişim ve Bilişim Federal Komisyonu) isimli, NSA benzeri bir kuruluş vardır. Sovyetler Birliği çöktükten sonra, 2003 yılında FAPSI'nın ismi "Özel İletişim ve Bilişim Servisi" olarak değiştirilmiştir. Güney Rusya'da Voronozh kentinde, FAPSI dünyanın en büyük hacker okulunu işletmektedir.[306]

Savunma ve saldırıya yönelik bilgi harekâtı kabiliyetleri Savunma Bakanlığına bağlı Elektronik Harp Birliklerinde toplanmıştır. Voronezh kentinde, 2001 yılından itibaren profesyonel siber korsanlık eğitimi veren Voronezh Askeri Telsiz-Elektronik Enstitüsü yer almaktadır. 2008 yılında Voronezh Askeri Havacılık Mühendisliği Üniversitesi kurulmuştur. 15 bin personel ve 6 bin öğrenci kapasitesine sahip olan okul, bilgi güvenliği ve bilgi harekâtı üzerine eğitim vermektedir.[307]

Rusya kaynaklı siber istihbarat faaliyetleri ile ilgili yaşanmış örnekler bulunmaktadır. Bunlardan biride örneğin; 1998 yılında ABD Savunma Bakanlığı Pentagon'un internet sitelerine siber saldırılar düzenlendiği anlaşılmıştır. Ayışığı Labirenti adı verilen siber saldırıların, ABD hükümetinin internet sitelerine yapılan en ciddi siber saldırı olduğu belirtilmiştir. Ayışığı Labirenti saldırısı, Amerikan Savunma Enformasyon Sistemleri Ajansı'nda çalışan bir uzman tarafından fark edilmiştir. Siber saldırganların Pentagon'un gizli dosyalarına, "tünel kazmak" denilen bir yöntemle girdiği tespit edilmiştir. Amerikan Ulusal Güvenlik Ajansı danışmanlarından James Adams, saldırıların 7 Rusya adresinden yapıldığını tespit edildiğini belirtmiştir.[308]

[306] Richard A. Clarke ve Robert K. Knake, ***Siber Savaş…a.g.e.***, s.37.
[307] Hasan Çifci, ***a.g.e.***, s.45.
[308] Ömer Özkaya, ***a.g.e.***, s.299-300.

SONUÇ

21. yüzyılda ulusal güvenliğin sağlanması çok boyutlu olarak ele alınmalı ve çalışmalar bu yönde yapılmalıdır. Sadece sınır güvenliğinin tesisi için çaba gösterilmesi günümüzde ulusal güvenliğin sağlanmasında yeterli görünmemektedir. Teknolojinin ulaştığı boyutlar ve teknolojik bileşenlerin başta devlet kurumları olmak üzere hayatın her alanında ve aşamasında yer alması, siber güvenliği ve bu çerçevede siber istihbaratı, ulusal güvenliğin önemli ve ayrılmaz parçası kılmaktadır.

Ulusal güvenliğin sağlanmasında güvenlik ortamını şekillendiren pek çok yeni aktör ve vasıta ortaya çıkmıştır. Ulusal ve uluslar arası düzeyde doğru politikalar üretebilmek ve uygulayabilmek için ulusal güvenliğe yönelen tehdit ve bunların kaynaklarını iyi algılayabilmek gerekmektedir. Bu doğrultuda ülkelerin karşı karşıya olduğu fırsatlar ve tehditler gerçekçi olarak öngörülmeli, doğru analiz edilebilmeli ve uygun vasıtalar ile karşı konulmalıdır.

Günümüzdeki teknolojik gelişmeler çerçevesinde ve özellikle internet kullanımının yaygınlaşması ile bilginin yayılması ve kullanımı kolaylaşmış ancak bilginin korunması da bir o kadar zorlaşmıştır. 21. yüzyılda gelişen teknoloji, dünyada meydana gelen değişimler, hemen hemen bütün ülkelerin bilgisayar, internet ve iletişim teknolojilerine bağımlı hale getirmiştir. Bu bağımlılıkta beraberinde karşılaşılabilecek risk durumlarının da artmasına yol açmaktadır.

Bilginin güç olduğu günümüzde, bilginin başkalarının eline geçmesine engel olmakta önemli bir konudur. Ülkelerin temel görevlerinden biri ulusal güvenliğin sağlanmasıdır ve günümüzde ülkelerin sahip olduğu kritik bilgiyi koruması da ulusal güvenliğin sağlanması kapsamındadır. Bu çerçevede siber uzayın güvenliğinin de sağlanması gerekmektedir. Günümüzde kritik altyapıların ve kamu kurumlarının bilgisayarlara olan bağımlılığı, siber uzayın güvenli olmaması ulusal güvenlik kavramını eskisinden çok daha farklı boyutlara taşımaktadır.

Günümüzde devlet, özel sektör kurumları ve bireyler giderek artan bir şekilde siber uzaya bağımlı hale gelmektedir. Bu alanda sahip olunan bilgilerin korunması ve bu alana yapılabilecek siber saldırıların önüne geçilmesi ulusal güvenlik açısından bir gereklilik olduğu değerlendirilmektedir.

Siber saldırılar ile nükleer santrallerde radyasyon sızıntılarına sebep olunabileceği, doğal gaz borularının patlatılabileceği, raylı sistemlerin kontrollerinin

ele geçirilerek kazalara sebebiyet verilebileceği, elektrik santrallerinin devre dışı bırakılabileceği, orduların silah sistemlerinin çalışamaz hale getirilebileceği, uyduların yörüngelerinden çıkartılabileceği, e-devlet faaliyetlerinin etkisiz hale getirilebileceği, ülke ekonomisinde önemli bir konumu olan bankacılık sisteminin çökertilebileceği, iletişim ağlarının devre dışı bırakılabileceği düşünüldüğünde ulusal güvenlik açısından siber uzay, siber saldırı ve bu çerçevede siber istihbaratın öneminin anlaşılabileceği öngörülmektedir. Bu çerçevede yapılacak bir siber saldırı veya siber istihbaratın ilk hedefi yukarıda sayılan altyapı sistemleri olacaktır.

Yukarıda belirtilen ve ulusal güvenlik açısından son derece önemli sayılan altyapı sistemlerinin siber saldırılar ve bu kapsamda siber istihbarat faaliyetlerinden korunması maksadıyla yapılabilecekler değerlendirilmiş ve bu çerçevede yapılabilecekler aşağıda açıklanmıştır.

Günümüz gelişmelerine bakıldığında elektronik ve ileri teknolojilerindeki büyüme ivme kazanarak devam edecek ve bu çerçevede siber istihbarat ta aynı doğrultuda gelişecek ve değişecektir. İlerde farklı siber saldırı yöntemlerinin ortaya çıkarak, siber istihbaratın farklı metotlarla yapılabileceği değerlendirilmektedir. Bu nedenle ülkeler, bilim ve teknoloji alanındaki gelişmeleri yakından takip etmelidir.

İlerleyen dönemlerde, bilgisayarların, internetin ve siber uzayın günlük hayatın ve çalışmaların bir parçası olacağından, devlet siber istihbarata yönelik AR-GE çalışmalarında bulunmalıdır. AR-GE faaliyetleri çeşitli kurumlarla ve özellikle üniversitelerle ortak çalışmalar yürütülerek, bu alanda önemli adımlar atılmalıdır.

Siber istihbarat faaliyetleri ulusal güvenliği tehdit edebildiğinden, bunlarla mücadelede yasal düzenlemeye ihtiyaç duyulmaktadır. Ayrıca siber saldırılar ve siber istihbarat konusundaki gelişmeler ve yöntemler çok hızlı bir şekilde değişmektedir. Siber saldırılar ve bu çerçevede siber istihbarat faaliyetleri konusunda yasal düzenlemeler ihtiyaçlar doğrultusunda değiştirilmelidir.

Siber istihbarat yapılanmasının tek bir elden yönetilmesi gerekmektedir. Siber saldırılara ve bu kapsamda siber istihbarata karşı mücadelede özel sektör ile kamu sektörü arasındaki işbirliği büyük önem arz etmektedir. Kamu sektörü ve özel sektör siber uzayda ulusal güvenliğin sağlanması ve bu alandan gelebilecek siber saldırılara karşı ortak çalışma yapmalıdır. Günümüzde özel sektörün faaliyetleri de

ulusal güvenliği doğrudan etkileyebilmektedir. Bu sebeple özel sektörün siber uzay çalışmaları da büyük öneme haizdir.

Ayrıca kritik altyapı sistemlerinde kullanılan yazılım ve donanımlar mümkün olduğu kadar milli olmalıdır. Kritik altyapı sistemlerinde kullanılmak üzere yurt dışından alınan yazılım ve donanımlar beraberinde riskleri de getirmektedir. Özellikle yazılımların içerisine yerleştirilmesi ihtimali bulunan gizli kodlar, arka kapılar vb. yazılımlar, sistemi siber saldırılara açık hale getirmektedir. Yaşanmış örnek olaylar değerlendirildiğinde yukarıdaki değinilen durumların gerçekleştiği görülmektedir. Bu nedenle, özellikle gelişmiş ülkeler kamu kurumlarındaki bilgisayarlarında kendi işletim sistemlerini kullanmaktadır.

Kamu hizmeti ağları ve internet arasında bağlantı olmaması gerekmektedir. E-devlet kapsamında yürütülen hizmetler siber uzayda internet vasıtasıyla yapıldığı takdirde siber saldırılara açık hale gelebilmekte ve saldırganlar buldukları açık kapılardan siber uzaydaki işlem yapılan bilgileri ele geçirebilmektedirler. Bu nedenle kamu faaliyetleri mümkün olduğu kadar internet dışında farklı bir ağ üzerinden yapılmalıdır.

Her seviyede siber istihbarat, siber saldırı, siber güvenlik vb. ile ilgili bilgilendirme ve bilinçlendirme çalışmaları yapılmalıdır. Özellikle kritik altyapıların güvenliğinden sorumlu personelin eğitimine gereken önem verilmeli ve bu doğrultuda yeterli mali kaynak ayrılmalıdır. Eğitimli ve nitelikli personelin her zaman anahtar role sahip olduğu akıldan çıkarılmamalıdır.

KAYNAKÇA

KİTAPLAR

ARI Tayyar, Uluslararası ilişkiler Teorileri, Alfa Yayınları, İstanbul, 2006.

AVCI Gültekin, İstihbarat Teknikleri: Aktörleri - Örgütleri ve Açmazları, Timaş Yayınları, İstanbul, 2004.

BAL Mehmet Ali, Modern Devlet ve Güvenlik, IQ Kültür Sanat ve Yayıncılık, İstanbul, 2003.

BAMFORD James, Sırlar Evreni: ABD Ulusal Güvenlik Dairesi'nin Dinleme ve İstihbarat Ağı, Dost Kitabevi Yayınları, Ankara, 2009.

BARAZ Barış vd., Büro Teknolojileri, Anadolu Üniversitesi Yayınları, Eskişehir, 2013.

BEREN Fatih, Demokrasi ve Özgürlüğün Teminatı Olarak İçgüvenlik İstihbaratı, Alfa Yayınları, İstanbul, 2011.

BIÇAKÇI Salih, 21. Yüzyılda Siber Güvenlik, İstanbul Bilgi Üniversitesi Yayınları, İstanbul,2013.

CANBEK Gürol ve SAĞIROĞLU Şeref , Bilgi ve Bilgisayar Güvenliği: Casus Yazılımlar ve Korunma Yöntemleri, Ankara, 2006.

CARR Jeffrey, Inside Cyber Warfare, Published by O'Reilly Media, USA, 2012.

CAŞIN Mesut Hakkı, Çağdaş Dünyada Uluslararası Güvenlik Stratejileri ve Silahsızlanma, SSM Yayınları, Ankara, 1995.

CLARKE Richard A. ve KNAKE Robert K., Cyber War: The Next Threat To National Security and What To Do About It, HarperCollins Publishers, 2010.

CLARKE Richard A. ve KNAKE Robert K., Siber Savaş, Çev. Murat Erduran, İkü Yayınevi, İstanbul, 2011.

ÇAKMAK Haydar ve ALTUNOK Taner, Suç, Terör ve Savaş Üçgeninde Siber Dünya, Barış Platin Kitabevi, Ankara, 2009.

ÇİFCİ Hasan, Her Yönüyle Siber Savaş, Tübitak Popüler Bilim Kitapları, Ankara, 2013.

DEDEOĞLU Beril, Uluslararası Güvenlik ve Strateji, Yeniyüzyıl Yayınları, İstanbul, 2008.

DİNDAR İsmail, 21.Yüzyılda Teknoloji ve İstihbarat Savaşları, IQ Kültürsanat Yayıncılık, İstanbul, 2004.

ERSANEL Nedret, Siber İstihbarat: Siber ve Dijital Casusluğun Anatomisi, Asam Yayınları, Ankara, 2001.

FM 2-22.3 (FM 34-52) Human Intelligence Collector Operations, Department of the Army, Washington, 2006.

HAAG Stephen and CUMMİNGS Maeve, Management Information Systems For The Information, 6 th Edition, New York, 2007.

HERMAN Michael, Intelligence Power in Peace and War, Cambridge University Press, Cambridge, 1999.

JANCZEWSKİ Lech J. and COLARİK Andrew Michael, Cyber warfare and cyber terrorism, IGI Global, London, 2008.

KARAGÜLMEZ Ali, Bilişim suçları ve Soruşturma-Kovuşturma Evreleri, Ankara, Seçkin Yayıncılık, 2005.

KOCH Egmont R. ve SPERBER Jochen, Bilgi mafyası: Gizli Servisler, Bilgisayar Casusluğu ve Yeni Bilgi Karteli, Çev.Kaan Ökten, Sarmal Yayınevi, İstanbul, 1996.

NİŞANYAN Sevan, Sözlerin Soyağacı, Everest Yayınları, İstanbul, 2009.

NUTTER John Jacob, CIA'nın Örtülü Operasyonları, Güncel Yayıncılık, İstanbul, 2005.

ÖZDAĞ Ümit, İstihbarat Teorisi, Kripto Yayınları, Ankara, 2010.

ÖZKAYA Ömer, Zihin Kontrolü, BSR Yayın Grubu, İstanbul, 2011.

SÖNMEZOĞLU Faruk, Uluslararası İlişkiler Sözlüğü, Der Yayınları, İstanbul,2000.

ŞENEL Muazzez ve ŞENEL Turhan, İstihbarat ve Genel Güvenlik Konularımız, Emniyet Genel Müdürlüğü Yayınları, Ankara, 1997.

ŞİMŞEK Erdal ve BAHAR İlhan, Türkiye'de İstihbaratçılık ve Mit, İstanbul, Kum Saati Yayınları, 2004.

TILISBIK Niyazi ve AKBAL Özdemir, İstihbarat ve Türkiye, Nüve Kültür Merkezi Yayınları, Konya, 2006.

TZU Sun, Savaş Sanatı, Çev. Şule Kılıçarslan, Form Yayınları, İstanbul, 1992.

TÜRKER Haşim, Avrupa Güvenlik ve Savunma Politikası, Nobel Yayın Dağıtım, Ankara, 2007, s.9

YARMAN Tolga, Geçmişte ve Bugün Nükleer Enerji Tartışması, Okan Üniversitesi Yayınları, İstanbul, 2011.

YILMAZ Sait, ABD İstihbaratı 1947-2013, Kripto Yayınevi, Ankara, 2013.

YILMAZ Sait, 21. Yüzyılda Güvenlik ve İstihbarat, Milenyum Yayınları, İstanbul, 2007.

YILMAZ Sait ve SALCAN Olay, Siber Uzay'da Güvenlik ve Türkiye, Milenyum Yayınları, İstanbul, 2008.

URHAL Ömer, Küreselleşen Dünyada Güvenlik, Adalet Yayınevi, Ankara, 2009.

MAKALELER

ALTUNOK Taner ve KATMAN Filiz, "Siber Tehdit Altyapısı ve Araçları", Suç, Terör ve Savaş Üçgeninde Siber Dünya, Barış Platin Kitabevi, Ankara, 2009, 23-54.

ALTUNOK Taner ve SÖKMEN Aşkın İnci, "Dünya'da Siber Terör Örnekleri", Suç, Terör ve Savaş Üçgeninde Siber Dünya, Barış Platin Kitabevi, Ankara, 2009, 85-110.

BALDWİN David A., "Güvenlik Kavramı", Çev. Çiğdem Şahin, Uluslararası Güvenlik Sorunları, ASAM Yayınları, Ankara, 2004, 1-36.

BALDWİN David A., "The Concept of Security", Rewiew of International Studies, 1997, Vol:23, Issue:01.

BAYLİS John, "Uluslararası İlişkilerde Güvenlik Kavramı", Uluslararası İlişkiler Dergisi, 2008, Cilt: 5, Sayı: 18, 69-85.

BİRDİŞLİ Fikret, "Ulusal Güvenlik Kavramının Tarihsel ve Düşünsel Temelleri", http://sbe.erciyes.edu.tr/dergi/2011-2/8-%20_149-169.%20syf._.pdf. (Erişim tarihi: 09.02.2014).

BRAUCH Hans Günter, "Güvenliğin Yeniden Kavramsallaştırılması: Barış, Güvenlik, Kalkınma ve Çevre Kavramsal Dörtlüsü",Uluslararası İlişkiler Akademik Dergisi, Cilt 5, Sayı 18, 2008, 1-47.

BOOTH Ken, "Güvenlik Ve Özgürleş(tir)me", Avrasya Dosyası Dergisi, Cilt: 9, Sayı: 2, 2003, 51-70.

CANBEK Gürol ve SAĞIROĞLU Şeref, "Casus Yazılımlar: Bulaşma Yöntemleri ve Önlemler", Gazi Üniv. Müh. Mim. Fak. Dergisi, Ankara, 2008, Cilt: 23, No:1, 165-180.

ÇAKMAK Haydar ve DEMİR Cenker Korhan, "Siber Dünyadaki Tehditler ve Kavramlar", Suç, Terör ve Savaş Üçgeninde Siber Dünya, Barış Platin Kitabevi, Ankara, 2009, 23-54.

ÇETİN Halis, "Liberalizmin Tarihsel Kökenleri", Cumhuriyet Üniversitesi İktisadi ve

İdari Bilimler Dergisi, Cilt:3, Sayı:1, 79–96.

ÇETİNKAYA Şeref, "Güvenlik Algılaması ve Uluslar arası İlişkiler Teorilerinin Güvenliğe Bakış Açıları", 21. Yüzyılda Sosyal Bilimler Dergisi, Sayı: 2, 2013, 239-260.

DEMİRAY Muhittin ve İŞCAN İsmail Hakkı, "Uluslararası Sistemde Güvenlik Kavramının Değişimi Ekonomik ve Jeopolitik Arka Planı", Dumlupınar Üniversitesi Sosyal Bilimler Dergisi, 2008, Sayı:21, 141-170.

DLAMİNİ Moses, ELOFF Mariki and ELOFF Jan, " Information Security: The Moving Target", Computers & Security**,** 2009, vol.28, issues 3-4, 189-198.

ERGÜL Nihal, "Yeni Güvenlik Anlayışı Kapsamında Birleşmiş Milletler'in Rolü ve Uygulamaları", Teoriler Işığında Güvenlik, Savaş, Barış Ve Çatışma Çözümleri, BİLGESAM Yayınları, 2012, 163-208.

ERİKSSON Johan and GİACOMELLO Giampiero, "The Information Revolution, Security, and International Relations: (IR) Relevant Theory?", International Political Science Review, Vol: 27, No: 3, 2006, 221-244.

GÜRSOY Barış, "Uluslararası Güvenliğin Bir Boyutu Olarak Askeri Alanda Devrim Tartışması ", Avrasya Dosyası Dergisi, Cilt: 9, Sayı: 2, 2003, 127-141.

KÜÇÜKSOLAK Övgü Kalkan, "Güvenlik Kavramının Realizm, Neorealizm Ve Kopenhang Okulu Çerçevesinde Tartışılması", Turan Stratejik Araştırmalar Merkezi Dergisi, 2012, Cilt: 4, Sayı:14, 202-208.

KÜÇÜKŞAHİN Ahmet ve AKKAN Tamer, "Değişen Güvenlik Algılamaları Işığında Tehdit ve Asimetrik Tehdit", Güvenlik Stratejileri Dergisi, 2007, Yıl: 3, Sayı: 5, 41-66.

MAURUSHAT Alana, "Zombie Botnets", Scripted, 2010, Volume 7, Issue 2, 370-383.

MİŞ Nebi, "Güvenlikleştirme Teorisi ve Siyasal Olanın Güvenlikleştirilmesi" http: //www. aid.sakarya.edu.tr/uploads/Pdf_2011_6_14.pdf, (ErişimTarihi:15.01.2014).

OĞUZLU Tarık, "Dünya Düzenleri ve Güvenlik: Ulus-Devlet Güvenlik Anlayışı Aşılıyor mu?", Güvenlik Stratejileri Dergisi, 2007, Yıl: 3, Sayı: 6, 7-41.

SANDIKLI Atilla ve EMEKLİER Bilgehan, "Güvenlik Yaklaşımlarında Değişim ve Dönüşüm", Teoriler Işığında Güvenlik, Savaş, Barış Ve Çatışma Çözümleri, BİLGESAM Yayınları, 2012, 3-67.

ŞAHİN Çiğdem, "Sözcelerin Gücü Adına, Güç Bush'ta Artık…", Uluslararası Güvenlik Sorunları, ASAM Yayınları, Ankara, 2004, 82-101.

ÜNSAL Şamil, "Milli Güç, Bileşenleri ve Vasıtaları", Türk Dünyası Araştırmaları, 2010, Sayı: 187, 27-50.

ÜNSAL Şamil, "Milli Güvenliğimizin Milletlerarası ve Küresel Boyutları", Türk Dünyası Araştırmaları, 2013, Sayı: 207, 1-12.

YARMAN Tolga, Teknoloji Alanında Türkiye'nin Güvenlik İhtiyaçları Ne Şekilde Karşılanabilir: Değişen Dünya Düzeni ve Türk Savunma Sanayi, Işık Üniversitesi,

2003, s.1.

YILMAZ Sait, “Güçsüz Güç”, Stratejik Araştırmalar Enstitüsü Güvenlik Stratejileri Dergisi, 2007, Yıl:3, Sayı:5,67-104.

YILMAZ Sait, “21’inci Yüzyılda Güvenlik Alanının Yeni Sivil Aktörleri: Özel Askeri Şirketler Ve Kontratçı Firmalar”, Güvenlik Stratejileri Dergisi, 2007, Yıl: 3, Sayı: 6, 43-70.

YILMAZ Sait, “ABD İstihbaratında Yaşanan Değişimler”, TURAN Stratejik Araştırmalar Merkezi Dergisi, 2012, Cilt: 4, Sayı: 13, 10-15.

WOLFERS Arnold, , “National Security: As an Ambiguous Symbol”, Political Science Quarterly, Vol: 67, No: 4, 1952, 481-502.

TEZLER

ATEŞ Hasan, Kamu Güvenliğinde İstihbarat Sisteminin Değerlendirilmesi, Sosyal Bilimler Enstitüsü, Atılım Üniversitesi, Ankara, 2012.

GÜNYEL Cihan, Avrupa’nın Güvenlik ve Savunma Politikalarının Oluşum ve Gelişim Süreci, Sosyal Bilimler Enstitüsü, Kadir Has Üniversitesi, İstanbul, 2011. (Yayımlanmış Uzmanlık Tezi).

KAYA Adem, Siber Güvenliğin Milli Güvenlik Açısından Önemi, Savunma Bilimleri Enstitüsü, Kara Harp Okulu, Ankara, 2012.

ÖZCAN Arif Behiç, Uluslararası Güvenlik Sorunları ve ABD’nin Güvenlik Stratejileri, Selçuk Üniversitesi, Sosyal Bilimler Enstitüsü, Uluslar arası İlişkiler Ana Bilim Dalı, Konya, 2004. (Yayınlanmamış Yüksek Lisans Tezi).

PEKER Adem, İnsani Değerler Yönelimli Psiko-Eğitim Programının Problemli İnternet Kullanımı ve Siber Zorbalık Üzerindeki Etkisi, Eğitim Bilimleri Enstitüsü, Sakarya Üniversitesi, 2013.

TORUN Abdullah, Ulusal Güvenlik ve Küreselleşme: Türkiye’nin Ulusal Güvenlik Politikasının Dönüşümünde Küreselleşmenin Rolü, Sosyal Bilimler Enstitüsü, Ankara Üniversitesi, Ankara, 2012.

RAPORLAR

AYDOĞAN Bekir ve AYDIN Hakan, Güç Kavramı, Kamu Diplomasisi ve Güvenlik Raporu, Rapor No: 11-02, Ekopolitik Uluslararası İlişkiler Masası Yayınları, İstanbul, 2011.

BARGER Deborah G., Toward A Revolution in Intelligence Affairs, RAND National Security Research Division Yayınları, 2005.

APT1 Exposing One of China’s Cyber Espionage Units Report, Mandiant Company, USA, 2013.

İNTERNET KAYNAKLARI

ABD İstihbaratı Google ve Yahoo'ya Sızmış, http://www.hurriyet.com.tr/avrupa/25015721.asp (Erişim tarihi: 10.03.2014).

Al Qaeda and the Internet:The Danger of "Cyberplanning", http://strategicstudiesinstitute. army.mil/pubs/parameters/articles/03spring/thomas.pdf, (Erişim tarihi: 12.02.2014).

Anatomy of an attack, https://blogs.rsa.com/anatomy-of-an-attack/,(Erişim tarihi: 11.04.2014).

Assange: Facebook en büyük ajan, http://www.sabah.com.tr/Teknoloji/Haber/2011/05/04/assange-facebook-dunyanin-en-buyuk-ajani-597582296690, (Erişim tarihi: 10.03.2014).

BEER Stafford, What is Cybernetics?, http://www.nickgreen.pwp.blueyonder.co.uk/beerWhatisCybernetics.pdf, (Erişim tarihi: 11.02.2014).

Caucasus Foes Fight Cyber War, http://news.bbc.co.uk/2/hi/europe/7559850.stm, (Erişim: 14.02.2014).

Cyberwar, http://unterm.un.org/DGAACS/unterm.nsf/WebView/E996B25EA7D3B36E85256B090056D806?OpenDocument,(Erişim: 14.02.2014).

Cyber Warfare An Analysıs of The Means And Motıvatıons of Selected Natıon States, http://www.ists.dartmouth.edu/docs/cyberwarfare.pdf, (Erişim: 14.02.2014).

Cyberterrorism, http://en.wikipedia.org/wiki/Cyberterrorism,(Erişim tarihi: 12.02.2014).

Department of Defense Dictionary of Military and Associated Terms, http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf, (Erişim tarihi: 21.01.2014).

Dünya Stuxnet tehdidine karşı mücadele veriyor, http://www.hurriyet.com.tr/planet/15876929.asp, (Erişim tarihi: 08.04.2014).

Dünya'nın en büyük siber casusluk operasyonu!, http://www.aksam.com.tr/ekonomi/teknoloji/dunyanin-en-buyuk-siber-casusluk-operasyonu/haber-284207, (Erişim tarihi: 15.04.2014).

Educating Your Customers on ID Theft, Phishing and eCrime, http://www.antiphishing.org/resources/Educate-Your-Customers/,(Erişim tarihi: 09.04.2014).

Google, Elindeki Müthiş Veri Tabanı Sayesinde Hakkımızdaki Herşeyi Biliyor!, http://yorumcahaber.com/haber_detay.asp?haberID=5167, (Erişim tarihi: 15.03.2014).

Hacker Gets Hold of Top Secret U.S. Space Codes, http://membrane.com/security/secure/Top_Secrets.html, (Erişim tarihi: 15.04.2014).

How Phising Works,http://computer.howstuffworks.com/phishing.htm, (Erişim tarihi: 12.03.2014).

How the F-35 Nearly Doubled In Price, http://nation.time.com/2012/07/09/f-35-nearly-doubles-in-cost-but-you-dont-know-thanks-to-its-rubber-baseline/,(Erişim Tarihi: 12.03.2014).

İki milyonluk vurgun yapan hacker yakalandı, http://www.sabah.com.tr/Yasam/2013/03/04/2-milyonluk-vurgun-yapan-hacker-yakalandi, (Erişim tarihi: 12.02.2014).

İnsan İstihbaratı ve Robin Sage Deneyi, http://www.siyahgribeyaz.com/2010/08/insan-istihbarat-ve-robin-sage-deneyi.html, (Erişim: 14.03.2014).

Internet censorship in the People's Republic of China, http://en.wikipedia.org/wiki/Internet_censorship_in_the_People%27s_Republic_of_China, (Erişim tarihi: 13.04.2014).

IP spoofing, http://www.cclub.metu.edu.tr/nenedir/Ip+spoofing,(Erişim tarihi: 09.04.2014).

Keyloggers: The Overlooked Threat to Computer Security, http://www.keylogger.org/articles/kishore-subramanyam/keyloggers-the-overlooked-threat-to-computer-security-7.html, (Erişim tarihi: 09.04.2014).

Kötü Virüs, http://tr.wikipedia.org/wiki/K%C3%B6t%C3%BC_vir%C3%BCs,(Erişim tarihi: 03.04.2014).

KULOĞLU Armağan, "Türkiye'ye Müteveccih Tehditler ve Güvenlik Anlayışı", http://www.beykent.edu.tr/WebProjects/Uploads/T%FCrkiyeye%20m%FCteveccih%20tehditler%20v %20g%FCvenlik%20anlay%FD%FE%FD.pdf, (Erişim tarihi: 11.01.2014).

Küresel Denizaltı Kablo Ağı http://people.hofstra.edu/geotrans/eng/ch2en/conc2en/global_submarine_cable_network.html(Erişim tarihi: 11.05.2014).

Millî İstihbarat Teşkilatı Resmî İnternet Sayfası, "İstihbarat Oluşumu", http://www.mit.gov.tr/isth-olusum.html (Erişim tarihi: 03.01.2014).
Operation Aurora, http://en.wikipedia.org/wiki/Operation_Aurora,(Erişim tarihi: 15.04.2014).

ÖZALP Yavuz, Siber İstihbarat ve Güvenlik Politikaları, http://bilgikultur.org/wp-content/uploads/S%C4%B0BER-%C4%B0ST%C4%B0HBARAT-ve-G%C3%9CVENL%C4%B0K-POL%C4%B0T%C4%B0KALARI.pdf,(Erişimtarihi: 21.01.2014).

ÖZCAN Mehmet, Siber Terörizm ve Ulusal Güvenliğe Tehdit Oluşturma Boyutu, http://bookre.org/reader?file=1183626&pg=2,(Erişim: 17.02.2014).

PKK'nın en önemli 'hacker'ı yakalandı, http://www.hurriyet.com.tr/gundem/10393202.asp, (Erişim: 14.02.2014).

Spam nedir?, http://spam.nedir.com/,(Erişim tarihi: 09.04.2014).

Statistics, http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx, (Erişim: 14.02.2014).

Siber Saldırılara Karşı Savunma Aracı Geliştirildi, http://www.tubitak.gov.tr/tr/haber/siber-saldirilara-karsi-yerli-savunma-araci-gelistirildi,(Erişim tarihi: 08.04.2014).

Social media, http://en.wikipedia.org/wiki/Social_media, (Erişim Tarihi: 12.03.2014).

Solucan virüs fena vurdu, http://arsiv.ntvmsnbc.com/news/198871.asp, (Erişim tarihi: 09.04.2014).

Sosyal Mühendislik Nedir?, http://www.cyber-warrior.org/dokuman/Default.Asp?Data_id=4442, (Erişim: 14.03.2014).

Türkiye'deki Kamu Kurumlarında Sosyal Mühendislik Uygulamaları, http://www.bilgiguvenligi.gov.tr/sosyal-muhendislik/turkiyedeki-kamu-kurumlarinda-sosyal-muhendislik-uygulamalari.html,(Erişim: 14.03.2014).

Türkiye'yi sahte fatura fırtınası vurdu, http://www.dha.com.tr/turkiyeyi-sahte-fatura-firtinasi-vurdu_555315.html, (Erişim tarihi: 08.04.2014).

The National Strategy to Secure Cyberspace, https://www.us-cert.gov/sites/default/files/ publications/cyberspace_strategy.pdf, (Erişim tarihi: 21.01.2014).

Türk Dil Kurumu Resmi İnternet sitesi, http://www.tdk.gov.tr/.

USAF Intelligence Targeting Guide Airforce Pamphlet, www.fas.org.pdf, (Erişim tarihi: 10.01.2014).

Virüs, solucan ve Truva atı nedir?, http://www.bilgiportal.com/zemin/yazi/1358/virus-solucan-ve-truva-ati-nedir, (Erişim tarihi: 05.04.2014).

WARNER Michael **,** Wanted: A Definition of "Intelligence" *Understanding Our Craft,* https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi studies/studies/vol46no3/article02.html, (Erişim tarihi: 29.01.2014).

YAYLA Mehmet, Hukuki Bir Terim Olarak "Siber Savaş", http://tbbdergisi.barobirlik.org.tr/m2013-104-1247, (Erişim: 14.02.2014).

61398: Çin'in siber birliği en büyük 'casusluk grubu', http://www.bbc.co.uk/turkce/haberler/2013/02/130219_china_cyber_espionage.shtml,(Erişim tarihi: 11.04.2014).

DİĞER

Harp Akademileri Yayınları, Milli Güvenlik Siyaseti ve Stratejisi, Harp Akademileri Basımevi, İstanbul, 1996.

Department of Defense Strategy for Operatıng in Cyberspace, Department of Defense, USA, 2011

ÖZ GEÇMİŞ

Cuma ÖZÇOBAN, 1982 yılında Gaziantep'te doğmuştur. İlk ve orta öğrenimini İstanbul'da tamamlamış, 2004 yılında Kara Harp Okulu'ndan mezun olmuştur. 2004–2012 yılları arasında Türk Silahlı Kuvvetlerinin çeşitli birliklerinde ve karargâhlarında görev yapmıştır. 2012–2014 yılları arasında, Harp Akademileri Stratejik Araştırmalar Enstitüsü Uluslararası İlişkiler Ana Bilim Dalında, İstihbarat Yüksek Lisans Eğitimini tamamlamıştır. Cuma ÖZÇOBAN, bekâr olup İngilizce bilmektedir.