KARADENİZ TEKNİK ÜNİVERSİTESİ * SOSYAL BİLİMLER ENSTİTÜSÜ

ULUSLARARASI İLİŞKİLER ANABİLİM DALI

ULUSLARARASI İLİŞKİLER PROGRAMI

ULUSLARARASI İLİŞKİLER TEMELİNDE SİBER GÜVENLİK: MİKRO SİBER İTTİFAK TEORİSİ (Micro-CAT)

DOKTORA TEZİ

Vahit GÜNTAY

EKİM-2016

TRABZON

KARADENİZ TEKNİK ÜNİVERSİTESİ * SOSYAL BİLİMLER ENSTİTÜSÜ

ULUSLARARASI İLİŞKİLER ANABİLİM DALI

ULUSLARARASI İLİŞKİLER PROGRAMI

ULUSLARARASI İLİŞKİLER TEMELİNDE SİBER GÜVENLİK: MİKRO SİBER İTTİFAK TEORİSİ (Micro-CAT)

DOKTORA TEZİ

Vahit GÜNTAY

Tez Danışmanı: Prof. Dr. Hayati AKTAŞ

EKİM-2016

TRABZON

ONAY

Vahit GÜNTAY tarafından hazırlanan "Uluslararası İlişkiler Temelinde Siber Güvenlik: Mikro Siber İttifak Teorisi (Micro-CAT)" adlı bu çalışma 11/11/2016 tarihinde yapılan savunma sınavı sonucunda oybirliği ile başarılı bulunarak jürimiz tarafından Uluslararası İlişkiler Anabilim dalında **doktora tezi** olarak kabul edilmiştir.

……

Prof. Dr. Hayati AKTAŞ (Başkan)

……

Prof. Dr. Coşkun TOPAL

……

Prof. Dr. Abdulkadir TOPAL

……

Prof. Dr. Fırat PURTAŞ

……

Doç. Dr. Yalçın SARIKAYA

Yukarıdaki imzaların, adı geçen öğretim üyelerine ait olduklarını onaylarım. ... / ... / …

Prof. Dr. Yusuf SÜRMEN

Enstitü Müdürü

BİLDİRİM

Tez içindeki bütün bilgilerin etik davranış ve akademik kurallar çerçevesinde elde edilerek sunulduğunu, ayrıca tez yazım kurallarına uygun olarak hazırlanan bu çalışmada orjinal olmayan her türlü kaynağa eksiksiz atıf yapıldığını, aksinin ortaya çıkması durumunda her tür yasal sonucu kabul ettiğimi beyan ediyorum.

Vahit GÜNTAY

13/10/2016

ÖNSÖZ

Bu çalışmada değişen dünyanın algısal olarak da geliştiği uluslararası ilişkiler disiplini içerisinde, siber güvenliğin unsurlarına değinilerek yeni bir yaklaşım sergilenmeye çalışılmıştır. Özellikle bu alanda gelişim seviyesini tam kapasiteye çıkaramamış Türkiye gibi ülkeler için alternatif bir politika çerçevesi oluşturulmuştur. Çalışmanın temelini oluşturan araştırma yöntemi açıklayıcı bir şekilde kurgulanmış, doktora tezinin ruhuna ve amacına sadık kalınarak bir yaklaşım denemesiyle öneriler sunulmuştur.

Araştırmanın hazırlanması ve sonuçlandırılması sürecinde beni yönlendiren ve her konuda bana yardımcı olan danışman hocam Prof. Dr. Hayati AKTAŞ başta olmak üzere; Prof. Dr. Coşkun TOPAL, Prof. Dr. Gökhan KOÇER, Doç. Dr. Süleyman ERKAN'a ve tez izleme jüriliği boyunca yardımlarından dolayı Prof. Dr. Abdulkadir TOPAL'a, tez savunma jürisinde yer alan Prof. Dr. Fırat Purtaş ve Doç. Dr. Yalçın Sarıkaya'ya, kattıkları ve tavsiyeleriyle Y.Doç.Dr. Bülent ŞENER'e teşekkür ederim. Eğitim hayatım boyunca bana kattıkları ve destekleriyle annem Ayşe GÜNTAY'a ve babam Ömer GÜNTAY'a, örnek aldığım abim Vedat GÜNTAY'a ve aileme içten sevgi, saygı ve teşekkürlerimi sunarım.

Trabzon, 2016 Vahit GÜNTAY

İÇİNDEKİLER

İKİNCİ BÖLÜM

ÜÇÜNCÜ BÖLÜM

ÖZET

Uluslararası ilişkilerin doğasındaki güç mücadelesi ve çatışma olgusu sahip olduğu niteliksel özelliklerle birlikte değişimini sürdürmektedir. Bu değişimin en önemli noktalarından birisi de güç konseptinin bu alanda farklılaştığı ve uluslararası politikalara etki ettiği siber güvenlik ve siber caydırıcılık alanıdır. Uluslararası güvenlik ile ilgili tarihsel yaklaşımlar ve gelişim siber güvenliğin; caydırıcılık, savaş, asimetri gibi kavramlarla birlikte uluslararası politikada yer edinebilirliğini karşımıza çıkarmıştır. Devletler arasındaki dönemsel çatışmaların farklı boyutlarda, siber saldırılar ve ittifaklar dahilinde ele alındığını varsayarsak uluslararası aktörler açısından çıkarın maksimize edilmesi hususu literatürün yönlendirdiği perspektif açısından önemli bir mantıksal çerçeveyi ele almamızı sağlamaktadır.

Siber mücadele anlamında devletler arasındaki ilişkileri bu yönde hareketlendirecek çok farklı veriler bulunmaktadır. Uluslararası ilişkiler boyutunda ve sahip olduğu interdisipliner alanın dışında, tartışma boyutunun oluşturulduğu ekonomik veriler uluslararası politikada farklı analizlerle desteklenmektedir. Bu konuda bölgesel özelliklere göre birtakım siber politikaların ortaya konulması ve teorik yaklaşımlar, uygulama alanı açısından bir ihtiyacı ortaya çıkarmaktadır. Daha önce uluslararası ittifaklar ve çıkar gruplarının birliktelikleri anlamında ele alınan verilerle, ortaya atılan teorik çerçeve kıyaslanarak; çalışmanın araştırma sorusunun ele alınışını daha da sağlam bir zemine oturtma amacı güdülmüştür. Uluslararası alanda önemli aktörlerden olan devletlerin birbirleri ile olan çıkarsal bölünmüşlüğü, siber sorunlar arasında nasıl bir yaklaşımla olumlu bir zemine oturtulabilir sorusu çalışma içerisinde önemli bir arayışı oluşturmuştur. Uluslararası güvenlik içerisindeki kargaşa ve zıtlık, siber güvenlik çalışmaları ve mantığı çerçevesinde, başta Türkiye olmak üzere benzer kapasiteli ülkelerde bir teori dahilinde nasıl tartışılabileceği hususundaki görüş, çalışma dahilinde inşa edilecek bir konseptin temelini oluşturmaktadır.

Anahtar Kelimeler: Uluslararası İlişkiler, Uluslararası Güvenlik, Siber Güvenlik, Siber Politikalar, Siber Caydırıcılık

ABSTRACT

Inherent of international relations, power struggle and conflict fact maintain its alteration with its qualitative characteristics. One of the most important point of this alteration is cyber security and cyber deterrence area, which have some effects to international politics and differentiated from power concept at this area. Historical approaches and progress about international security have indicated that cyber security has some arguments at international politics with the concepts like deterrence, war and asymmetry. If we assumed that periodical conflicts are dealt with cyber attacks and alliances at interstates, maximizing the interest of international actors could provide an important logical framework with regard to perspective of literature.

There are many different data for activating the relations of interstates in the meaning of cyber struggle. With the dimension of international relations and apart from its interdisciplinary area, economical data of argument dimension have been assisted with different analysis at international politics. In this subject, some of the cyber politics and theoretical approaches with regard to regional characteristics reveal a necessity in terms of application area. With comparing theoretical framework and data which have been dealt with coupling international alliances and interest groups, it is purposed for strengthening the research question of study. States as an important actor of international area and their interest dividedness have been focused with special approach for clarifying the problem of cyber conflicts. An idea about the arguments of cyber security studies and with the concept of theory in similar states like Turkey, constitutes the base of approach in this study.

Keywords: International Relations, International Security, Cyber Security, Cyber Politics, Cyber Deterrence

TABLOLAR LİSTESİ

TABLOLAR LİSTESİ (Devamı)

ŞEKİLLER LİSTESİ

ŞEKİLLER LİSTESİ (Devamı)

GRAFİKLER LİSTESİ

GRAFİKLER LİSTESİ (Devamı)

KISALTMALAR LİSTESİ

3G : Third Generation
AB : Avrupa Birliği
ABD : Amerika Birleşik Devletleri
AGİT : Avrupa Güvenlik ve İşbirliği Teşkilatı
AGSP : Avrupa Güvenlik ve Savunma Politikası
AMAN : Military Intelligence Directorate
ANSSI : Agence Nationale de la Sécurité des Systèmes d'information
APEC : Asia-Pacific Economic Cooperation
APT : Advanced Persistent Threat
AR-GE : Araştırma ve Geliştirme
ARPA : Advanced Research Projects Agency
ARPAnet : Advanced Research Projects Agency Network
ASEAN : Association of Southeast Asian Nations
BİLGEM : Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi
BLACKSEAFOR: The Black Sea Naval Force
BM : Birleşmiş Milletler
BOME : Bilgisayar Olaylarına Müdahele Ekibi
BSG : Bilgi Sistemleri Güvenliği
BT : Bilgi Teknolojisi/Teknolojileri
BTE : Bilişim Teknolojileri Enstitüsü
BTK : Bilgi Teknolojileri ve İletişim Kurumu
CIA : Central Intelligence Agency
CCC : The Chaos Computer Club
CCDCOE : Cooperative Cyber Defence Centre of Excellence
CD-DSC : Cyber Defense-Defense Support Coordination
CDMA : Cyber Defence Management Authority
CERT : The Computer Emergency Response Team
CERT/CC : The Coordination Center of The Computer Emergency Response Team
CERT-EU : The Computer Emergency Response Team of The European Union

CNCI : The Comprehensive National Cybersecurity Initiative
COMECON : The Council for Mutual Economic Assistance
COMPUSEC : Computer Security
COMSEC : Communications Security
CSOC : Cyber Security Operations Centre
DARPA : The Defense Advanced Research Projects Agency
DDoS : Distributed Denial of Service
DGSE : Directorate-General for External Security
DGSI : Directorate-General for Internal Security
DHS : Department of Homeland Security
DNC : Democratic National Committee
DoD : Department of Defense
DOJ : Department of Justice
ECOWAS : Economic Community of West Africa States
EGM : Emniyet Genel Müdürlüğü
ELINT : Electronic Intelligence
EMC : Egan Marino Company
EMC : Electromagnetic Compatibility
EMI : Electromagnetic Interference
ENISA : European Network and Information Security Agency
EUROPOL : The European Police Office
FAGCI : Federal Agency of Government Communications and Information
FBI : Federal Bureau of Investigation
FSB : Federal'naya sluzhba bezopasnosti Rossiyskoy Federatsii
G8 : The Group of Eight
GB : Gigabyte
GCC : Gulf Cooperation Council
GCHQ : Government Communications Headquarters
HSPD : Homeland Security Presidential Directive
IA : Information Assurance
IBM : International Business Machines
IC3 : Internet Core Competency Certification
IC3 : Internet Crime Complaint Center

ICIJ : International Consortium of Investigative Journalists
ICIRC : Intelligence Community-Incident Response Center
IEC : International Electrotechnical Commission
İLTAREN : İleri Teknoloji Araştırma Enstitüsü
INTERPOL : International Criminal Police Organization
IP : Internet Protocol
IRC : Internet Relay Chat
ISO : International Organization for Standardization
IT : Information Technology
KEİ : Karadeniz Ekonomik İşbirliği
KGB : Komitet Gosudarstvennoy Bezopasnosti
MGK : Milli Güvenlik Kurulu
Micro-CAT : Micro Cyber Alliance Theory
MİT : Milli İstihbarat Teşkilatı
MOSSAD : The Institute for Intelligence and Special Operations
NASA : The National Aeronautics and Space Administration
NATO : North Atlantic Treaty Organization
NATO IA : NATO Information Assurance
NC3A : NATO Consultation, Command and Control Agency
NCIRC : NATO Computer Incident Response Capability
NCIRC TC : NATO Computer Incident Response Capability Technical Centre
NCSS : The National Cyber Security Strategy
NIATC : NATO Information Assurance Technical Centre
NIS : Network Information Service
NSA : National Security Agency
NTOC : NSA Threat Operations Center
NWC3 : National White Collar Crime Center
OAS : Organization of American States
OAU : Organisation of African Unity
OCSIA : The Office of Cyber Security and Information Assurance
OECD : The Organisation for Economic Co-operaiton and Development
OHAL : Olağanüstü Hal

OPANAL : Organismo para la Proscripción de las Armas Nucleares en la América Latina y el Caribe
OSCE : Organization for Security and Co-operation in Europe
RHA : Red Hackers Alliance
RSA : Rivest Shamir Adleman
SBU : Sluzhba Bezpeky Ukrayiny
SAARC : South Asian Association for Regional Cooperation
SCADA : Supervisory Control and Data Acquisition
SGE : Siber Güvenlik Enstitüsü
SIGINT : Signals Intelligence
SOME : Siber Olaylara Müdahele Ekibi
SORM : System for Operative Investigative Activities
SSCB : Sovyet Sosyalist Cumhuriyetler Birliği
SSL : Secure Sockets Layer
TB : Terabyte
TBAE : Temel Bilimler Araştırma Enstitüsü
TCP : The Transmission Control Protocol
TEMPEST : Transient Electromagnetic Pulse Emanation Surveillance Technology
TİB : Telekominikasyon İletişim Başkanlığı
TOR : The Onion Router
TSK : Türk Silahlı Kuvvetleri
TÜBİTAK : Türkiye Bilimsel ve Teknolojik Araştırma Kurumu
UDHB : Ulaştırma, Denizcilik ve Haberleşme Bakanlığı
UEKAE : Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü
UGK : Ulusal Güvenlik Stratejisi
UK : United Kingdom
US : United States
USOM : Ulusal Siber Olaylara Müdahale Merkezi
USCYBERCOM: United States Cyber Command
YTE : Yazılım Teknolojisi Araştırma Enstitüsü
www : World Wide Web

GİRİŞ

Teknolojik olarak ve yapısal anlamda toplumsal hareketlenmeler, çoğu zaman askeri teknolojilerin tür ve seviyesine göre farklılık göstermektedir. Teknolojik olarak bu düzeyi sadece askeri sistem veya düzlem temelinde düşünmemek gerekmektedir. Bu düzlemin tartışıldığı boyut güvenlik anlamında farklılaşmayı ve tartışma alanını daha da ciddi bir kapsama oturtmuştur.

Siber alan ve uluslararası ilişkiler boyutunda *"siber politikalar"* adı altında çalışma aritmetiği bulan siber güvenlik, devletlerin kendilerini korumak için ve siber saldırılar ile birlikte yeni bir çalışma alanını karşımıza çıkarmıştır. Ulus devletlerin veya bu düzeyde tartışma niteliği gösteren güncel çalışmalar da siber güvenlik konseptine ve özüne atıflarda bulunmaktadır. *Askeri işlerde ve gelişmelerde devrim* olarak adlandırılan bu durum elektronik, ileri teknolojik savaş unsurlarının ortaya çıkmasıyla çok boyutlu bir paradoks haline dönüşmüştür.

Siber savaş gibi bir olgunun askeri teknolojiler açısından önemli olduğu, konvansiyonel ve nükleer silahlar ile bunların caydırıcılığı gibi unsurlar bakımından artık ortak bir hiyerarşide yer alması ayrı bir başlığı oluşturmaktadır. Bu başlığın şekillenmesinde uluslararası ilişkiler temeli açısından kritik altyapıların, iletişim sistemlerinin ya da özelde hava savunma sistemleri gibi birçok unsurun tehlikede olması ve caydırıcı bir özellik kazanması siber güvenliği önemli bir analiz düzeyine taşımaktadır.

Siber savaş belli yönleri itibariyle asimetrik çatışmalara benzetilmektedir ve bunu güçlendiren en önemli gösterge, zayıf durumda olanın da kimi manevralarla güçlü veya baskın olanı alt edebileceği ile ilgilidir. Uluslararası ilişkiler boyutundaki tartışma alanı ve konunun ele alındığı boyut bu yönde yoğunlaşmaktadır. Uluslararası aktörler adına makro savaş teorileri açısından kimi zaman tarafların ihtiyacı olan basit bir bilgisayar ve yazılım olabilmektedir. Bu derece basite indirgediğimiz bir durumla ilgili de doğal olarak ilk eleştiri siber savaşta kullanılan silahların, iyi birer silah olmadığı ile ilgili durumdur ve düşmana

ciddi, yıkıcı zararlar vermediği için kışkırtma açısından bir riski içinde barındırabileceğidir. Çalışmanın konseptini bu nedenle teknik kapasite açısından, özellikle siber alanda gelişmekte ya da gelişme arzusu içinde olan devletler temelinde bir yaklaşım denemesi oluşturmaktadır.

Siber savaşların ve saldırı niteliklerinin nereden geldiği ile ilgili tespitler yapılabilmekte, sorumlular kimi zaman kolaylıkla ortaya çıkarılabilmekte ve bu durum uluslararası düzeydeki saldırgan yapıyı daha da körükleyebilmektedir. Bu ve benzeri türden siber güvenlik ile ilgili yaklaşımlarda, uluslararası politika açısından diplomasi masaları tesis edilebilir ve bunların uygulamadaki başarılarına göre çalışmalar oluşturulabilir. Bu çerçevede devlet merkezli olaya yaklaşılması ve siber güvenlik gibi alanın tek pencereden incelenmesi çoğu zaman teorik olarak beraberinde belirli sorunsalları getirse de çalışmanın temelinde bu sorunsalı kırma isteği yer almaktadır.

Siber tehditler uluslararası sistem açısından, bilgi teknolojilerinin farklılaşması ile birlikte siber uzay ortamında farklı bir savaş konsepti olarak konvansiyonel anlamdaki savaşlardan ve hatta nükleer anlamdaki caydırıcılıktan daha önemli bir basamağı oluşturma yolunda hızla yol almaktadır. Soğuk Savaş ve sonrasında güvenlik algılamalarındaki farklılık, tehdit parametrelerinin değişimiyle bu konunun gelişimini hızlandırmıştır. Devletlerin siber uzayda bir aktör haline gelmesi, farklı aktörlerle ilişkilendirildiğinde günümüz gelişmeleri açısından artık bir gerçekliktir ve uluslararası ilişkiler temelinde daha çok gündeme gelmektedir.

Bu boyutlar açısından ele alındığında, siber savaşın günümüzde çağdaş devletler açısından bir tehdit oluşturduğu, ciddi bir problem sahası ve tartışma alanı haline geldiği bir gerçektir. Eksik olan ise, uluslararası ilişkilere ilgi duyanlar açısından konunun hangi teorik yaklaşımlarla ele alınacağıdır. Görünen güçlerin, görünmeyen saldırısı haline gelen siber saldırılar, devletlerin ulusal güvenlikleri açısından ciddi bir risktir ve konunun analizi açısından önemli bir tartışma noktasını oluşturmuştur. Bu doğrultuda devletlerin siber alandaki tehditlerle mücadele edebilmek amacıyla siber savunma yöntemlerini geliştirdikleri, siber tehditlere karşı önleyici bir yaklaşımla siber taarruz tekniklerini araştırdıkları ve bu alanda politikalar geliştirdikleri bilinmektedir. Bu çalışmanın açıklığa

kavuşturmak istediği diğer bir nokta da bu politikaların oluşumunda hangi birimlerin yer aldığı ve kurumsal anlamda ne tür adımlar atıldığı ile ilgilidir.

Güvenik ve teknolojik gelişmeler arasındaki bağ, uluslararası ilişkiler özelinde hegemon yapılar açısından dış politika çıktıları oluşturabilirken, Türkiye ve yakın coğrafyasındaki benzer ülkeler açısından bu üretkenlikten bahsetmek oldukça zordur. Her ne kadar siber alanın baskın aktörleri haline gelen birçok ülkeyle kıyaslanması zor olsa da, Türkiye gibi ülkelerin de alanda politik manevralar yapabilmesi adına bir yaklaşım sergilemek ve bu yaklaşımı tartışmak, çalışmanın hedeflerinden birisi olmuştur.

Siber savaş kavramının geldiği boyutta bu kavramın savaş olarak nasıl ele alınacağı, eğer savaşsa devamında barışın nasıl bir anlayışla ortaya çıkacağı veya çıkabileceği gibi yaklaşımlar felsefi olarak güvenlik çalışmaları açısından önemli bir parametreyi oluştururken çalışmanın da temel yaklaşımı haline gelmiştir. Siber alana ilişkin felsefi ve sosyolojik bir yaklaşım sergilemek ve entegre olabilmek bu alanda gelişen ülkeler adına tartışılması gereken temel unsurlar arasındadır. Kimi toplumsal haraketlerin de yönlendirilebildiği siber alanda devletlerin politikalar geliştirmesi ve bu alanda çıktılar üretebilmesi çalışma kapsamında tartışılan bir parametre olmuştur.

Bu çalışma kapsamında sorgulanmak istenen temel; artık kara, deniz, hava ve uzay ortamından beşinci savaş ortamı olarak görülmeye başlanan siber uzayda yapılan savaşların niteliği ve gelişimidir. Bu doğrultuda ortaya konulmak istenen, analiz düzeyi açısından özgün bir yaklaşım denemesiyle bu hususun desteklenmesidir. NATO gibi bir örgütün son gelişmelerle birlikte kara, hava ve deniz kuvvetleri önceliğine siber uzayı da eklemesi, bu teorilerin amatör de olsa Türkiye gibi ülkeler açısından tartışılması ve politikalar üretilmesi gerektiğini gözler önüne sermektedir. Çalışma içerisinde ulaşılmak istenen sonuç da bunun üzerine kurgulanmıştır. Bu çalışma kapsamında uluslararası politikada, güvenlik yaklaşımlarına yeni bir bakış açısı ve farklı bir boyut getirilmesi amaçlanmıştır.

Çalışmanın araştırma soruları; *"Siber alanda gelişmekte olan ülkeler için uluslararası politika alanında farklı yaklaşımlar oluşturulabilir mi?"* ve *"Uluslararası güvenlik perspektifinde, siber alanda gelişmekte olan ülkeler siber ittifaklar kurabilir mi ve çıkar elde edebilir mi?"* şeklinde belirlenmiştir. Oluşturulan hipotez; *"Siber alanda gelişen*

veya gelişmekte olan ülkeler, coğrafi yakınlık ve tarihsel bütünlük açısından mikro anlamda siber ittifaklar oluşturabilir ve çıkarsal bütünlük sağlayabilir." şeklinde kurgulanmıştır.

Çalışma temelinde kullanılan veriler; *NATO, TÜBİTAK, Kaspersky, McAfee, Panda Security, Ponemon Institute, The Statistics Portal, Internet Core Competency Certification, Hackmageddon; Information Security Timeline and Statistics, CB Insigths* ve *Trend Micro* gibi kurum, kuruluş ve platformlar üzerinden derlenmiştir. Siber güvenliğin uluslararası ilişkiler çalışma alanına yaklaştığı veriler çalışmanın 1. ve 2. bölümlerinde siber alanın en genel hatlarına ilişkin olarak sunulmaya çalışılırken, 3. bölümde başta devletler olmak üzere alanın gelişmelerine ilişkin bir yaklaşım sergileme adına derlenmiştir.

Üç bölümden oluşan çalışmada, siber güvenlik ve siber uzaya ilişkin kapsam uluslararası ilişkiler temelinde incelenmiş olup, siber politikalara ilişkin bir teorik düzlem oluşturulmaya çalışılmıştır. Bu kapsamda uluslararası gelişmelerin ve siber güvenlik içerisindeki argümanların kapsamı en basit ve temel düzeyde ele alınmaya çalışılarak konuya ilişkin sosyal bilimler alanında anlaşılabilir bir çalışma oluşturulması amaçlanmıştır. Böylece oluşturulan başlıklar dahilinde hem teknik bilgiyi literatüre kazandırmayı amaçlayan bir metodoloji kullanılmış, hem de öze ilişkin özgün bir bakış açısı sunulmaya çalışılmıştır.

Bir yaklaşım denemesi olarak tartışılan *"Mikro Siber İttifak Teorisi"*, siber alanda gelişmekte olan devletlerin tartışıldığı boyut üzerine bir alternatif sunmaya çalışmıştır. Çalışmanın ele alındığı tüm unsurlar, yaklaşımın uygulanışı ve atılacak adımlarla anlam kazanabilicektir ve denenebilecektir. Farklı kurum ve kuruluşlara ait dönemsel veriler bunu doğrular niteliktedir. Uluslararası alanda ortaya konulan verilerin belirli ülkeleri kapsaması siber alanın yaygınlığı ile ilişkilendirilmiştir. Siber alana bağlılığın tüm ülkeler düzeyinde farklı olması, uluslararası ilişkiler adına bölgesel olarak kesin bir sonuca varılmasını zorlaştırmaktadır.

Birinci bölüm dahilinde, siber güvenliğin sosyal bilimler ve uluslararası ilişkiler özelinde anlaşılmasını kolaylaştıracak kavramsal bir giriş ortaya konulmuştur. Siber politikalar dediğimiz unsurun uluslararası ilişkiler içerisinde yer edinmesi ve güvenlik çalışmaları açısından önemi, savaş ve terörizm kavramlarıyla ele alınmaya çalışılmıştır.

Siber savaş alanına ilişkin unsurlar ortaya konulmuş ve konunun anlaşılması açısından sosyal bilimlerde siber güvenlik kavramının geldiği nokta ele alınmıştır. Uluslararası ilişkiler perspektifinde önemli bir yere sahip olan uluslararası hukuk açısından siber güvenlik ve barındırdığı sorunsal bu bölüm içerisinde açıklığa kavuşturulmak istenen diğer bir husus olmuştur. Özellikle uluslararası hukuk yönünde kesin bir bütünlüğün oluşmadığı siber alanda, literatüre ilişkin temel yaklaşımlar ve kavramlar tartışılmıştır. Başta ABD olmak üzere Batı temelli çalışmalarda, siber güvenliğin kavramsal boyutuna ilişkin ciddi düzeyde çalışmaların varlığı bölüm dahilinde ortaya konulmuştur.

İkinci bölüm kapsamında özellikle siber güvenliğe dair parametrik gelişmeler ve unsurlar hem olaylar hem de tarihi süreç dahilinde ortaya konulmaya çalışılmıştır. I. Dünya Savaşı sonrasında askeri teknoloji altyapılarının geliştirilmesi yönündeki farkındalık, II. Dünya Savaşı sonrasında ciddi bir dinamiğe dönüşmüştür ve gelişmeler, bölüm dahilinde temel nitelikleriyle sunulmuştur. Konunun incelendiği ve tartışıldığı devletlere ilişkin veriler ele alınabilecek en geniş yelpazede sunulmuş ve devletlerin sahip olduğu kapasitelere dair belli başlı unsurlar açıklanmıştır. Bu noktada kurumsal niteliklerine değinilmiş, nasıl bir örgütlenme biçimiyle hareket ettikleri detaylandırılarak ortaya konulmuştur. Gerek siber savunma disiplininde, gerekse siber saldırı noktasında devletlerin kurumsal altyapıları incelenmiştir.

Son olarak üçüncü bölümde çalışmanın özüne ilişkin uluslararası ilişkiler temelinde bir yaklaşım sergilenmiştir. Uluslararası ortamın getirmiş olduğu yenilik ve değişikliğe ilişkin kavramlar kullanılarak özgün bir yaklaşım ortaya konulmaya çalışılmıştır. Bu doğrultuda özellikle uluslararası sistemin temel parametreleri ele alınmış ve siber güvenlik kavramıyla ilişkilendirilmiş, özgün bir yaklaşım ve duruş sergilenmesi yönünde *"Mikro Siber İttifak Teorisi"* adında bir perspektif sunulmaya çalışılmıştır. Bu perspektif uluslararası ilişkiler yaklaşımı açısından *"İnşacı"* teoriye yakınlaştırılmıştır.

BİRİNCİ BÖLÜM

1. ULUSLARARASI İLİŞKİLER PERSPEKTİFİNDE SİBER GÜVENLİK, KAVRAMSAL ÇERÇEVE

"Objektif anlamda güvenlik, kazanılmış değerlere yönelik tehditlerin varlığını ölçer; subjektif anlamda güvenlik ise bu değerlere saldırılacağına dair korkunun olmamasıdır."

Arnold Wolfers

Devlet ve güvenlik hakkında kuram geliştirmenin çok eski zamanlara kadar uzandığı bir gerçektir. Devletlerarası ilişkilerde yoğrulduğu boyut ve güvenliğe ilişkin temel sorgulamalar I. Dünya Savaşı'ndan az bir süre öncesine gitmektedir. Bu doğrultuda ele alınacak kavram ve çerçeve başlı başına bir araştırma konusu ve inceleme alanıdır. Süreç itibariyle ve tanımsal olarak ele alınmaya çalışılacak husus ise daha çok siber güvenliğe yakınlaştırılacak ve çalışma kapsamında alt başlıklar dahilinde vurgulanacaktır. Uluslararası ilişkiler perspektifinde ele alınacak güvenlik kavramı, siber güvenlik denildiğinde farklı aktörlerin baskınlığı da ele alınırsa strateji kavramından bağımsız da düşünülmemelidir.[1]

1.1. Uluslararası İlişkiler ve Güvenlik[2]

Devletler, 1648 Vestfalya Anlaşması'ndan bu yana uluslararası sistemin açık farkla en güçlü aktörleri olarak kabul edilse de gözle görülür bir değişim güvenlik algısı ve onun

---

[1] Sun Tzu'nun her dil ve dönemde askeri konularda klasik bir eser olan *"Harp Sanatı"* adlı yapıtından bu yana yaklaşık olarak geçen 2500 yıllık süreçte strateji ve gelişimine ilişkin farklı tanım ve yorumların yapıldığı görülmektedir. Güvenlik ve strateji kavramlarının temel niteliğine ilişkin kullanım; Vegetius'un *"Romalıların Askeri Kurumları"*, Marshal de Saxe'nin *"Harp Sanatı Üzerine Düşüncelerim"*, Clausewitz'in *"Harp Üzerine"*, Liddel Hart'ın *"Strateji: Dolaylı Tutum"* adlı yapıtında, Büyük Frederick'in generallerine direktifler'i, Napolyon'un askeri vecizeleri ve Francis Fukuyama, Samuel Huntington, Paul Kennedy, Zbigniew Brezezinski gibi birçok düşünür ve stratejistin yorumlarında günümüz gelişmelerine ışık tutar nitelikte güce vurgu yapmaktadır.

[2] Çalımanın bu başlığı kapsamında güvenlik çalışmalarına ilişkin tarihi perspektif ve teorik alan ayrıntılı irdelenmeyecektir. Bunun en önemli sebebi siber güvenliğe ilişkin verilerin ve çalışmaların daha çok politik düzlemde *"siber politikalar"* olarak ele alınması ve uluslararası ilişkiler içerisinde yer edinmeye başlamasıdır.

aktörleri için yadsınamaz. Devletlerarası ilişkileri düzenleyen bir üst otoritenin olmadığı bir ortamda, devletler siyasi meşruiyetin evrensel standardını oluşturmaktadır. Bu durum, güvenliğin, devlet hükümetlerinin temel sorumluluğu olduğu anlamına gelmektedir. Devletler diğer taraftan kendi kendine yeterliliğe dayanan bir dünyada, kendilerini korumak dışında alternatifleri olmadığı düşüncesindedirler (Baylis, 2008: 71).

Bu alternatifsizliğin de getirmiş olduğu birikimle birlikte güvenlik alanındaki ilk çalışmalar ABD'de II. Dünya Savaşı sonrasında başlamış ve başlangıçta dar bir kapsam içererek, uluslararası gerilimin daha çok askeri yönlerine odaklanmıştır.[3] Güvenlik çalışmaları bu kapsamda günümüzdeki siber güvenlik çalışmalarıyla buluştuğu noktada, 1970'lerin ortasında For Vakfı'nın güvenlik sorunlarına ilişkin çeşitli akademik merkezleri destekleme kararı almasıyla başlamıştır ve özellikle temel bilimsel bir forum haline gelen *"International Security"* dergisinin kurulmasıyla günümüz çalışmaları şekillenmiştir (Çetinkaya, 2012: 242).[4] Güvenlik alanındaki çalışmaların karar alıcıları ne yönde, nasıl etkilediği konusu, günümüzde siber güvenlik konusundaki gelişmelerle paralellik göstermemiştir (Walt, 2004: 4).

Bu türden çalışmaların uluslararası güvenlik perspektifine yapmış olduğu katkı önemli gözükmektedir. Uluslararası ilişkiler ve güvenlik ile ilgili temel varsayım; 1990'lara gelindiğinde, Soğuk Savaş'ın bitimiyle birlikte özellikle büyük güçlerin sorunlarının azalacağı gibi bir yanılgıyı ortaya çıkarmıştır.

11 Eylül olayları, hiç beklenmedik bir şekilde yeni tehditleri beraberinde getirmiştir. Zengin ve güçlü ülkelerin de her an tetikte olmaları gerektiğini göstermiştir. Bazı devletler için ise Soğuk Savaş'ın çift-kutuplu sistemi sona erdikten sonra güvenlik sorunları daha da işin içinden çıkılmaz bir hal almıştır. Devletler adına zincirler daha da kopmuş ve devletlerin birçoğu kitle imha silahları arayışına girmiştir. Siber kapasiteye dayandırılan unsurlar için ise maddi arayışlar kendini hissettirmeye başlamıştır.

---

[3] Güvenlik çalışmaları özellikle uluslararası ilişkiler açısından da, kuvvet kullanımına zemin hazırlayan koşulları belirlemeye çalışmaktadır. Ayrıca bu çalışmalar kuvvet kullanımının; bireyleri, devletleri, toplumları ve devletlerin savaşla hazırlanmak, savaşı engellemek ve savaş girmek için uyguladıkları belirli politikaları ne şekilde etkilediğini belirlemektedir. (Bkz. Çetinkaya, 2012)

[4] Özellikle siber güvenlik alanına ilişkin yazınsal ve kavramsal temel de bu derginin öncülüğünde gerçekleşmiştir.

1.1.1. Güvenlik Kavramı ve Algısı

Uluslararası ilişkilerde güvenlik kavramı, uluslararası ilişkiler anlatısının dayandığı sacayaklarından birisidir. Disiplinin dayandığı düşünce geleneklerinin her birinde güvenlik perspektifi teorik kurgunun temelindedir. Güvenlik kavramının boyutu ve önemi kimi yazarlarca daha da önemsenerek uluslararası ilişkiler disiplininin önüne dahi geçirilmiştir (Çiçekçi, 2012: 6).

Güvenlik kavramı, farklı sözlüklerdeki ortak anlamıyla en genel biçimde tehditlerden, korkulardan ve tehlikelerden uzak olma anlamına gelmektedir. Karabulut (2015: 7) bir kimsenin ya da birimin güvende olmasını, Benjamin Miller'ın *"The Concept of Secuirty: Should it be Redefined"* adlı makalesine dayandırarak iki koşula bağlamaktadır. Bunlar; eldeki değerlere yönelik bir tehdidin olmaması ve eğer böyle bir tehdit varsa tehdide maruz kalanın rasyonel bir maliyetle bu tehdidi savuşturma kapasitesine sahip olmasıdır.

Baldwin (2004: 1) kapsayıcı bir çalışma olan *"Güvenlik Kavramı"* adlı çalışmasında kavramın yeniden tanımlanmasının disiplin içi bir endüstri haline geldiğini belirtmektedir. Bu gibi çabaların büyük bölümü, güvenlik kavramının kendisi ile ilgili olmaktan çok, ulus devletlerin politika gündemlerinin yeniden tanımlanması ile igilidir. Soğuk Savaş'ın sona erişine kadar güvenliği yeniden tanımlama girişimlerinin fazlalığı göz önüne alınarak güvenliğin ihmal edilen bir kavram olarak ele alınması gerektiği sorgulanabilir.[5]

Güvenlik kavramı temel olarak sorgulandığında ise savaşlar hala ulusal güvenlik konusunda en büyük tehlike durumundadır. Nükleer, kimyasal ve biyolojik kitle imha silahlarının yaygın olduğu, ihtilafların ve sınırların, etnik ve dini güçlerin, kaynakların, mültecilerin, insan haklarının ve ticaretin ötesinde sorunların yoğunlaştığı uluslararası sistemde, güvenlik her devletin programında üst sıralarda yer almaktadır. Bu doğrultuda birçok devlet güvenliğini tehdit edecek ihtilafları sonuçlandırmak için uluslararası organizasyonlar kurmakta ve çatışmaların sebebi derinde ve ciddiyse uluslararası

[5] Baldwin'in güvenlik sorunsalını belirlemede kullandığı; *Kimin için güvenlik?, Hangi değerler için güvenlik?, Ne kadar güvenlik?, Hangi tehditlere karşı güvenlik?, Hangi araçlar yoluyla güvenlik?, Güvenliğin maliyeti nedir?, Hangi zaman periyodunda güvenlik?* gibi sorular temel olarak cevaplanabilirliğinde sübjektif unsurlar barındırmaktadır.

yapılanmaların faydası olmamaktadır (Roskin ve Berry, 2014: 277). Tartışmaların bir kısmını da bu çerçevede, uluslararası yapılanmalarla oluşabilecek güvenlik anlayışı ya da kolektif güvenlik diye ifade edilen güvenlik yaklaşımı oluşturmaktadır. Fakat bu konuda oluşabilecek güvenlik perspektifine ilişkin oluşturulmuş uluslararası bir ortak akıl bulunmamaktadır (McSweeney, 1999: 5).

Devletlerin üst sıralarında yer alan güvenlik kavramı bu açıdan bakıldığında, uluslararası ilişkiler çalışmaları açısından ise birçok yazar tarafından tartışmalı bulunmaktadır. Eğer devletler uluslararası örgütlenmeler ve girişimler sonucunda amaçlarına ulaşamayacaksa güvenlik üzerindeki samimiyet ve algı nasıl düzeltilebilecektir?

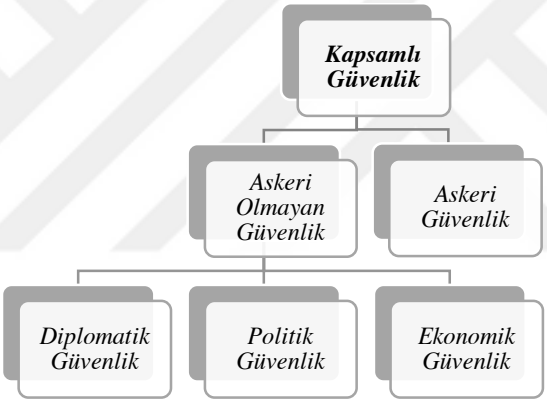
Uluslararası alanda uzmanların birçoğu güvenliğin temel değerlere yönelik tehditlerden özgür olunması anlamına geldiği konusunda uzlaşsalar da analizlerin temel odağının *"bireysel"*, *"ulusal"* ya da *"uluslararası"* güvenlik mi olması gerektiği hususunda farklılaşmaktadırlar. Büyük ölçüde askeri açıdan tanımlanan ulusal güvenlik tarihsel olarak literatüre hakim olmuştur. Temel ilgi alanı ise devletlerin kendilerine yönelik tehditlerle mücadele etmek için geliştirmeleri gereken askeri imkan ve kabiliyetler üzerine eğilimleridir (Baylis, 2008: 73).[6]

Temel olarak bu kabiliyetlerin güvenlik algısındaki boyutu, nükleer silahların, haberleşme ve ulaşım teknolojilerinin, özellikle savaşlar üzerindeki etkisi üzerine gelişmiştir. Bu duruma askeri işlerde devrim adı verilmiştir. Savaşlar giderek elektronik unsurlarla donatılmış, cephe kavramı değişmiş, insansız hava araçları, hassas güdümlü mühimmatlar, küresel konum belirleme sistemleri, haberleşme ağları ve bilgisayarlar belirleyici hale gelmiştir. Güvenlik kavramının algısal değişimi de bu gibi unsurların baskınlığının artmasıyla farklı çalışma alanlarını ortaya çıkarmıştır. Bu farklı çalışma alanlarının uluslararası ilişkiler içerisinde bölünmüşlüğü teorik alanı zenginleştirse de yine alana ilişkin objektif unsurlar birbirinden uzaklaşmaya başlamıştır.

[6] Son zamanlarda, bu güvenlik anlayışı eleştirilmiş ve birçok uluslararası ilişkiler uzmanı, ulusal güvenlik anlayışını diğer meseleleri de içerecek şekilde genişleterek, genişletilmiş bir güvenlik kavramı önerisinde bulunmuştur. Barry Buzan, siyasi, ekonomik, sosyal ve çevresel, askeri boyutları analizine dahil etmiş ve güvenliği daha geniş bir uluslararası çerçevede tanımlamıştır. Bu, devletlerin sadece kendilerini referans alarak geliştirdikleri güvenlik politikalarını terk etmelerini ve komşularının güvenlik çıkarlarını da dikkate almalarını içermektedir. (Bkz. Baylis, 2008)

Güvenlik algısının değiştiği ya da kimi araştırmacılara göre farklı algılandığı artık bir gerçektir. Temel olarak silahların ve harp unsurlarının değişimi ile cephe kavramının tanımının zorlaştığı günümüzde modern siyaset kuramları da bu algının unsurları üzerinde durmaktadır.[7] Şekil 1'de Sun Tzu'nun yaklaşımındanda esinlenen Geeraertz ve Jing güvenliği askeri olmayan ve askeri güvenlik olarak iki şekilde alt gruplara ayırmıştır. Benzer yaklaşımdaki sınıflandırmalarda uluslararası ilişkilerin doğasına ilişkin yapılan askeri kavramsallaştırmaya dair iyi bir örnek olan bu türden tipolojilerde devletlerin var oluş temeliyle ilgili bir fikir ortaya konulmaktadır. Tartışılabilirliği açık olan bu tür sınıflandırmalarda siber güvenlik kavramının ne şekilde ve nerede yer alabileceği hususu düşündürücüdür.

Şekil 1: *"Kapsamlı Güvenlik"* Anlayışıyla Sınıflandırma



Kaynak: Geeraerts ve Jing, 1999

Güvenlik algısındaki böyle bir değişimin temelinde Soğuk Savaş'ın sona ermesi, büyük bir dönüşüm olarak yorumlanmıştır. Bu dönüşümünde nasıl ve hangi yönde olduğuna ilişkin, bunun yanında hangi yönde ilerlediğine ilişkin sayısız imge ve kuram üretilmiştir.[8] Bu imgelerin başdöndürücü bir şekilde algısal değişimi ABD'de İkiz Kuleler ve Pentagon'a

[7] Modern siyaset kuramlarının başlangıç noktası olarak genelde *"mutlakiyetçi Hobbes"* ve *"liberal Locke"* üzerinden örneklenen duruşların çatışması anlaşılmaktadır ve güvenlik algısına ilişkin temel parametreler günümüze kadar farklı temalarla ele alınıp incelenmektedir. *"Güvenliğimiz için yeterince büyük güç"* gereklidir savı halen birçok düşünür tarafından savunulmaktadır. Egemenliğin doğasına ilişkin yaklaşımlar ve gücün algısı güvenliğin anlaşılabilirliği üzerine sorunlar çıkarmaktadır.

[8] Soğuk Savaş'ın hemen sonrasında, kapitalizm ve demokrasinin nihai zaferi ile birlikte dünyanın barışçı bir döneme girdiğini iddia eden Francis Fukuyama (1992: 418), savaş ve çatışmanın dönüşümüne dair dönemin en popüler imgesini üretmiş ve tarihin sonunun geldiğini ilan etmiştir.

çarpan uçaklardan sonra yaşanmıştır (Paker, 2012: 17). Devletler arasında süren mücadeleler illegal yapılanmalara sıçramış ve uluslararası aktörler arasındaki güvenlik algısı artık bir algısızlığa dönüşmüştür.

1.1.2. Farklı Yaklaşımlarda Güvenlik

Güvenlik kavramı ve barındırdığı bütünlük, insanın gelişimiyle birlikte var olduğu her noktada kullanılan bir kavramdır. Aynı zamanda varlığını koruma ve sürdürme amacı taşıyan her davranış biçiminde karşılaşılan bir olgudur. Bireye ilişkin bu durum tüm toplumsal, ulusal ve uluslararası kurumlara da yayılmıştır. Bunun temelinde tehdit olgusu ve insan doğasındaki kimi çatışmacı unsurlar etkili olmuştur.

Uluslararası ilişkiler içinde güvenlik anlayışına göre ise aktörler büyüklük ve amaçlarına göre fakrlı güvenlik perspektifi sergilemektedirler. Dedeoğlu (2003: 12) uluslararası ilişkilerde güvenlik kavramının esas olarak birkaç düzlemde ifade bulacağını belirterek şu sınıflandırmayı yapmıştır:

- *Uluslararası sistemin bütünü ya da bütüne yakınının güvenliği,*[9]
- *Coğrafi ya da işlevsel alt-sistemlerin, bölgelerin güvenliği,*
- *Devletin güvenliği,*
- *Toplumun güvenliği,*
- *Toplumsal alt-grupların güvenliği,*
- *Bireylerin güvenliği*.

Yaklaşımsal olarak farklı unsurlarla ele alınan güvenlik kavramı içerisinde siber güvenlik olgusunun araştırılması önceliği bizleri yakın tarihe yaklaştırsa da antik dönemlerden gelen güvenlik parametreleri belli bir birikimle de evrimini sürdürmektedir. Din kavramının; devrimler, sınıf çatışmaları gibi unsurlarla yoğrulduğu ve teknolojik

[9] Uluslararası sistemin anlaşılabilirliği ve genel olarak sistem içerisinde tüm aktörlerin mutabık oldukları genel kurallardan bahsetmek oldukça güç gözükmektedir. Uluslararası sistemin bütünlüğü ya da bu bütünlükten anlaşılması gereken genelin kabullendiği bir güvenlik anlayışıyla ilişkilidir. Bu anlayışın temellendirilmesinde temel aktör devlettir. Realizmden itibaren devletin uluslararası ilişkiler içerisinde merkezde yer alması bu bütünlüğün anlaşılabilirliğini de oldukça zorlaştırmaktadır.

gelişmelerle dünyanın algılanmasına ilişkin değişimin güvenlik parametrelerinde hissedildiği uluslararası ortam başlı başına büyük bir tartışma ve araştırma alanıdır.

20. yüzyıl başlarındaki gelişmeler güvenliğe ilişkin yaklaşımsal tutumu özellikle uluslararası ilişkiler adına daha özel bir noktaya taşımış ve günümüz çalışmaları açısından temel mimariyi oluşturmuştur. Uluslararası ilişkilerin temel modern düşünürlerinin 20. yüzyıl başlarındaki gelişmelerle yoğurduğu uluslararası sistem *Machiavelli, Hugo Grotius, Thomas Hobbes, Hegel, Kjellen, Ratzel, Haushofer, Marx* gibi birçok düşünürün fikirleriyle temel eleştiri noktaları bulmuştur.

Bu birikim dahilinde, yaklaşımsal olarak güvenlik uzun bir süre realizmin egemenliğinde gelişmiştir. Bu gelişim iki kutuplu yapının Sovyetler Birliği'nin dağılması sonrasında ortadan kalkmasıyla ortaya çıkan devlet-altı ve ötesi gelişmelerle birlikte yeni bir görünüme de kavuşmuştur (Çiçekçi, 2012: 30). Küreselleşen dünyanın getirmiş olduğu farklı parametreler realizm temelindeki yaklaşımı ve tartışmaları kendi içerisinde eritmiştir. Ekonomik unsurlar ve savaş stratejileri gücün farklı şekillerde farklı tanımlarla ele alınmasını zorunlu kılmıştır.

Colin Elman (2007: 15) *"yükselen ve düşen" realizm* tanımlamasıyla gelişen ve değişen bu durumu güzel bir şekilde analiz etmiştir. Uluslararası sistemin dinamikleri kendi içerisinde gücün döngüsünü ekonomik beklentiler ve çıkarlar ile bireyleri ve kurumları dahi kimi zaman en üst noktaya taşırken kimi zaman kendi içinde çıkarlar doğrultusunda bertaraf etmektedir. Bu durumu Gilpin'in 1981 yılındaki eseri, *"War and Change in World Politics"* ile de ilişkilendiren Elman uluslararası ilişkilerin özünde aslında hiç değişmediğini, kabuk değiştirdiğini vurgulayarak günümüz siber güvenlik çalışmalarının özüne ilişkin de bir çeşit atıfta bulunmuştur.

İki kutuplu uluslararası sistemin yumuşamaya başladığı dönemde etkili olan bir diğer yaklaşım olan neorealist yaklaşım değişen koşullara ilişkin durumu etkileyici bir şekilde ifade etmektedir. Devletlerin uluslararası sistemde dış politika toplamı olarak ele alınmadığı gerçeğini, kendi güvenliklerinden sorumlu olan devlet anlayışıyla çok yönlü olarak hissettirmiştir. Sistemin kuralının, bunu kurabilecek büyüklüğe sahip aktör tarafından

belirleneceği anlayışa göre aktör çatışmacı ise sistem kaotik, uyuşmacı ise barışçı olacaktır (Dedeoğlu, 2013: 45).

Güvenliğe ilişkin önemli diğer bir yaklaşım kaynaklarından olan liberalizm felsefi ve farklı bir bakış açısıyla çok yönlülüğü arttırarak, insan doğasını dikkate alarak onu değiştirmeye çalışmak yerine pozitif yönde yönlendirmeyi tercih etmektedir (Birdişli, 2016: 39).[10] Liberalizm güvenlik yaklaşımları açısından, kendi içerisinde farklılıklar barındırır ve siber güvenlik çalışmaları yönünde teorik bir zeminde yorumlanması oldukça zorlaşmaktadır.

Teorik olarak uluslararası sistem açısından güvenlik yaklaşımlarında benzer bir zorluk ve karmaşıklığı yaşayan diğer bir paradigma da marksizmdir. Uluslararası çatışmanın kendi içerisindeki dinamiklerin bir ürünü olduğunu her fırsatta vurgulayan bu yaklaşımsal gelenek, hegemonik yapının sorunsal bütünlüğünü emperyalist gelenek ve küreselleşme ile bağdaştırmaktadır (Rupert, 2007: 42). Marksist gelenekte devletin, egemen sınıfın baskınlığını devam ettirmelerinin bir aracı olarak olarak görülmesi, güç ilişkisini açıklamada ve siber güvenlik gibi alanlarda teorik bir tutum oluşturmayı zorlaştırmaktadır. Bu noktada eleştiri temelinde baskın bakış açısı güvenlik alanının geneline ilişkin, sadece ideolojik bir perspektif sunabilmektedir (Wallerstein, 2004: 130).

Konstrüktivist (İnşacı) yaklaşımın ise teorik olmanın ötesinde, özellikle liberalizm ve marksismden farklılaşarak analiz yöntemi olarak uluslararası sisteme ilişkin çok boyutlu ya da multidisipliner bir bakış açısı getirmesi, özellike yeni güvenlik algısı açısından kayda değer bir temeli oluşturmaktadır. Materyalizm ve idealizmin sentezinden oluşarak çok yönlü bir yaklaşımın güvenliğe katkısı bu yaklaşım içinde önemli bir yere sahiptir (Birdişli, 2016: 84).

Tablo 1'de farklı yaklaşımların ana aktörlerle birlikte değişkenler, davranış, seviye ve metot bakımından sınıflandırılması yapılmıştır. Ana değişkenler arasında ve beklenen davranış açısından bu yaklaşımlar arasındaki zenginlik ve farklılık aslında güvenliğe ilişkin

[10] Liberalizmin kaynak çeşitliliği, düşünce dünyasında da farklı içeriklerin oluşmasına neden olmuştur. Günümüzde liberalizm; *politik liberalizm, kültürel liberalizm, ekonomik liberalizm, sosyal liberalizm, muhafazakar liberalizm ve neoliberalizm* başlıkları altında incelenmektedir.

her bir yaklaşımın kendine özgü duruşunu ortaya koymaktadır. Ana değişkenler arasında liberal ve marksist yaklaşımların ekonomiye olan vurgusu ve farklılığı gözlerden kaçırılmamalıdır.

Tablo 1: Güvenlik Paradigmalarının Kıyaslanması

Düşünce Okulu	***Ana Aktörler***	***Ana Değişkenler***	***Beklenen Davranış***	***Analiz Seviyesi***	***Metot(lar)***
Realizm	*Devlet*	*Şiddet/ Askeri Güç*	*Çatışma/ Rakiple İşbirliği*	*Devletten Devlete*	*Tarihsel/ Analitik*
Neorealizm	*Devletler Sistemi*	*Siddet/ Askeri Güç*	*Çatışma/ İşbirliği Mümkün*	*Sistem*	*Tarihsel/ Analitik*
Liberal Kurumsalcı	*Diğer Aktörler ile Sınırlı Devlet*	*Şiddet/ Askeri Güç ve Ekonomik*	*İşbirliği*	*Devletten Devlete/ Ulusaşan Güç*	*Tarihsel/ Bilimsel/ Analitik/ Davranışsal*
Klasik Liberalizm	*Birey (Kişi/ Şirket)*	*Teknolojik/ Ekonomik*	*İşbirliği*	*Bireysel*	*Metodolojik*
Neomarksism	*Şirketler*	*Teknolojik/ Ekonomik*	*Çatışma*	*Sistem/ Pazarlar*	*Tarihsel/ Analitik*
İnşacı	*Sosyal İnşacı Olarak Aktör*	*Fikirler/ Değerler*	*İşbirliği/ Çatışma(?)*	*Sosyal İnşa İle Değişim*	*Sosyal ve Sosyo-Psikolojik*
Davranışsal	*Araştırma Bağımlısı*	*Araştırma Bağımlısı*	*Çatışma/ İşbirliği*	*Bütün Seviyeler*	*Modelleme ve Ölçme*

Kaynak: Buzan ve Hansen, 2009

1.1.3. Güvenlik ve Strateji

Strateji kavramını Prusyalı General *Carl von Clausewitz*, 1832'de yayınlanan *"Savaş Üzerine"* adlı çalışmasında *"savaşın amaçlarına ulaşmak için muharebenin araç olarak kullanılması teorisi"* şeklinde tanımlamıştır. Benzer şekilde İngiliz askeri tarihçisi *Hanry*

Liddell Hart da 1941'deki *"Strateji: Dolaylı Tutum"* adlı eserinde *"Strateji; politikanın amaçlarının gerçekleştirilmesi için askeri imkanların dağıtımı ve uygulanması sanatıdır."* diyerek kavramı klasik anlayışı içerisinde ele almışlardır (Açıkmeşe, 2012a: 3). Günümüz tanımlamaları ve anlayışı içerisinde kavram genellikle savaş ve politik amaçlar düzleminde ele alınışıyla bu geleneği devam ettirmektedir.[11]

Strateji, genel olarak askeri bir kavram olarak algılansa da, kavramın askeri anlamda algılanışı tümüyle doğru bir durumu ifade etmemektedir. Ulusal ve uluslararası düzlemlerde aktör sayısının artması ve karşılıklı ilişkilerin daha karmaşık bir hale gelmesiyle birlikte, strateji kavramının kullanıldığı alan yaygınlaşmıştır. Doğal olarak güvenlik kavramının tehdit kavramıyla birlikte ele alınması gibi strateji kavramı da büyük ölçüde güvenlik kavramı ile birlikte değerlendirilmektedir (Dedeoğlu, 2003: 56). Strateji ve güvenlik kavramlarının sistematik bir teori zemininde ele alınışı ile çalışmalar kullanıldığı alana göre farklılık göstermektedir (Smith ve diğerleri, 1994: 5).

Yakın zaman itibariyle de uluslararası alandaki tüm ilişkiler çatışma ya da savaş bağlamında gelişmemiştir ve farklı, karmaşık ilişkilerin biçimine ya da gelişimine göre aktörler stratejiler geliştirebilmektedir. Siber güvenlik alanında sadece çatışmacı bir yaklaşımla uluslararası ilişkiler boyutunda çalışmaların yönlendirilmesi önemli bir yanılgıyı beraberinde getirebilir. Bunun en önemli sebebi inşacı teorinin konuya yaklaşımıyla oldukça iyi özetlenebilir. Gelişim tek taraflı olarak devletler temelinde değildir. Bireysel ve toplumsal beklentiler de siber güvenlik alanındaki strateji düzeyini farklı alanlara taşıyabilir.

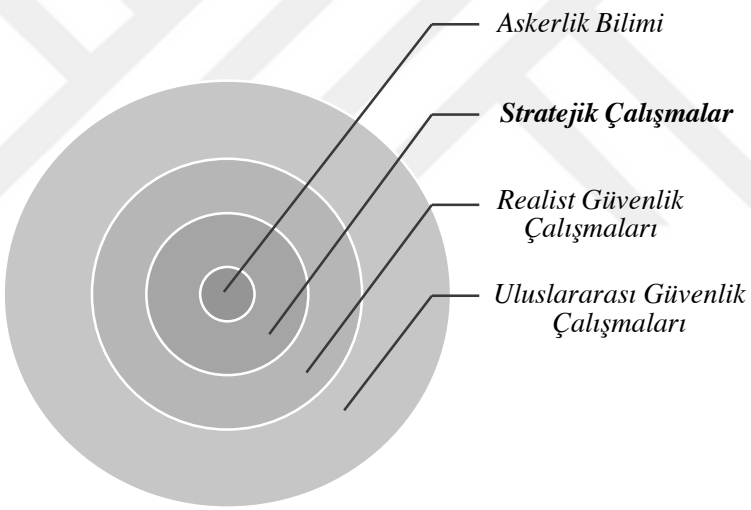
Uluslararası sistemde bir aktörün stratejisinden söz etmek, aynı zamanda o aktörün amaçlarının neler olabileceğinden ve gücünden söz etmek anlamına gelmektedir. Zengin, gelişmiş ve güç kriterlerini büyük ölçüde karşılayan bir aktörün amaçları ile bu amaçlarını karşılama ve tehditleri bertaraf etme kapasitesi, doğal olarak kendisine benzemeyenden farklı olacaktır (Dedeoğlu, 2003: 61). Bu noktada siber güvenlik stratejisi ve aktörler arasındaki farklılığa ilişin saldırı ve savunma unsurları klasik güç yaklaşımına

[11] Klasik dönem açısından Sun Tzu'nun, Thucydides'in ve Machiavelli'nin; modern dönem açısından ise Napoleon'un, Jomini'nin, Clausewitz'in ve Hart'ın strateji anlayışları ve yaklaşımları strateji düşüncesinin gelişiminde en güncel tartışmaları dahi şekillendirmektedir ve stratejik düşüncenin doğru anlaşılması açısından temel parametreleri oluşturmaktadır.

benzememektedir. Ülkelerin gelişmişlikleri ya da siber uzaya olan bağımlılığı ciddi sorunlara neden olabilmektedir (Kilroy, 2008: 443).

Güvenlik ve strateji ikilisine, güvenlik çalışmaları açısından bakacak olursak; Açıkmeşe (2012b: 35) güvenlik gündeminin askeri sorunlar ve devlet-merkezlilik ötesinde tanımlanması çabalarının ve stratejik çalışmalara alternatif anlayışın gelişimini Şekil 2'de görüldüğü gibi Betts'in iç içe geçen halkalar yaklaşımıyla açıklamıştır. Önceleri realizmle beraber anılan *"Stratejik Çalışmalar"*, 1980'lerden itibaren daha teknik nitelik taşıyan askerlik bilimine yakınlaşınca stratejik çalışmaların temsil ettiği genel alanın adı *"Realist Güvenlik Çalışmaları"*na dönüşmüştür.

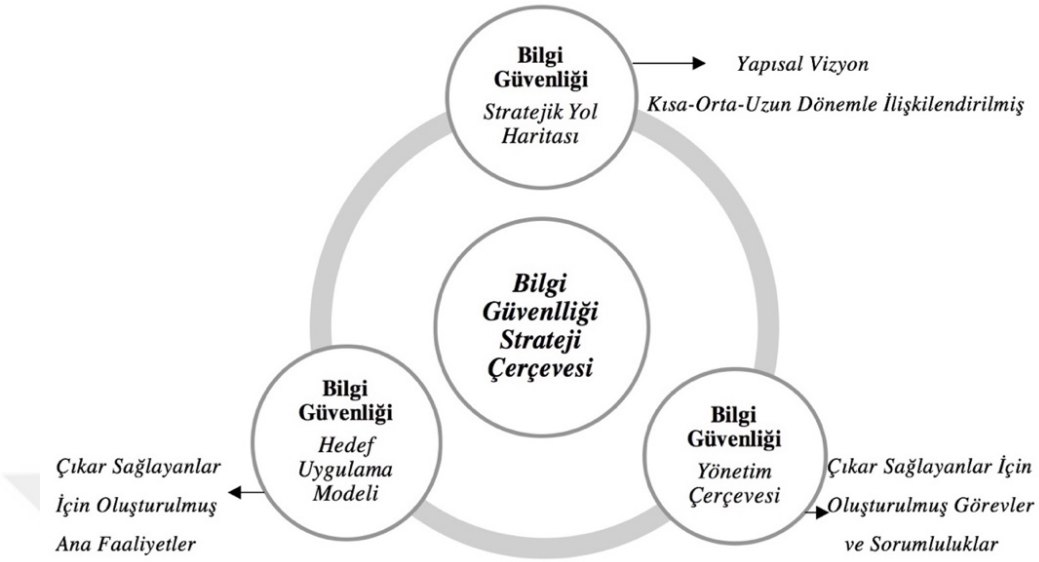
Şekil 2: Stratejik Çalışmaların Güvenlik Çalışmaları Kapsamındaki Mevcut Konumu



Kaynak: Açıkmeşe, 2012b: 35

Uluslararası güvenlik çalışmaları açısından daha önce vurgulanan strateji kavramıyla özdeşleştirebileceğimiz bilgi güvenliği ve siber güvenlik ile ilgili çalışmalarda örnek bir strateji çerçevesi Şekil 3'te görüldüğü üzere belirlenecek politikalara ilişkin şekillendirilmektedir. Daha önce stratejiye ilişkin gerek yapılan tanımlamalarda, gerekse Betts'in iç içe geçen halkalar yaklaşımındaki gücün fiziksel hali ve askeri unsurları, bilgi güvenliğine ve siber güvenliğe ilişkin yaklaşımlarda daha çok kısa-orta-uzun vadeli politikalarda kendini hissettirmektedir. Uluslararası güvenlik çalışmaları içerisinde tartışılan boyutta siber güvenlik benzer yapılanmalarda ele alınmaktadır.

Şekil 3: Örnek Bir Bilgi Güvenliği Strateji Çerçevesi



Kaynak: Corix Partners, 2016

1.1.3.1. Barışçıl Güvenlik Stratejileri

Barışçıl güvenlik stratejileri, aktörlerin çatışmaya varmayan yöntemlerle güvenliklerini ve çıkarlarını gerçekleştirme yolundaki uygulamalarını ifade etmektedir. İçinde, şiddet kullanma ve caydırıcı olma hatırlatmalarını barındırsa da, bunlar üzerine bir eylem biçimi geliştirmeyeceği algılamasına dayanmaktadır (Dedeoğlu, 2003: 112). Bu noktadaki anlayış aktörlerin kendi güvenlikleri açısından karşıdaki aktörün de zarara uğratılmayacağına dair bir yaklaşıma dayanır (Walker, 2007: 151).

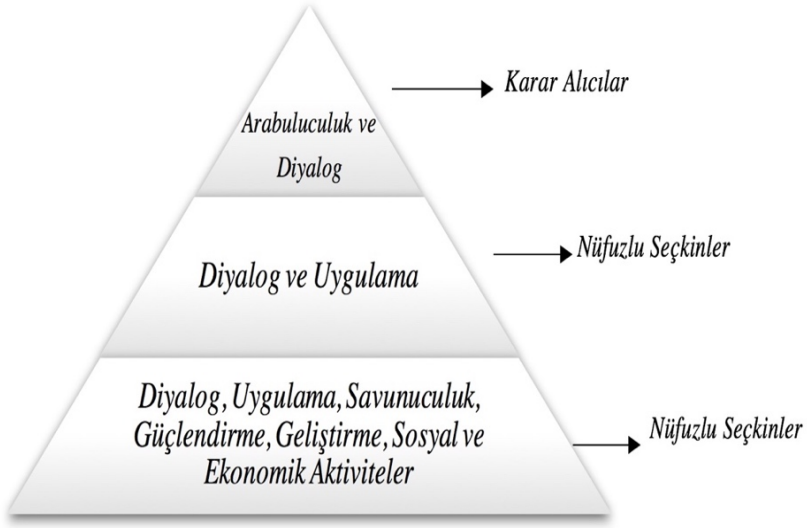
Dedeoğlu (2003) barışçıl güvenlik stratejilerinde diplomatik yöntemler ayağını müzakereler, uzlaştırıcılık ve arabuluculuk, haber alma ve karar alıcıları yönlendirme şeklinde gruplandırmıştır. Ekonomik yöntemler açısından ödüllendirme ve dış yardım şeklinde gruplandırmaya giderken; iş birliği ve ortaklık kurma anlamında ittifakları bölgesel ve evrensel nitelikte gruplandırmıştır.

Diplomatik yöntemler ayağında müzakereler, diplomasi kavramı anıldığında genelde tek araç gibi gözükse de müzakerenin temelinde "güç kavramına" sıkça atıf yapılmaktadır. Devletler diplomatik müzakerelerin çıkmaza girdiği durumlarda kuvvet kullanmaya dayalı

bir etki yönteminden yararlanmayı pek çok açıdan tercih edebilmektedirler. Bu anlayışın temelinde olay döngüsü ve tarafların birbirlerini ne kadar tanıdığı önemli bir kıstastır. Kimi zaman gizli, kimi zaman açık ve tarafların sayısına göre çeşitlenebilen müzakerelerde sürece ilişkin net veriler sunmak zorlaşmaktadır.

Müzakere ve arabuluculuk açısından tarafların belirginliği kesin ve net bir çevrede gerçekleşmeyebilir ve bu noktada üçüncü taraflar da etkili bir şekilde bu konsept içerisinde yer alabilir. Şekil 4'te görüldüğü üzere, resmi olmayan üçüncü tarafların görevleri açısından nüfuzu olan seçkinler diyalog ve uygulamada karar alıcılardan sonra devreye girebilirler. Özellikle siber güvenliğe ilişkin kimi konuların gelecek planlarının oluşturulmasında bu düzleme sıkça rastlanılmaktadır.

Şekil 4: Resmi Olmayan Üçüncü Tarafların Görevleri



Kaynak: Chigas, 2003

Müzakereler başarısız olduğunda veya bazı sebeplerden dolayı çatışmanın taraflarından birisi ya da her ikisi diğeri ile görüşmeyi reddetttiğinde, devletler çoğunlukla çatışma çözümleri çabalarına yardımcı olunması anlamında dışarıdan bir kişinin, bir grubun ya da bir örgütün arabuluculuğunu aramakta ya da kabul etmektedir. Arabuluculuğun, bir anlaşmazlığın taraflarının aralarındaki farklılıkları kabul edilebilir üçüncü bir tarafın yardımıyla çözmeye çalıştığı bir süreç olarak tanımlandığını düşünürsek konuya ilişkin farklı modellerin geliştirilmesi olağandır (Burgess ve Burgess, 1997: 211).

Haber alma ve karar alıcıların yönlendirilmesinde, sürecin yapısal çerçevesinin belirlenmesinde, karar birimi kavramı temel bir öneme sahiptir. Normal olarak bütün dış politika kararları, çeşitli faktörler nedeniyle, bazı farklılıklar gösteren belirli türden karar birimleri içerisinde oluşmaktadır (Sönmezoğlu, 2014: 315). Karar alıcıların bu birimlerin yönlendiricileri olarak etkilenmelerinde; zaaflarını, amaçlarını, yöntemlerini, eksik ve fazlalıklarını tespit etmek adına haber alma sistemlerinin varlığı önemli bir yere sahiptir (Mintz ve DeRouen, 2010: 27).

Ekonomik yöntemler bazında ise mali araçlara, güvenlikle ilgili olarak geliştirilen stratejilerde sıkça başvurulmaktadır. Dış yardım, belirli projelerin desteklenmesi, yeni ekonomik kaynakların kullanıma hazırlanması, yeni ticaret yollarının yaratılması, hibe yardımları ve teçhizat yardımları en bilinen ekonomik ödül türleri olarak literatürde yerini almıştır (Dedeoğlu, 2003: 116). Siber güvenlik çalışmaları açısından bu türden dış yardımların ekonomik boyutta siber politikalar oluşturmak yerine daha çok internet altyapılarının kurulması ya da teknolojik unsurların geliştirilmesi anlamında şekillendiğini görmekteyiz.

Çalışmanında konseptini oluşturan ittifak oluşturma ya da iş birliği-ortaklık kurma gerek yakın tarih gerekse günümüz barışçıl güvenlik stratejileri açısından en çok tercih edilenler arasındadır. Her ne kadar ittifak algısı ve kurgusu bir tehdit olarak kabul edilse de güvenlik duvarı oluşturma adına bir bütünlük konseptidir. Siber caydırıcılık oluşturma adına bu türden ittifakların uzun ömürlü olması günümüz gelişmeleri açısından oldukça zor gözükse de, devletler çıkar elde amaçlı olarak geçici ittifaklar oluşturabilirler. İşbirliği stratejileri genel olarak uluslararası sistemde tek başına çıkarların gerçekleştirme maliyetinin yüksek olduğu durumlarda tercih edilmektedir.

1.1.3.2. Çatışmacı Güvenlik Stratejileri

Çatışmacı güvenlik stratejilerinin bir kısmı, diplomatik yöntemlerde ifade bulmaktadır. Çatışmacı diplomatik yöntemlerin ilki, *tek yanlı karar* almaktır. Bunun ardından ise, *oldu bittiye getirme* yöntemi uygulanır. Her iki yöntem de, barışçıl diplomatik yöntemlerin sürdürülemeyeceğinin anlaşılması durumunda kullanılmaktdır. Diğer bir ifadeyle, taraflar arasındaki sorunların daha önce müzakere edilmiş olması söz konusudur

(Dedeoğlu, 2003: 121).[12] Teorik olarak taraflar arasında müzakere edilen konunun kapsamı ve içeriği çatışmacı güvenlik stratejilerinde daha çok tartışılmaktadır. Tarafların sahip olduğu güç ve güvenlik ikileminin oluşturduğu temalarla meydana gelen müzakereler teorik zeminde ele alınmamaktadır (Kolodziej, 2005: 118).

Çatışmacı güvenlik stratejileri içinde, barışçıl güvenlik stratejilerinde olduğu gibi *ekonomik yöntemler* vardır ve *boykot, ambargo, abluka* gibi bilinen yöntemlerle çeşitlenmektedir. Diğer bir çeşit olarak *savaşa varmayan sıcak yöntemler* ise *tahrik etme, tedhiş, sabotaj* ya da *rakip içerisinde darbe yapmak* veya *darbeyi desteklemek* gibi unsurlara dayanmaktadır. *Askeri yöntemler* ise çatışmacı güvenlik stratejileri içerisinde en şiddet barındıran yöntemdir.

Ekonomik yöntemler arasında boykot diğeri üzerinde etkide bulunmak isteyen bir ülkenin hedef ülkenin bazı veya tüm mal ve hizmetlerine pazarlarını kapatması anlamına gelmektedir.[13] Boykotun simetriği olan ambargoda ise önlemi uygulayan ülkenin karar alıcıları bazı veya tüm mal ve hizmetlerin hedef ülkeye satış veya benzeri bir yolla aktarılmasını yasaklamaktadır.[14] Abluka ise belirli bir yönde etkilenmek istenen hedef ülkenin tümünün veya belirli bir bölümünün dış ile olan bağlantısının kısmen veya tamamen denetim altına alınmasını, kesilmesini ifade etmektedir (Sönmezoğlu, 2014: 495).[15]

Savaşa varmayan sıcak yöntemler arasında tahrik etme, güvenlik olarak tehdit unsuru düşündüğü aktörü, kendisine ya da bir başka aktöre karşı hata yapmaya itebilecek davranışa zorlamaktır. Tedhiş yaratmak ise, rakibin içinde ulusal bütünlüğe ve karar alıcılara, iktidarlara, istikrara yönelik olarak, varolan muhalefetin çatışmacı eylemler yapmasını destekleme biçiminde kendisini göstermektedir. Sabotaj, kimi zaman rakip ülkeden kişiler

[12] Karşı tarafı yanlış bilgilendirerek, gizli ittifaklar oluşturarak ya da pazarlıklara konu edilmemiş unsurları devreye sokarak uygulanan bu yöntemler, genel olarak taraflar arasında sıcak çatışmaya dönüşebilecek süreçlerin göze alındığını ifade etmektedir.

[13] Örneğin; ABD, İngiltere'ye karşı yürütülen bağımsızlık mücadelesi sırasında bu ülkenin mallarını boykot etmiştir. Arap ülkeleri de uzun yıllardır İsrail mallarına karşı benzer bir tutum izlemektedir.

[14] 1979 yılı Kasım ayında Tahran'da vatandaşlarının rehin alınması üzerine ABD, İran'a karşı genel nitelik bir ambargo uygulamaya başlamış, müttefiklerinin de bu yönde davranmasını sağlamaya çalışmıştır. 1974 Kıbrıs harekatının ardından Türkiye'ye karşı silah ambargosu uygulamıştır.

[15] Ablukanın en eski ve en sık başvurulan biçimi deniz ablukasıdır. ABD, 1962 yılında Küba'ya, 1972 yılında Kuzay Vietnam'a karşı bu türden bir abluka uygulamıştır.

ile iş birliği dahilinde, siyasal karar alıcıların, önemli teçhizatın, yeraltı ve yerüstü zenginliklerinin bertaraf edilmesine yönelik uygulanan bir stratejidir.

Çatışmacı güvenlik stratejileri açısından en sert unsurları barındıran askeri yöntemlerde, aşamalı şiddet uygulanması söz konusudur. Askeri yöntemler, genel olarak diğer yöntemlerle sonuç alınamaması durumlarında, ya da diğer yöntemlerin işlerlik kazanmalarını sağlama aşamalarında kullanılmaktadır. Askeri harekatlar, savaşın bölgesel kalması ya da küresel düzleme taşınması olasılıklarına göre farklı düzlemlerde tasarlanmaktadırlar (Dedeoğlu, 2003: 125). Çalışma içinde siber güvenliğe ilişkin vurgulanan hususta siber saldırıların karşı taraf açısından konvansiyonel bir cevap gerektirebileceği ya da bu yönde askeri bir harekat karşılığı bulup bulmayacağı tartışmalı hususlar arasındadır.

1.1.4. Siber Güvenlik ve Uluslararası İlişkiler Teorileri

Uluslararası ilişkilerin doğası temel olarak uluslararası alandaki olayların ortaya çıkış şekilleri ve sebepleri üzerinde durmaktadır. Pek çok teorisyen de, egemen devletlerarasındaki ilişkiler hakkında fikirler öne sürmüşlerdir. Temel olarak amaçları, devletler arasındaki ve içindeki siyasi etkileşimin modellerini anlayabilmek olmuştur. Bu teorisyenlerden bazıları geçmiş olayları açıklama ve gelecekle ilgili öngörülerde bulunarak teorik modellemeler üretme ve bu modeller vasıtasıyla genel ilkeler çıkarma çabası içine girmiştir.

Bu modellemeler tartışılırken savaş ve barış, sınırlar ile güç ilişkileri temel paradigmalar olarak belli başlı sorular olarak uluslararası ilişkilerin doğasını yoğurmuştur. Teknolojideki hızlı değişme, devletlerarası ilişkilerde büyük gelişmelere yol açmıştır. Uluslararası alanda savaş ve siyaset biçimlerinin de değişmesine neden olmuştur (Knutsen, 2006: 346). Bu değişimle birlikte, *"Digital-age Security"* kavramının kendiliğinden tartışıldığı yeni dönemde özel bir etkinin olduğu ve yeni yaklaşımlara ihtiyaç olduğu kaçınılmaz bir gerçeklik haline dönüşmüştür (Dunn, 2007: 86).

Uluslararaı ilişkiler ve siber güvenlik ikilisi adına, 1991 sonrasında sivilleşen ve dünyanın kullanımına açılan internet, uluslararası sistemin aktörleri olan devlet, toplum ve

bireyleri birbirlerine daha etkin şekilde bağlamıştır. Bu noktada, internetin uluslararası sistemdeki olayların katalizörü olduğunu belirtmekte fayda vardır. İnternet, zihinlerdeki Soğuk Savaş tansiyonunun düşmesinde ve farklı kamplardaki insanlar arasındaki perdelerin kalkmasında önemli bir rol oynamıştır. 1991 Körfez Savaşı'nın detaylarının internet ve medya üzerinden canlı biçimde takip edilmesi yeni dönemin farklı olacağının en büyük göstergesi olmuştur (Bıçakçı, 2012: 207). Uluslararası ilişkilerin sahip olduğu doğa ile siber güvenliğin kesiştiği nokta bu düzlemde başlamıştır. Bunlar tüm dünyada iletişimin ötesine geçip verilerin transferini sağlayan ve manipülasyon gücüne sahip olan bir ağ (www) ve devletlerarası çıkarlar olarak karşımıza çıkmıştır (O'Connell, 2012: 191).

Uluslararası ilişkilerin kalbinde yer alan devletler siber uzayın aktörü haline gelmesiyle devletlerarası çıkarlar, var olan güç potansiyelini siber güvenlik alanına kaydırmış ve ayrıca bir parantez açmıştır. Devletlerin siber uzayın bir aktörü haline gelmesi, siber suçların etki alanının genişlemesine ve yarattığı tehdit potansiyelinin artmasına neden olmaktadır. Bu durum uluslararası ilişkiler içerisinde devletlerin siber güvenlik kavramını daha ciddi bir şekilde ele almaları zorunluluğunu getirmiştir. Siber güvenlik, iki büyük dünya savaşında olduğu gibi askeri ve jeopolitik üstünlüğü ön plana çıkaran taarruzlar yerine, bilgi sistemleri üzerinden yapılan, siber uzayın sunduğu sınırsız özgürlük ortamı içinde daha kolay ve kısa sürede gerçekleştirilebilen saldırıları mümkün kılmıştır (Bayraktar, 2015: 24).

Uluslararası ilişkiler temelinde siber güvenlik olgusunun askeri teknolojide son nokta olduğuna, hava kuvvetleri ve nükleer savaşlar kadar önemli olduğu da varsayılmaktadır. Günümüze dek birçok siber saldırı sadece hedefteki bilgisayar ağlarına aşırı yük bindirmiş, sistemlerinin yavaşlamalarına veya çökmelerine sebep olmuştur. Rusya, 2008'deki Gürcistan işgalini bilgisayar sistemlerini aşırı yükleyerek gerçekleştirmiştir. Uluslararası ilişkilerdeki güç baskınlığı mücadelesinde, savunma sistemlerine saldıracak daha gelişmiş yöntemler tartışılmaktadır. (Roskin ve Berry, 2014: 328). Bu gelişmeler neticesinde, klasik olarak güç algısı yerine, farklı yöntemlerle gücün kapsamını artırma ve küresel boyutta etkin olma adına farklı teorik yaklaşımların çıkış noktaları oluşturulmuştur. Uluslararası ilişkilerin aktörleri arasındaki mücadelenin de teknolojik bir devrim sonrasında teorik tartışmalarla yeni bir boyutta tartışılması kaçınılmaz hale gelmiştir.

Değişen ve gelişen dünyanın[16] ortaya çıkarmış olduğu bu türden girişimler ve yenilikler, teknolojik olarak uluslararası aktörlerin saldırı ve savaş stratejilerini de etkilemiştir. Bu durum an itibariyle o kadar gelişmiştir ki, siber saldırıların zamana ve mekana göre bir kapasitesi olmuştur. Tartışılan ve tam olarak adının koyulamadığı boyut ise, yaşanılanların tek taraflı bir saldırı olduğu mu yoksa savaş kavramıyla beraber anılan bir unsur olduğumudur. Uluslararası ilişkiler dahilinde bir zemine oturtulan siber güvenlik ve beraberinde getirdiği algısal düzey siber uzayı çatışma alanı haline dönüştürerek teorik bir zemin hazırlamıştır.

Uluslararası ilişkiler alanında, siber güvenlik ile etkileşimde teorik çalışmaların oluşturulması adına, ABD'de özel sektör bünyesindeki destek ve konuya ilişkin çalışmalar kayda değerdir. Bilgi teknolojileri ve bu alanın getirmiş olduğu yeniliklerle birlikte yoğrulan devletlerin kurumsal bazda yapmış oldukları çalışmalar ve üniversitelerin bu konudaki çalışmalara olan destekleri karar alıcılara çoğu zaman raporlar halinde sunulmaktadır. Bu türden gelişmeler, uluslararası ilişkiler teorilerinin siber güvenlik zemininde gelişimini mümkün kılmaktadır (Choucri ve diğerleri, 2013: 97). Uluslararası ilişkilerin teorik boyutunda da ABD'deki atılımın temelinde bu unsur önemli bir yere sahiptir.

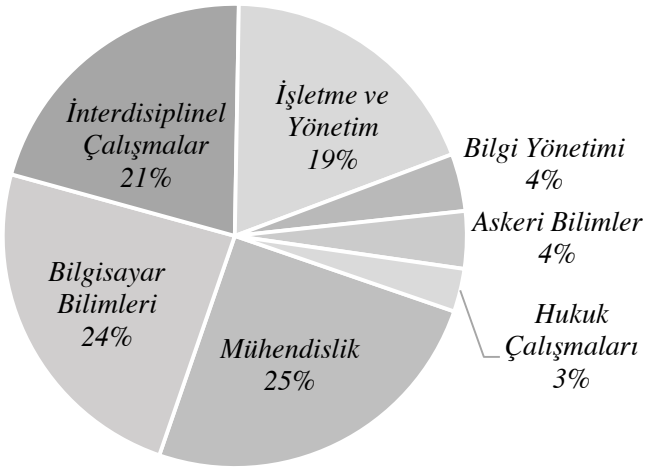
Uluslararası ilişkiler adına, uluslararası aktörlerin de etkilendiği ve çalışmanın konusunu oluşturan siber güvenlik akademik ve profesyonel düzlemde, farklı alanlarda da gelişimini sürdürmüştür. Grafik 1'de görüleceği üzere siber güvenliğin çalışılmasına ilişkin genel araştırma alanlarında, teknik başlıklarda bir baskınlık göze çarpmaktadır. Uluslararası ilişkiler boyutundaki çalışmalar interdisipliner boyutta ele alınmakta ve konunun doğru anlaşılması adına teknik boyuttan asla kopulmamaktadır. Özellikle bilişim suçlarına ilişkin artış göz önünde alındığında siber güvenliğin hukuk çalışmaları boyutundaki eksiklik dikkat çekicidir.[17]

---

[16] Vurgulanan bu kavramın algısı dünyanın farklı yerlerinde farklı şekillerde yorumlanmaktadır. Dünyanın değişimi gelişmiş ülkelerde hayatı kolaylaştıran bir algı olarak yer edinirken, gelişmekte olan ülkelerde yeni ufuklar ve umutlar olarak algılanmakta, az gelişmiş ve gelişmemiş ülkelerde ise değişimin ve teknolojinin dünyayı ipotek altına aldığı ve bu gelişimin belirli bir zümreye hitap ettiği yönündedir. Bu türden benzeri felsefi yaklaşımlar karar alıcılar açısından da geçerlidir. Dünyayı algılama misyonu ve bu konuda atılacak adımlar toplumla birlikte dünyayı anlamada bir dinamik haline dönüşmüştür.

[17] İncelen raporlarda University of Washington, US Military Academy West Point, West Chester University of Pennsylvania, University of Pittsburgh, George Mason University akademik yetkinlikleri en iyi okullar olarak değerlendirilerek çalışma düzeyinde baz alınmıştır.

Grafik 1: ABD'de Siber Güvenlik Çalışmalarının Yayıldığı Akademik Departmanlar[18]



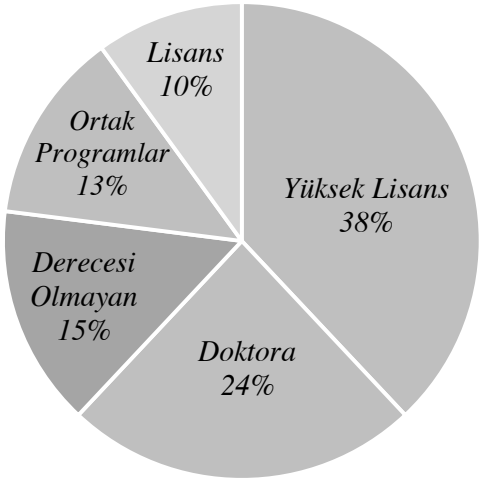
Kaynak: Ponemon Institute, 2014: 8

Grafik 2'de ise siber güvenlik çalışmalarının derecelerine göre dağılımı bu alanda uzmanlaşmanın oransal olarak oldukça ilerlediğini göstermektedir. Yüksek Lisans ve Doktora derecelerinin artış içerisinde olduğunu ve uluslararası alanda bu çalışmaların bir eğilime dönüştüğünü vurgulamakta fayda vardır. ABD gibi ülkelerde teorik alana katkı sağlayan yaklaşımlar bu uzmanlık derecelerinin artmasıyla ciddi bir atılım gerçekleştirmiştir. Siber güvenlik ve interdisipliner çalışmaların buluştuğu noktalarda sertifika ve uzmanlık programları da hızla artış göstermektedir.

AB ve NATO gibi örgütlerin de ajandalarında yer alan sertifika ve uzmanlık programları, siber güvenlik alanında sadece teknik konulara yönelmemektedir. Uluslararası ilişkiler alanında, siber alanda risk yönetimi ve karar alıcıların yönlendirilmesi anlamında yer alan uzmanlık programları dikkat çekici bir şekilde artış göstermektedir. Özellikle bölgesel düzeyde siber sorunların yer aldığı bu türden programlarda, uluslararası ilişkilerin temel disiplinel çerçevesinde yapılan çalışmalar, teorik alana da katkı sağlamaktadır (Renard, 2014: 12).

[18] Ponemon Enstitüsü tarafından yayınlanan *"Siber Güvenlik Alanında En İyi Okullar"* adlı raporda toplam 183 siber güvenlik programı incelenmiştir.

Grafik 2: ABD Siber Güvenlik Alanında Verilen Uzmanlık Derecelerinin Dağılımı[19]



Kaynak: Ponemon Institute, 2014: 9

Uluslararası ilişkiler açısından teorik çerçevede siber güvenliğin nasıl tartışıldığı veya tartışılması gerektiği hem çalışmaların dağılımı, hem de bilimsel açıdan önemli bir husustur. Teori; veri almak, soru sormak ve karmaşık bir dünyadan anlam çıkarabilmek adına elimizdeki tek nedensel araçtır. Uluslararası ilişkiler ve onun özelinde hızla tırmanışta olan siber güvenlik ve siber politika çalışmaları günümüze en yakın teorik yaklaşımlarla birlikte kendine yer bulabilmektedir. Bu teorilerin uluslararası ilişkiler içinde, siber güvenlik çerçevesinde açıklama bulanları "*Realizm", "Neorealizm"* ve çalışmanın da konseptini oluşturan "*Konstrüktivizm"*dir.

1.1.4.1. Realizm ve Siber Güvenlik

Günümüze yaklaştığı noktada eski bir teorik düzlem olarak siber güvenlik çalışmalarında yer edinebilen *realizm,* hala küçük farklılıklarla da olsa kabul görebilmektedir. Realizmin temel tartışma noktası askeri güçten daha geniş bir kavram olarak gücün ele alınışıdır. Gücün askeri unsurlarıyla birlikte vurgulanması ve varolma mücadelesi içindeki bütünlüğü siber saldırılar ve kapasiteleri açısından salt bir özellik

[19] Ponemon Enstitüsü tarafından yayınlanan *"Siber Güvenlik Alanında En İyi Okullar"* adlı raporda toplam 183 siber güvenlik programı incelenmiştir. Raporda *"Derecesi Olmayan"* olarak beliritilen programlarda sertifika alma amaçlı bir tanımlama yapılmıştır.

taşımaktadır. Bu yaklaşım haricinde siber güvenliğe ilişkin yaklaşımsal boyutu eksik kalmaktadır.[20]

Siber politikalara ilişkin mantığın realizme en büyük eleştirisi devletin tek ve bütüncül bir aktör olarak varsayılması ve devlet içi dinamiklerin göz ardı edilmesidir. Askeri konulara öncelik veren realistler açısından gözden kaçırılan nokta siber güvenliğe ilişkin verilerin ciddi parametreler üzerinden tartışıldığıdır. Uluslararası ilişkilere yönelik aksaklıklar ve anlaşmazlıkların giderilmesinde en etkili yöntem olarak güç kullanımının baz alınması siber saldırılara zıt düşmektedir (Stone, 1994: 449). Özellikle realizm temelindeki tartışmaların birçoğu siber güvenlik gelişmeleri açısından bu yönüyle zıtlaşmaktadır.

Realizm perspektifinde, iş birliği konusunda karamsar bir duruş vardır ve güvenliğin ancak güçlerin dengelenmesiyle sağlanabileceği savunulmaktadır. Bu yaklaşıma göre güçlü devletler denge kurmaya çalışmalıdır ancak hegemonik bir ülkenin kontrolü altında başarılı bir iş birliği olasılığı az gözükmektedir. Siber güvenlik açısından saldırganın bilinmediği bir dünyada ve illegal yapılanmalarla iş birliği içindeki devletler açısından bu durum, realizm temelindeki bir yaklaşımı siber güvenlik açısından zora sokmaktadır. Realistler iş birliğini engelleyen en önemli etkenin başka ülkenin kazancının, diğerinden fazla olma endişesi olarak görmektedirler (Çetinkaya, 2012: 247). Morgenthau'nun da belirttiği gibi ABD'nin patolojik sorunlarından olan *"büyük güç"* olma ve bunun sürdürülebilirliği ile ilgili adımları kazancın maksimize edilmesi anlamında uluslararası toplumun tepkisini çekmektedir ve iş birliğini kendi içerisindeki samimiyet boyutunda zora sokmaktadır (Scheuerman, 2007: 85).

Realizmin temel perspektifi içinde siber güvenik yapısına ilişkin zıt düştüğü noktalar yanında örtüştüğü noktalar da vardır. Bu eleştirel yöndedir ve siber güvenliğin özüne ilişkin bir örtüşmedir. Tablo 2 üzerinde görüleceği üzere realizmin temel olarak birincil analiz düzeyi insan gruplarıdır ve sibernetiğe ilişkin temel varsayımlar da insan odaklı ele alınmaktadır. Birincil analiz düzeyi açısından devletlerarası seviye kısmen kendi içindeki yapısal özelliklerle benzeşim göstermektedir. Siyasi düşünce yapıları içindeki rasyonalizmin

[20] Edward Hallett Carr, II. Dünya Savaşı sonrasında Amerika'da Hans Morgenthau'nun güçlendirdiği realist akımın temellerini atmıştır ve özellikle yaşanılan sürecin yıllar sonra farklı boyutlar kazanabileceği ile ilgili yaklaşımı siber güvenlik boyutuna yaklaşan tespitler arasındadır.

bireysel seviyesi ile tartışabileceğimiz siber güvenlik bu noktada eleştirel bir bakış açısı getirmektedir.

Tablo 2: Uluslararası İlişkilere Dair Üç Önemli Paradigma

Siyasal Düşünce Yapıları	***Birincil Analiz Düzeyi***	***Birincil Analiz Seviyesi***	***Açıklayıcı Unsurlar***	***(Esas) Konu veya Odak***	***İdeolojik Gelenek***
Realizm (Gerçekçilik)	*İnsan Grupları*	*Devletlerarası Seviye*	*Askeri Güç Dengesi*	*Çatışma ortamında Düzen*	*Muhafazakarlık*
Rasyonalizm (Akılcılık)	*Rasyonel Aktörler*	*Bireysel Düzey*	*Müzakere, Çıkarlar*	*Rasyonel İşbirliği*	*Liberalizm*
Revolüsyonizm (Devrimcilik)	*Kapitalist Sistem*	*Dünya Sistemleri Düzeyi*	*Yapısal Güç*	*İktisadi Gelişme*	*Radikalizm*

Kaynak: Knutsen, 2006: 342

Siyasal düşüncel yapıları açısından rasyonalizmin birincil analiz seviyesindeki bireysel düzey, siber güvenlik tanımlaması içinde teorik olarak bu alana daha yakın durmaktadır. İdeolojik gelenekler açısından realizmin, rasyonalizmin ve revolüsyonizmin siber güvenliğin felsefi boyutuyla uyuşmadığı da bir gerçekliktir. Bunun temelinde konunun dinamiklerinin yeni döneme ilişkin parametrelerle yoğrulması yer almaktadır.

1.1.4.2. Neorealizm ve Siber Güvenlik

Uluslararası ilişkiler alanında önde gelen teorilerden biri olan neorealizm, 1970'li yılların sonuna doğru ortaya çıkmıştır ve realizmin sorgulanmaya ve eleştirilmeye başlanması yeni bir teorik çerçeveyi beraberinde getirmiştir.[21] Uluslararası politikanın temel

[21] Neorealizmin en ünlü temsilcisi *Kenneth N. Waltz*'tur. Kendisi de bir realist olan Waltz, 1979'da basılan *"Theory of International Politics"* adlı çalışmasında yeni fikirler ortaya koymakta ve o güne kadar bir sonuç olarak bakılan ve anarşik bir ortam olarak görülen uluslararası yapının devletlerin davranışlarını sınırlandırdığını söylemekte, ayrıca güç kavramına yeni anlamlar yüklemektedir.

aktörünün devlet olarak görülmesi, devletlerin üniter yapılar olarak değerlendirilmesi, devletlerin ve devlet adamlarının rasyonel davrandıklarının varsayılması, devletlerin kendi çıkarları için bencilce hareket ettiklerinin kabul edilmesi gibi yaklaşımlar realizm ve neorealizmin ortak özellikleri olarak belirginleşmiştir (Çetinkaya, 2012: 248). Karar alıcıların davranış şekilleri ve uluslararası politikaların seyrine ilişkin neorealizmin getirmiş olduğu çalışmalar kendi içerisinde oldukça geniş bir tartışma alanı bulmuştur (Rosecrance ve Steiner, 2010: 346).

Tarihsel süreç uluslararası aktörlerin kendi kimliklerini kazanmasıyla müdahaleleri genelde askeri unsurlarıyla karşımıza çıkarmıştır. Fakat günümüz imkanları ve stratejileri askeri unsurların yıkıcı özelliklerini inanılmaz boyutlara taşımıştır. Bu durumu göze almak istemeyen aktörler, birbirlerini caydırmada ve etkilemede farklı saldırı ve savaş tekniklerini geliştirmeye başlamıştır.

Bu değişim aslında önemli bir teorisyen olan *Kenneth Waltz*'un 1954'te vurguladığı verileri destekler niteliktedir. *"Man, State and the War"* adlı eserinde savaşın nedenleri ve gelişimi ile ilgili görüş ayrılıklarını ortaya koymaya çalışan Waltz, filozoflar arasındaki görüş ayrılıklarının aslında belirleyici olmadığını, sadece zamanın ve uygulamanın değiştiğine dikkat çekmektedir. Aslında kendi zamanından örneklerle yola çıkan Waltz, farklı teorilerin farklı yaklaşımları beraberinde getirdiğini, eğer ortada bir çatışma varsa bunun niteliğinin değişebileceğini vurgulamaktadır. Weber (2010: 35), Waltz'un, *"Theory of International Politics"* adlı eserinin uluslararası ilişkiler geleneğinde neorealizmin teorik altyapısını oluşturduğunu özellikle belirtmektedir.

Değişen nitelikler arasında, uluslararası anlamda başgösteren güvensizlik ortamı uluslararası ilişkilerin temelini oluşturmuştur. Bu güvensizlik ortamında her devletin öncelikli amacı egemenliğini ve güvenliğini korumak olmuştur. Bu kapsamda realistler gücü, uluslararası politikanın bir amacı olarak görürlerken, neorealistler devletin varlığını sürdürmesinin ve güvenliğinin sağlanmasının bir aracı olarak değerlendirmektedir (Bayraktar, 2015: 46). Bu durumda siber saldırılara ilişkin caydırıcılık oluşturma ya da saldırı kapasitesi yaratma adına varlığın sürdürülmesi gibi amaçların günümüzde devletler adına bir ajandaya bağlanması, bu yaklaşım altında neorealizmi siber güvenlik çalışmalarında bir adım öne çıkarmaktadır.

Güvenlik paradigmaları açısından neorealizmin temel olarak ana aktör olarak devlet yerine devletler sisteminden bahsetmesi siber güvenlik açısından daha açıklayıcı olmaktadır. *Tablo 1*'de[22] görüldüğü üzere realizm ve neorealizmde benzerlik gösteren ana değişkenler şiddet-askeri güç ikilisiyle açıklanmaktadır ve siber saldırı kapasiteleri açısından da bir benzerlik göstermektedir. Yine analiz seviyesi açısından sistemsel vurgu dikkat çekicidir ve neorealizm için günümüz çalışmalarını açıklamada daha kavramsal bir özellik göstermektedir.

Siber güvenlik ve caydırıcılık açısından realizmi, neorealizmin gölgesinde bırakan unsur bu kuramın Soğuk Savaş gibi eski dönemlerde işe yarayabileceği ve günümüzde rasyonel teklifleri dikkate alınmayan ideolojik alt kimlik grupları tarafından yaratılan şiddet dolu dünyada geçerli olmadığı hususudur. Diğer bir sorunsal da Morgenthau'nun değindiği bazda güç dengesidir (Kurki, 2008: 92). Güvenlik oluşturmaya çalışırken, ülkeler *"güvenlik ikilemi"* diye bilinen güvensiz bir ortama düşmektedirler.

1.1.4.3. Konstrüktivizm (İnşacılık) ve Siber Güvenlik

Uluslararası ilişkiler teorilerinin içinde en yenilerinden olan inşacılık, dünya siyasetinde yapanların ya da aktörlerin sosyal etkileşimine odaklanan, uluslararası ilişkiler alanına özgün bir yaklaşımdır. İnşacılara göre devlet etkileşimi kimliklerin, çıkarların ve değerlerin zaman içerisinde devlet eylemini şekillendirdiği ve aynı zamanda bunların devlet eylemince şekillendirildikleri bir öğrenme sürecini yansıtmaktadır (Griffiths ve diğerleri, 2011: 123).

Kimliksel unsurlardan kasıt ve anlayış özellikle siber güvenlikte de açıklanması gereken hususların başında gelmektedir. Uluslararası ilişkilerin genç bir disiplin oluşu itibariyle ve yakın zamanda siber alanda gelişen unsurlar aynı potada erimeye başlamıştır (Jabri, 2008: 11). Teknolojik verilerin ve gelişimin bireyler ve toplumlar özelinde nasıl anlaşıldığı ve manipüle edildiği, bunun uluslararası ilişkilerde nasıl yankılandığı bu teorik yaklaşım içerisinde kendine cevap aramaya çalışmaktadır. İnşacılık açısından bir analiz düzeyinin sunulması gelişen dünyayı anlamada iyi bir düzey ortaya çıkarmaktadır.

[22] (Bkz.; Sayfa 13), **"Tablo 1. Güvenlik Paradigmalarının Kıyaslanması"**

Tablo 1'de,[23] inşacı yaklaşıma ilişkin ana değişkenlerin fikirler ve değerler olduğu, beklenen davranışın çatışma ve iş birliğinin doğasında olduğu ve kabullenişi; hem hukuksal düzlemde siber güvenliğin daha doğru anlaşılmasında, hem de gelecekte siber uzayın inşa edilmesinde önemli bir parametreyi oluşturmaktadır. Bu doğrultuda inşacılar uluslararası kurumların hem düzenleyici hem de oluşturucu işlevlerini kabul etmişlerdir ve oluşabilecek siber ittifaklar açısından bu önemli bir yaklaşımdır.

Diğer taraftan ana akım inşacılar dışarıda bir dünya olduğunun farkındadırlar fakat kişi bazında bunun bir hazırlığının olmadığı durumlarda anlamsız bir durumdan bahsetmektedirler.[24] Genellikle gerçeklerin iç yüzünü kavrayana kadar geçen süreç uluslararası sistemin işlerliği bakımından zaman kaybına neden olabilmektedir (Roskin ve Berry, 2014: 60).[25] Bu işlerliğin oluşmasında inşacılık bir analiz düzeyi sunmaktadır ve bunu uluslararası ilişkiler içerisinde doğrudan olmasa da, dolaylı olarak siber güvenliğe ilişkin yapmış olduğu atıflarla ispatlamaktadır. Siber güvenliğin uluslararası ilişkiler boyutuna yaklaştığı analiz düzeyinde çok yönlülük gerekmektedir.

Somut olarak vurgulanan noktada inşacılık ve siber güvenlik çalışmalarına ilişkin belirtilmesi gereken husus güvenlik sorunlarına tepkisel olarak gelişen silahlanma yarışıdır. Siber silahlar, fiziksel etki doğuran silahlara göre nasıl sınıflandırılacaktır sorusu literatürde yer edinmeye başlamıştır. Silahlanma yarışlarının da en azından belirli düzeyde bir rekabeti önceden var saydığı ve başladıktan sonra bu rekabeti daha da yoğunlaştırdığı yönünde bir uzlaşı mevcuttur. Bu noktada devletler siber saldırı yönlerinin geliştirilmesi ve caydırıcılık

---

[23] (Bkz.; Sayfa 13), **"Tablo 1. Güvenlik Paradigmalarının Kıyaslanması"**

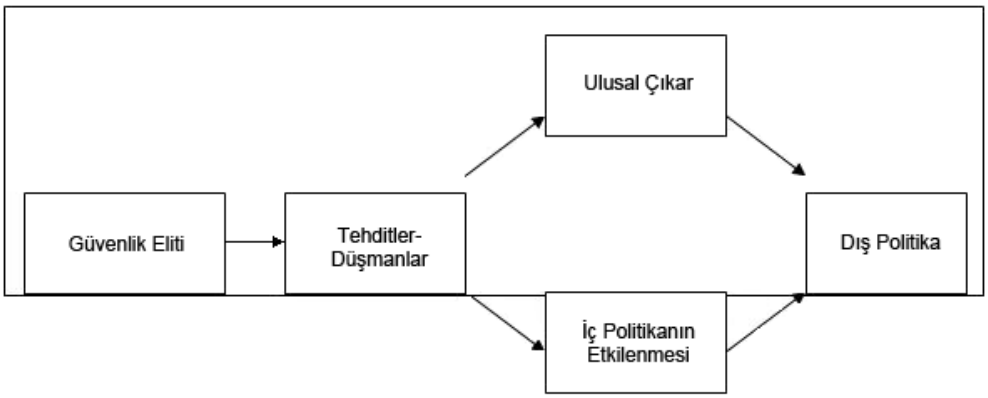
[24] Friedrich Kratochwill'in bilinen ya da varsayılan sosyal düzen üzerine inşa edilmiş yaklaşımlar hakkında yapmış olduğu eleştirel durum siber güvenlik çalışmaları açısından da bir vurgudur. Nicholas Onuf ise yıllar önce uluslararası ilişkileri sosyal bilimler içerisinde yeniden yapılandarmaya başladığımızda söylemlerin zorluğuyla ilgili tavrı gerçekten kayda değerdir. Özellikle siber güvenlik açısından kesin ve net yargılarla sosyal bilimlerin uluslararası ilişkiler alanında söylemler üretmek oldukça güçtür. Christian Reus-Smit'in söylemsel teorisi özellikle inşacılık temelinde Habermas'ın iletişimsel eylem teorisine dayanmaktadır. Kurumlar tartışma ve müzakere için etik ve ahlaki talepleri veya kural ve normların kurumsallaştırılması gerektiğine dair diğerlerini ikna edecek yeterince zorlayıcı sebep barındırmaktadır. Siber güvenlik açısından özellikle uluslararası alandaki kurallar bütününün eksikliği zorlayıcı sebepler de olmadıkça devletleri illegal girişimlere itmektedir.

[25] Bush ve neomuhafazakarlık, Amerikalılara Irak'ın kötü olduğunu böyle bir yaklaşımla sunmuştur. Irak'ın 2003'te işgali, Irak'ta kitle imha silahlarının olmadığını veya El-Kaide ile bir bağlantının olmadığını ortaya çıkarmıştır. Irak ile ilgili düşünceler bir anda değişmiştir. Irak ile ilgili düşünceler müdahele öncesi temellendirilirken siber anlamda bir mücadele de yürütülmüş ve çok yönlülük belirginleşmiştir. Siber güvenliğe ilişkin benzer belli-belirsiz veriler inşacılık içinde politikalar üretimini de olanaklı kılmaktadır.

oluşturma adına, siber uzayda etkili olabilmek için ekonomik önlemler almaktadır ve bu alanda çalışan uzmanlara ihtiyaç duymaktadır (Vazquez, 2015: 193).[26]

Finansal açıdan yük getirmeyen ve nitelikli personeli oluşturma siber güvenlik oluşumları ve yapılanmaları adına bambaşka bir süreç başlatmıştır. Şekil 5'te görüldüğü üzere tehditler siber güvenlik adına güvenlikleştirme modeli açısından iç politikanın etkilenmesinde kendisine yer edinmeye başlamıştır. İç politikanın etkilenmesi ve ulusal çıkarın farklılaştırdığı tehdit algısı siber saldırılar ve siber caydırıcılık açısından dış politikada sonuçlar doğurmaktadır. İnşacılığın, güvenlikleştirme süreciyle buluştuğu noktada; diplomasi konusunda, siber politikalar üretebilen uzmanlara duyulan ihtiyaç ve bu konudaki acil eylem planları farklı alanlarla etkileşimi zorunlu kılmaktadır.

Şekil 5. Güvenlikleştirme Süreci



Kaynak: Aras ve diğerleri, 2010: 20

İnşacılık temelinde siber güvenliği tartışırken sorunun eski ve yeni oluşuyla ilgili değil de, gerçeklik olarak ele alınan noktanın bağımsızlığı doğru anlaşılmalıdır. Gerçeklik algısı ve siber saldırılara ilişkin daha sonra da değinilecek olan siber müdahele araçları somut bir çıktıda ne tür sonuçlar doğurmaktadır? Bu konuda farklı perspektiflere ihtiyaç vardır ve uluslararası ilişkiler yaklaşımında inşacı teori, bunu kısmen başarabilmektedir. Siber uzaya ilişkin müdahele ve araçlar elbette vardır fakat bunun doğru anlaşılmasına dair teorik çerçeve

[26] Kuvvet kullanımına işaret edebilecek bir olayın gerçekleşmesi genel bir güvensizliğe; rakip bir ülkenin daha fazla askeri yetenekleri olduğunun ortaya çıkması, silahlanması veya ittifaklar kurarak gücünü artırdığı şeklinde bir algının oluşması, özel bir korkuya dönüşmektedir. (Bkz. Singer, 1979)

somut gerçekliklerle ilişkilendirilmelidir.

Diplomatik konularda ve farklı eylem planlarının oluşturulmasında siber güvenlik perspektifi açısından Kopenhag ekolü ve inşacılık bazı yönleriyle benzerlik göstermektedir. Kopenhag ekolü de, geleneksel güvenlik çalışmalarının ve onların askeri güvenliğe olan odaklanmalarının ötesinde, güvenliğe yönelik çok boyutlu bir yaklaşım benimsemiştir.[27] Bunun yanı sıra, güvenliği askeri konuların dışına genişletmek suretiyle güvenlik çalışmalarını devlet dışı aktörleri de içerecek şekilde derinleştirmiştir (Çetinsaya, 2012: 256). Siber saldırı ve güvenlik mekanizmaları açısından özellikle farklı hacker gruplarının devlet içindeki yapılanmaları ve koordineli çalışmaları bu durum için iyi bir örnek oluşturmaktadır (Gartzke, 2013: 49).

1.2. Siber Güvenlik - Siber Politikalar[28]

"Siber Güvenlik" ve bu alana ilişkin çalışmaların temeli, alan çalışmaları açısından herhangi bir başlığın tekelinde değildir. Dünya siyasetinin geleceği açısından çalışmalara konu olan siber güvenlik kavramı, *"Siber Politikalar"* kavramı ile ayrıştırılarak uluslararası ilişkiler açısından son yıllarda teorik olarak tartışılmaya başlanmıştır.

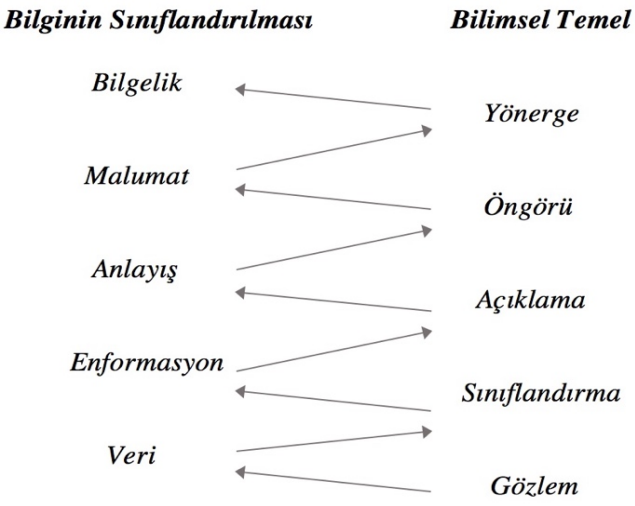
Hayes ve Alberts (1995), Şekil 6'da ortaya koydukları enformasyon ve bilim tipolojisinde, enformasyon kaynaklarıyla ilişkilendirilen temellendirmelerde sürecin ilk çıkış noktasını izlenecek yönergelere bağlarken, gözlem temelinde bu basamağı sonlandırmıştır. Siber güvenliğin temelindeki bilgi çeşitliliğinde uluslararası ilişkiler açısından, bilimsel olarak bir güvenlik anlayışı ortaya çıkacaksa politik düzlemde bu ilişkinin sınıflandırılmış olması gerekmektedir. Bu tipolojide, bilginin sınıflandırılmasındaki basamaklar ve bilimsel temel, siber güvenlik anlayışının politik düzleme dönüşünde temel alınabilir.

---

[27] *"Kopenhag Ekolü"* güvenlik çalışmalarına teorik bir taslak hazırlama konusunu öncelikli olarak ele alırken, ampirik çalışmalara yeteri kadar önem vermemektedir. Bu durum siber güvenliğin uygulama alanına ilişkin Kopenhag ekolüne bir eleştiri olarak literatürde yer edinmelidir. Siber güvenliğin uygulama alanı tek bir boyutta, uluslararası ilişkiler çalışmaları açısından ele alınamaz.

[28] *"Siber Politikalar"* kavramı özellikle uluslararası literatür açısından *"Cyber Politics"* olarak uluslararası ilişkiler temelinde çerçevesini bulmuştur ve birçok çalışmada *"Siber Güvenlik (Cyber Security)"* yerine kullanılmaktadır. Siber Güvenlik kavramının kullanımı teknik bilimler açısından daha ağır basmaktadır ve özellikle bu alandaki çalışmalarla sosyal bilimler alanındaki kullanımına ilişkin bir ihtilaf oluşmaktadır.

Şekil 6: Enformasyon ve Bilimin Tipolojisi



Kaynak: Hayes ve Alberts, 1995

Kamu ve özel sektörü ilgilendiren belli bir alana ilişkin temel parametreler sunan siber politikalar, uluslararası ilişkiler temelinde kimi zaman dünyayı salt saldırı-savunma ikileminde görmekte; kimi zaman da teknik durumları kavramada başarısız olan bir tablo karşımıza çıkarmaktadır (Stone, 2012: 102). Siber güvenliğe ilişkin sosyal bilimler temelinde ve uluslararası ilişkiler temelindeki çalışmaları doğru anlama adına *sibernetik, siber toplum, siber terörizm, siber tehdit, siber caydırıcılık, siber savaş, siber istihbarat* gibi kavramların doğru anlaşılması gerekmektedir.

1.2.1. Sibernetik Kavramının Güvenliğe Girişi ve Siber Uzay

Sibernetik canlı ve cansız tüm karmaşık sistemlerin denetlenmesi ve yönetilmesini inceler. Sibernetik, düzenli sistemlerin, bu sistemlerin yapılarının, limitlerinin ve sistemin imkanlarının araştırılmasına ilişkin disiplinlerarası bir yaklaşım içermektedir. Konu aldığı sistemler mekanik, fiziksel, biyolojik, düşüncel ve sosyal bilimlerin birçok farklı alanına ilişkin olabilmektedir.[29] Modern sibernetiğin kurucuları arasında gösterilen Amerikalı matematikçi ve felsefeci Norbert Wiener, sibernetiği insan ve hayvanlarda kontrol ve iletişimi konu alan çalışma alanı olarak tanımlamıştır (Wiener, 1948: 54).

[29] Sibernetiğin etkilediği ya da sibernetikten etkilenen çalışma alanları arasında oyun teorisi, sistem teorisi, algısal kontrol teorisi, sosyoloji, psikoloji, felsefe ve mimarlık yer almaktadır.

Sibernetiğin kavramsal olarak güvenliğe girişi, teknolojik gelişim ve bunun doğurduğu etkileşim ile ortaya çıkmıştır. Tüm canlılar arasındaki bilişsel etkileşim teknolojik gelişmeler ile birlikte ekonomik ve fiziksel sonuçlar doğurmaya başlamıştır. Özellikle bilgi güvenliği ve korunmasına ilişkin siber araçlar ile birlikte uluslararası ilişkiler temelinde bireyler ve devletler de nasibini almıştır.

"Siber uzay"[30] ise sibernetik dediğimiz kavramın verisel olarak etkileşimde bulunduğu alana ilişkin bir terimdir ve uluslararası güvenlik açısından yeni bir savaş ortamını doğurmuştur. Siber uzay, içerisinde bilginin çevrim içi olarak saklandığı, paylaşıldığı ve iletildiği, bilgisayar ağlarının ve arkalarındaki kullanıcıların yer aldığı karmaşık bir ortamdır. Siber uzayın en başta bir bilgi ortamı olduğunun anlaşılması önemli bir hususdur. Bu durum aynı zamanda siber uzayın fiziki bir yer olmadığının anlaşılması ile ilişkili bir durumdur (Singer ve Friedman, 2015: 29).[31] Dikkat edilmesi gereken husus etki doğurabildiği alanla ilgilidir ve burada fiziksel çevre devreye girmektedir.

Şekil 7'de sibernetik kavramının alana ilişkin kapsayıcılığı ile ilgili kurulum, sosyal bilimler ve sayısal bilimler dağılımıyla ortaya konulmaya çalışılmıştır. Özellikle siber uzay açısından kapsayıcılık insan ve makine özelinde bilimsel bir nitelik olarak çeşitlenmektedir ve sibernetiğin çıkış noktasını oluşturmaktadır. Her ne kadar sosyal bilimler içerisindeki çalışmalar son yıllara özgü gibi görünse de siber güvenliğe ilişkin felsefi ve sosyolojik yaklaşımlar yıllar öncesine dayanmaktadır. Siber güvenlik ve alana ilişkin yapılan çalışmaların sosyal bilimlerde adaptasyonunu da kolaylaştıran bu unsur olmuştur. Hatta günümüzde politik çıktılarla tartışılması bu uzantının bir devamı niteliğindedir.[32]

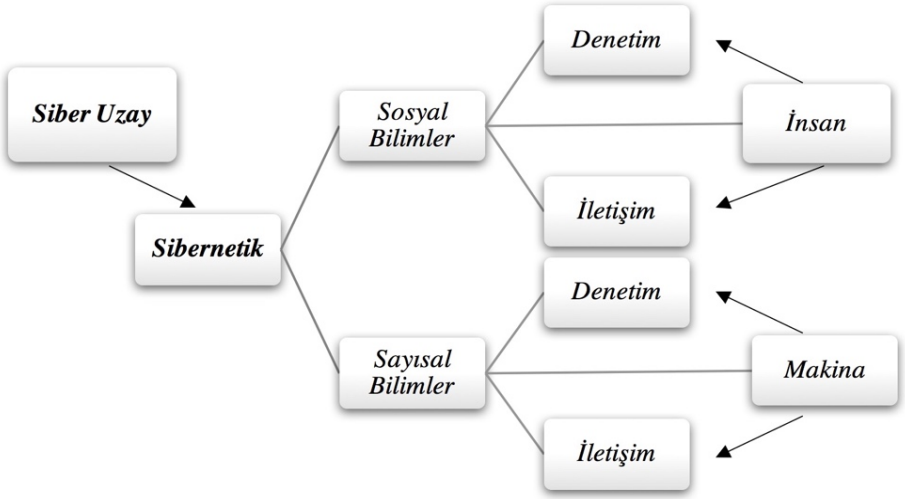
---

[30] *Siber uzay (Cyberspace)* terimi ilk kez Amerikalı bilim-kurgu yazarı William Gibson tarafından kullanılmıştır. Terim, 1982 yılında basılan *"Burning Chrome"* adlı hikaye kitabında geçmiştir. Gibson, siber uzayı tasarladığı karakterler için şifre maksadıyla "çağrışım yapan ve özellikle anlamsız" bir terim olarak tanımlamıştır. (Bkz. Çifçi, 2013)

[31] Siber ortam denildiğinde; genellikle *sanal alem* ve sanal alemden kastedilen *internet ortamı* ilk olarak akla gelmektedir. Siber ortam, internet ortamını da kapsayan bir üst kavramdır. İnternete bağlanamayan fakat sadece bir ekran vasıtasıyla içindeki sayısal değerlere ulaştığımız elektronik cihazdaki veriler siber ortamdadır. Siber ortam kapsamına; bilgisayarla ulaşılan *sayısal ortam, internet ortamı, sanal gerçeklik ortamı* ve elektronik teçhizat ile ulaşılabilen *imgesel ortamlar* (rüya gibi) girmektedir.

[32] Farklı toplumlar birçok alanda olduğu gibi, sibernetik alanında da kendi yetiştirdikleri bilim adamlarıyla övünmektedirler. Fransızlar bu konuda ünlü matematikçi Paskal ve ünlü düşünür Descartes ile öğünmektedirler. İngilizler ise aynı konuya bilgisayar biliminin babası sayılan Charles Babbage'in öncülük ettiğini ileri sürmektedirler. Almanlar ise Leibniz'i bu konuda en büyük önder olarak tanımaktadırlar.

Şekil 7: Sibernetiğin, Siber Uzay İçerisinde Bilimsel Olarak Kurulumu



Kaynak: Vinnakota, 2013: 109

Siber uzayın uluslararası güvenlik açısından tartışılması, devletlerin dış politikada ve iç politikada sahip olduğu çıktılara ilişkin nedensel bir düzlem oluşturmasıdır. Güvenlik yaygın olarak anlaşıldığı gibi sadece tehlikeden uzak olmak değil, aynı zamanda bir düşmanın olmasıyla da ilgilidir ve siber uzay açısından taraflar farklı araçlarla bu mücadelenin içindedir. Siber uzaya ilişkin, uluslararası ilişkiler açısından bir savaş alanı olup olmadığına dair en büyük eleştiri, teknik anlamda dijital ortamdaki tüm araçların fişinin çekilmesi durumunda son bulacağıdır ve göreceli olduğudur. Böyle bir durumda da organik bir durumun devam edeceği gözlerden kaçırılmamalıdır.

1.2.2. Sibernetik Toplum ve Karar Alıcılar

Canlı ve cansız varlıkların denetimine ilişkin kullandığımız sibernetik kavramı toplumun nitelendirilmesinde ve kavramın siyasileşmesinde öze ilişkin bazı unsurlar barındırmaktadır. Özellikle *bilgi teknolojilerinin*[33] günlük hayatın bir parçası haline gelmesi ve insanların haberleşme şekillerini değiştirmesi, sadece sosyalleşme adına bir çerçeve

[33] Günümüzde *"Bilgi Teknolojisi"* terimi, bilgisayar ve teknolojinin çeşitli yönlerini içine alacak şekilde genişlemiş ve bilinir hale gelmiştir. *BT* alanında çalışanlar, uygulama yüklenmesinden karmaşık bilgisayar ağlarının ve veri tabanlarının tasarımına varan çeşitli görevleri yerine getirirler. Bu görevlerden bazıları, veri yönetimi, ağ bağlantıları, bilgisayar donanımı, veri tabanı-yazılım tasarımı ve sistem yönetimini içerir.

oluşturmamış; bunun yanında bilgi, tavsiye ve karar verme sürecinde iş birliği yapabilir hale gelmiştir (Bayraktar, 2015: 139).

Bilişim teknolojilerindeki gelişme, toplum ile karar alıcılar arasında iki yönlü bir iletişim kanalı da oluşturmuştur. Bu iletişim kanallarından ilki bireylerin karar alıcılara etki edebilmesi ile igilidir ve başlı başına, medyadaki gelişmelerle birlikte ayrı bir çalışma konusudur. Sibernetik toplum ve karar alıcılar arasındaki yönetim biçimi de bu geniş çalışma içinde otokontrol, bilgi aktarımı, bilişsellik gibi unsurlarla interdisipliner bir yön göstermektedir.[34] Bu konudaki gelişim tahmin edilemeyecek bir boyuta ulaşmıştır ve devletler yönünde artık bir yarış haline gelmiştir.

Bilgi teknolojileri, özellikle karar alıcılar açısından toplumsal tepkinin ölçülmesi ve takip edilmesi adına önemli bir araç haline gelmiştir. Diğer yönü ise bu çalışmanın da kapsamını ve derinliğini oluşturan politika oluşturmaya ilişkindir. Devletler bu kapsam dahilinde kendi içerisinde uzman ekipler oluşturarak karar alıcılar açısından takip edilen bir alanı ortaya çıkarmıştır. Bu alan içerisine askeri unsurların da dahil olması, organizasyonel bir gerekliliği gündeme getirmiştir. Siber uzayda stratejistler ve karar alıcıların caydırıcı olma adına taktiksel unsurlar geliştirmesi, toplumsal değişimi de sağlamıştır. Fakat karar alıcılar ve toplumsal özellikler açısından bu alanda gelişmiş ve gelişen/gelişme arzusu içinde olan devletler arasındaki fark daha açık bir şekilde ortaya çıkmıştır (Stevens, 2012: 149).

Toplumsal alanda siber güvenliğe ilişkin karar alınmasında vurguladığımız bilgi teknolojilerinin kullanılış amacı ve ortaya çıkış noktası ile karar alma sürecinde karar alıcıların sahip olduğu arka plan belirleyici olmaktadır. Oluşturulan uzman ekipler de bu vizyon dahilinde ortaya çıkmaktadır. Şekil 8'de karar alma sürecinde inancın felsefi boyutunda ve uygulama niteliğinde, çeşitli imajlarla bilginin karar alma çıktısına dönüşümü gösterilmektedir. Sibernetik toplum adına da bilginin, bilgi teknolojileri ile daha kapsamlı hale gelmesi ve karar alıcının siber güvenlik alanına da verdiği öncelik stratejik açıdan bir kazanç oluşturacaksa benzer bir süreçle ele alınmalıdır. Bu noktada karar alıcının kendisine

[34] Sibernetik konusunda çeşitli üniversite ve tıp fakültelerinde çalışmalar yapılmaktadır. Bu çalışmalar sonunda, artık sibernetik bilim çevrelerinin olduğu kadar halkın da ilgilendiği bir bilim dalı haline gelmiştir. Mesela, günümüzde bilgisayar işlemleriyle beynin çalışmaları arasındaki ilgi birçok kesimin yakından bilgi sahibi olduğu bir konu haline gelmiştir.

ve dış dünyaya ilişkin bilgileri ile sahip olduğu toplumsal değerler bu döngüde belirleyici olacaktır.

Şekil 8: İnanç Sistemi, İmaj ve Karar Alma Süreci

Kaynak: Sönmezoğlu, 2014: 322

Bu alan içerisindeki toplumsal dalgalanmalar, günümüzde çağdaş toplumun biçimlendirilmesinde önemli bir yere sahip olmuştur ve teknolojinin yarattığı olanaklar sayesinde birbirine elektronik olarak bağlanmış bilgisayar kullanıcılarının her biri özel birer aktör haline gelmiştir. Karar alıcıların bu konudaki çelişkisi iç ve dış politikaya ilişkin alanda şeffaflık ile politika üretmeye ilişkin olmuştur (Çakmak ve Altunok, 2009: 27).

Politika üretiminde karar alıcıların siber güvenliğe ilişkin gizlilik esasları bu alandaki belirleyici unsur haline gelerek toplumsal bir gelecek kurgusunun temelini oluşturmaktadır. Teknolojik anlamda günümüzün gelişmiş ülkelerinde dış politika kararlarının geniş ve karmaşık bir düzende ortaya çıkışı, kişilerin psikolojik çevrelerinin de oluşumunda sibernetik toplum açısından ciddi farklılıklar oluşturmaktadır.

1.2.3. Siber Terörizm ve Siber Tehdit Algısı

Terörizmin tarihsel düzlemde gelişimi analiz edildiğinde, devletlerin güç kullanmalarının bir devamı olarak, savaşların sonunda galip tarafın mağlupları cezalandırarak, asker ve sivil halka karşı yaygın bir şekilde şiddet uygulaması olarak gözlenmiştir. Savaş ve diplomasi yoluyla elde edilemeyenin sonuçlarına yaklaşmak

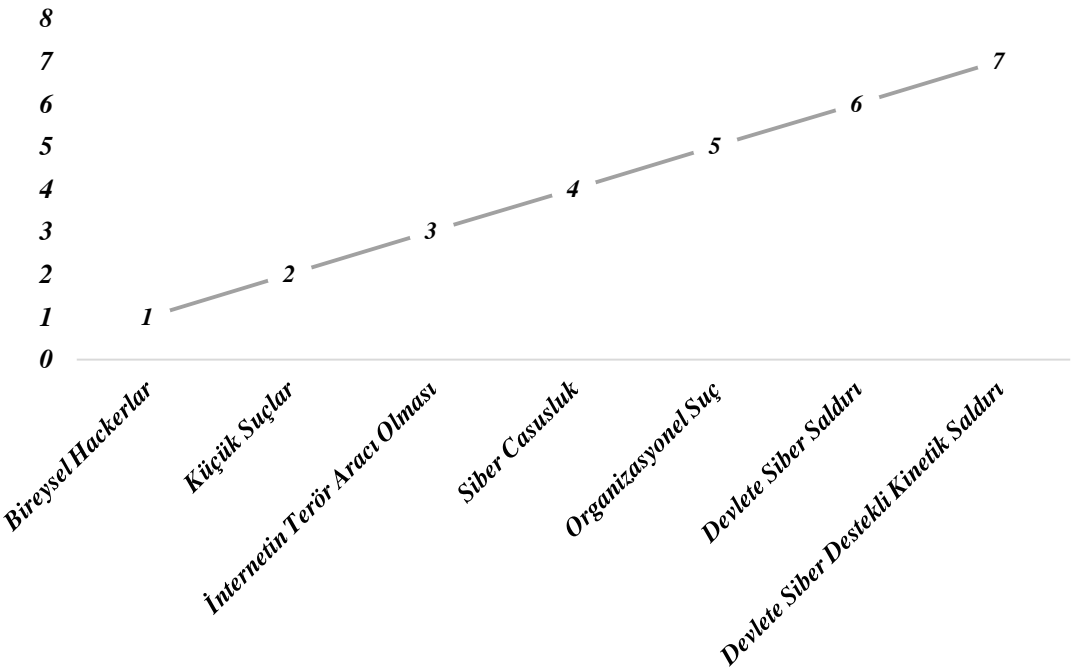
amacıyla, korkutmak ve itaat ettirmek için bir teoriye, felsefeye ve ideolojiye dayandırılarak siyasi maksatlarla, iradi olarak şiddetin sistemli bir şekilde kullanılmasına "*terörizm"* denmektedir (Caşın, 2008: 35).

"Siber terörizm"[35] kavramının ise uluslararası alanda gelişimine ilişkin tartışmalı bir durum söz konusudur. Siber terörizm, bilgisayar ağlarını bozmaya yönelik kasıtlı ve geniş kapsamlı eylemler dahil olmak üzere, terör eylemlerinde internet tabanlı saldırıları ve internete bağlı kişisel bilgisayarları kullanmaktadır. Dar anlamına bakıldığında siber terörizm açısından insanların can ve mallarını tehdit eden saldırılar bu kapsama girerken; geniş anlamda, can ve mal tehdidine ilave olarak, sosyal, dini, ideolojik, politik veya başka amaçlarla bilgisayar ağlarına yapılan saldırılar da siber terörizm kapsamına girmektedir (Çifçi, 2013: 6). Günümüze kadar gelen tarihin stratejik olarak şekillenmesinde, olayların sonuçlarına ilişkin yaklaşımda tehdit olgusunun algısı ve modern olarak tehdit, siber terörizmin kapsamını da şekillendirmektedir (Gray, 2007: 264).

Siber terörizmin beslendiği nokta ve harekat bulma süreci *siber tehditlerle* ilgilidir ve kaynaklandığı noktalar da bu kavrama dahildir. Siber tehditler internete bağlanmayı sağlayan ve çevrimiçi saldırılara maruz kalmayı olanaklı kılan araçların oluşturduğu unsurlardır. Siber tehdit yöntemleri ve ortaya çıkış süreci sanal bir ortamda gerçekleşince maddi ve manevi, fiziksel sonuçlar doğurmaktadır ve bu sonuçların geri dönüşü olmayabilir. Bu suçların etkileyici olmaları bireysel olmalarına, kurumsal bir etki oluşturmasına ya da devlet gibi uluslararası aktörlere etki edişine göre farklılaşmaktadır. Grafik 3'te görüldüğü üzere özellikle bireysel anlamda işlenen bilişim suçları ve bunların etki düzeyleri, istihbarat alanına ilişkin tehditsel unsurlar ve devlete yönelik siber saldırı ya da devlete siber destekli kinetik saldırılar aynı derecede değildir ve bir etki alanına sahiptir. Devletlerin çoğu zaman müdahil olduğu siber olaylar, çoğu zaman organizasyonel suçlardan daha etkili sonuçlar doğurabilmektedir.

[35] Terörizmin nitelikleri göz önüne alındığında yapılan siber faaliyetlerin bir terörizm mi olduğu ya da siber terörizm olarak ifade edilmesi hususu halen tartışma konusudur. Mehmet Özcan siber terörü şu şekilde ifade etmektedir: *"Siber terörizm belirli bir politik ve sosyal amaca ulaşabilmek için bilgisayar sistemlerinin bireylere ve mallara karşı bir hükümeti veya toplumu yıldırma, baskın altında tutma amacıyla kullanılmasıdır."* Konu ile ilgili ciddi çalışmalar yürüten FBI siber terörizmi *"alt-ulus grupları veya gizli örgütler tarafından, savaşçı olmayan hedeflere karşı şiddete son bulan bilgi, bilgisayar sistemleri, bilgisayar sistemleri, bilgisayar programları ve verilere karşı önceden planlanmış siyasi güdümlü saldırı."* olarak tanımlamıştır.

Grafik 3: Siber Tehditlerin Dereceleri



Kaynak: Bucci, 2009

Siber tehditlerin uluslararasılaştığı boyutta felsefi ve ideolojik yaklaşım uluslararası güvenlik sorunlarıyla birlikte ele alınmaktadır. Bu noktada siber güvenliğe ilişkin veriler ve çalışmalar siber terörizmin gelişimine ilişkin kavramsal bir durumu ortaya çıkarmaktadır. Siber uzaya artan bağımlılık, terörizm boyutuyla farklı derecelendirmeler sunmaktadır (Choucri, 2013: 19).

Siber terörizmin hem uluslararası alanda verisel güvenliği tehdit eden düzeyi hem de bireylerin sahip olduğu kapasite Tablo 3 üzerinde sınıflandırılmıştır. Siber terörizme ilişkin verilerin örgütsel kapasiteye sahip olması durumunda ve koordinasyonlu boyutunda daha stratejik ve karmaşık eylemler gerçekleştirilebilmektedir. Bu konuda hedeflenilen amaca yönelik strateji belirlenmesinde, ciddi ve derin bir analize ihtiyaç duyulmaktadır. İleri düzey ve karmaşık koordinasyonlu siber terör düzeylerinde, birden fazla hedef gösterilen ağlarda, tehdit derecelerinin artmasıyla, yıkıcı ve fiziksel sonuçlar doğabilmektedir. Karmaşık-koordinasyonlu düzeylerde fayda olarak stratejik eylemler, potansiyel fayda olarak tanımlanmaktadır ve hedef analizi ayrıntılı bir şekilde yer almaktadır.

Tablo 3: Siber Terör Eylem Düzeyleri

Siber Terör Düzeyleri	*Hedef*	*Hedef Analizi*	*Örgütsel Kapasite*	*Etki Kontrolü*	*Potansiyel Fayda*
Basit-Yapılandırılmamış	*Tek Sistem ya da Ağ*	*Başlangıç Seviyesinde*	*Az Seviyede*	*Odaklı Değil*	*Propaganda*
İleri Düzeyde-Yapılandırılmış	*Birden Çok Sistem ya da Ağ*	*Orta Seviyede*	*Orta Seviyede*	*Odaklı*	*Taktiksel Eylemler*
Karmaşık-Koordinasyonlu	*Birden Çok Ağ*	*Detaylı*	*Çok İleri Düzeyde*	*Kontrol Edilebilir*	*Stratejik Eylemler*

Kaynak: Bayraktar, 2015: 80

Düzey olarak; sosyal, dini, ideolojik ve politik amaçlarla siber tehdit oluşturan terörist ya da terörist grupların bilgi harekatlarını kullanış mantığı ve çerçevesi de değişmiştir. Özellikle *kritik altyapıların*[36] hedef alınması uluslararası terörizm açısından siber terörizmin daha anlaşılabilir ve mücadele edilmesi gereken bir yönünün de olduğunu ispatlamıştır. 2011 sonrasında, ABD'deki kritik altyapı bilgisayar ağlarının yoklanması ve izinsiz girişler %1700 artmıştır (Singer ve Friedman, 2015: 136).

Kritik altyapı gibi unsurlara saldırılar özellikle siber terörün, klasik terör mantığı ve anlayışıyla ayrıştığı ve benzeştiği noktaları da gruplandırma olanağını bizlere sunmuştur. Tablo 4'te görüldüğü üzere, klasik terör ve siber terör arasındaki farklara ilişkin temel noktada kullanılan araçların ve etki alanın baskın şekilde farklı olduğunu görmekteyiz. Donanımsal ve yazılımsal anlamdaki silahların artık fiziksel sonuçlar doğurduğu, kullanılan araçların çıktısı açısından benzerlik göstermektedir. Siber terörün yaşamsal risk olmadan neticeye götürmesi ve sonuç verdirmesi bu alandaki terörist aktivitenin çok büyük

[36] *Kritik altyapı* kavramı özel bir öneme sahiptir. Bu altyapılardan işlenilen bilginin gizliliği, bütünlüğü veya erişilebilirliği bozulduğunda; can kaybına, büyük ölçekli ekonomik zarara, ulusal güvenlik açıklarına veya kamu düzeninin bozulmasına varabilecek ciddi sıkıntılar doğabilmektedir. Kritik altyapılar devlet düzeninin ve toplumsal düzenin sağlıklı bir şekilde işlemesi için gerekli olan ve birbirleri arasında bağımlılıkları olan fiziksel ve sayısal sistemlerdir. Enerji üretim ve dağıtım sistemleri, telekomünikasyon altyapısı, finansal servisler, su ve kanalizasyon sistemleri, güvenlik servisleri, sağlık servisleri ve ulaştırma servisleri en başta gelen kritik altyapılar olarak sıralanabilir.

derecelerde artmasını sağlamıştır. Denetim açısından da ciddi bir avantaja sahip olan siber terör, özellikle karar alıcılar açısından tercih edilir bir noktada, illegal gruplarla iş birliğini de kolaylaştırmıştır.

Tablo 4: Klasik Terör ile Siber Terör Arasındaki Farklar

	Klasik Terör	***Siber Terör***
Kullanılan Araç	*Silah, bomba gibi araçlar*	*Çipler, bilgisayarlar veya bilgi sistemlerinde kullanılan diğer donanımlar, yazılımlar*
Amaç	*Siyasi rejime ve topluma mesaj vermek için terörizm bir amaç*	*Yaplan eylemler ile topluma veya devlete zarar verme, siyasi ve sosyal olarak etkilemek için terörizm bir amaç*
Etki Alanı	*Saldırının yapıldığı bölge ya da alan ile sınırlı*	*Ulusal veya uluslararası boyutlarda etkili*
Karşılaşılan Risk	*Eylemi gerçekleştiren kişi ya da grup yaşamsal risk altında*	*Herhangi yaşamsal riski olmadan etkili saldırı*
Denetim	*Terörü kontrol altında tutma, izlemek ve yok etmek kısmi anlamda mümkün*	*Siber teröristleri tespit etmek veya yok etmek imkansız*
Uygulanacak Ceza	*Suçun niteliğine göre uygulanacak ceza belli*	*Suçun niteliğine göre uygulanacak ceza belli*

Kaynak: Bayraktar, 2015: 77

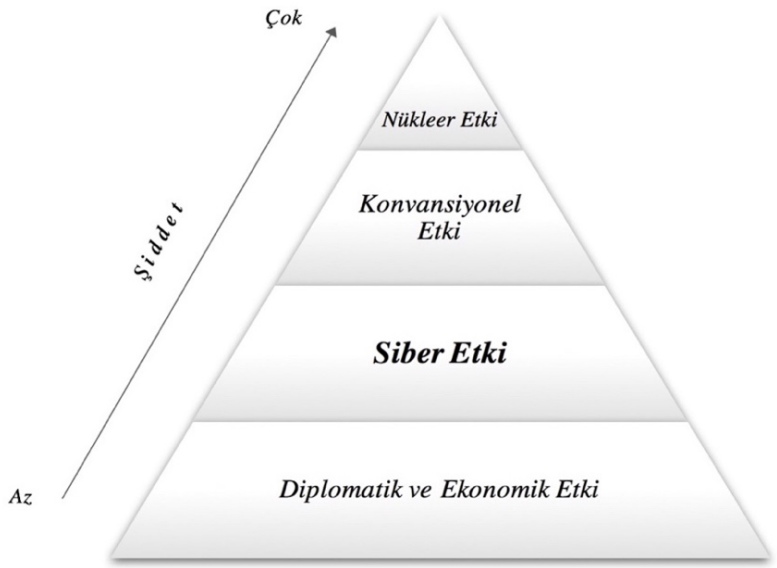
1.2.4. Siber Caydırıcılık

Caydırıcılık; bir devlet veya topluluğun, başka bir devlet veya topluluğun aleyhine olabilecek hareketlerden sakınması için gerekli tedbirleri alması olarak tanımlanmaktadır. Caydırıcılık bir bakıma, anlaşmazlığın tırmanarak askeri kuvvet kullanımını gerektirmesine engel olmaktadır. Uluslararası güvenlik literatüründe caydırıcılığın *esirgeme (deterrence by denial)* ve *missileme (deterrence by retaliation)* olmak üzere iki yönü bulunmaktadır (İduğ ve diğerleri, 2013: 287).

"Siber Caydırıcılık"[37] kavramı üzerinden birçok çalışmaya dair tespitler, caydırıclık kavramının Soğuk Savaş teorileriyle kıyaslanması üzerinden ele alınmaktadır ve tartışılmaktadır (Lupovici, 2011: 51). Bunun en önemli sebebi caydıcılığa ilişkin uluslararası ilişkiler perspektifinde daha önce bahsettiğimiz iki yönlülüğe dair, savunmayla ilgili kargaşa ve yanlış anlaşılmanın mevcut oluşudur. Siber saldırıların bir yönü vardır fakat savunması zordur ve tespitine ilişkin kesin veriler kimi zaman olmayabilmektedir.

Libicki (2009) verisel gelişmelere bağlı olarak siber etkiyi ve oluşturduğu caydırıcılığın, diplomatik ve ekonomik yaptırımların önüne geçtiğini yapmış olduğu karşılaştırma ile göstermiştir. Şekil 9'da görüleceği üzere, hala konvansiyonel ve nükleer etkinin sahip olduğu caydırıcılık temeli şiddet olarak daha üstlerde yer alsa da, konvansiyonel ve nükleer altyapıların siber altyapılara bağlandığı uluslararası sistemde bu şiddet sarmalı ve hiyerarşisi her an değişiklik gösterilebilir ve hatta farklı örneklerde siber etki üst sıralara taşınabilir.[38]

Şekil 9: Siber Caydırıcılığın Etkisel Olarak Karşılaştırılması



Kaynak: Libicki, 2009: 29

[37] Caydırıcılık dediğimiz kavram stratejik olarak farklı tarzlarda incelenmektedir. Bazıları *tekil (tek defalık)*, bazıları *tekrarlı*, bazıları *simetrik (karşılıklı)*, bazıları ise *asimetrik (tek taraflı)* olabilir.

[38] Siber güvenlik konularında uzman olan Martin Libicki'ye göre siber caydırıcılık, Soğuk Savaş dönemindeki nükleer caydırıcılık gibi işe yarayabilir. Fakat bunun imkanlı olması için devletlerin siber uzaya bağlılığı tam ve eksiksiz olmalıdır.

Nükleer caydırıcılık, tekil ve simetrik bir özellik göstermektedir. Tekil olmasının sebebi etkilerinin korkutucu ve geri dönüşünün olmayışından kaynaklanmaktadır. Bu anlayış çerçevesinde kimse kullanmaya da cesaret edememektedir. Misilleme durumunda karşı tarafın saldırıya cevap vermesi ile her iki taraf için de büyük yıkım olabilir. Siber caydırıcılıkta ise tekrarlılık söz konusudur. Uygulanan siber misilleme, muhtemelen saldıran devleti bertaraf etmez, hükümetin düşmesine neden olmaz veya saldıranın silah bırakmasını sağlamaz. Siber saldırılar, emsaller arasında meydana geldiği için aynı zamanda simetrik bir özellik gösterir (Çifçi, 2013: 306). Uluslararası güvenlik açısından siber saldırıların savunulmasındaki belirsizlik ya da kimi zaman anlam kargaşası, klasik anlayış açısından caydırıclığın farklı tarzlarda gerçekleşmesi ve hiyerarşisi açısından bir tespiti de gerekli kılmaktadır (Hosein ve Eriksson, 2007: 162).

Siber caydırıcılığa yapılan en büyük eleştiri, bir siber saldırının nereden gerçekleştiğini bulmanın güç oluşudur. Siber savunma kabiliyeti yüksek olduğu sürece siber saldırılar boş çaba olarak görülecek ve bu yola başvurulmayacaktır. Böylece siber savunma kendi başına bir caydırıcılık sağlayacaktır. Stuxnet örneği göstermiştir ki, hedefte büyük tahribata yol açmayan siber saldırılar hedefin güvenlik açıklarını görmesini sağlayarak bu açıklıkları gidermesine olanak verecek bir sonraki benzer saldırıları boşa çıkarabilecektir (İduğ ve diğerleri, 2013: 288).

Libicki'nin modeliyle benzerlik gösteren tırmanma modelinde saldırıların niteliğine göre tırmanmanın en üstünde nükleer silahlar yer almaktadır. Bendier ve Metzger (2015: 11); yapmış oldukları bu analizde, Şekil 10'da görüleceği üzere yüksek seviyeli siber saldırıların niteliksel olarak kinetik vuruşlardan daha etkin olduğunu vurgulamıştır ve özellikle son yıllardaki gelişmelere paralel olarak doğru bir tespittir. Kritik altyapılara ilişkin fiziksel saldırıların niteliği korkutucu boyutlarda etki yaratma kapasitesine sahiptir. Düşük seviyeli siber saldırılar bu kapsamda tırmanma modeli açısından politik ve ekonomik yaptırımlardan daha etkili sonuçlar doğurabilmektedir.[39]

[39] İran'ın Natanz Nükleer Santrali'ni hedef alan Stuxnet örneğinde görüldüğü gibi, siber dünyada başlatılan ancak fiziksel dünyada yıkıcı sonuçlar doğuran gelişmiş siber silahlar günümüzde yadsınamayacak bir gerçekliktir. Boru hatlarını, elektrik altyapılarını hedef alan saldırılar hatırı sayılır derecede artmış durumdadır. Maryland Üniversitesi'nin oluşturduğu *"Küresel Terörizm Veri Tabanı"*na göre 1970'lerden 1990'lı yılların ortalarına kadar enerji üretim tesislerine, boru hatlarına ve sektör çalışanlarına yönelik yılda 100'den az saldırı kaydedilmişken, yalnızca 2013 yılında bu saldırıların sayısı 600'e yaklaşmıştır (Gücüyener, 2015).

Şekil 10: Tırmanma Modeli

Kaynak: Bendiek ve Metzger, 2015: 11

Siber caydırıcılığın amacı, siber saldırı riskini kabul edilebilir bir maliyet ve seviyeye indirmektir. Siber savunma ve bilgi güvenliği kimi zaman çok pahalı da olabilmektedir. Saldırı, siber saldırı kapasitesi oluşturulması açısından daha ucuzdur. Diğer taraftan siber caydırıcılık politikası sayesinde kurtarılacak maddi durum da abartılmamalıdır.

Richard Clark'ın[40] özellikle caydırıcılık ve siber caydırıcılığın bütününe ilişkin yapmış olduğu tespitler kayda değerdir ve düzlem olarak siber uzaya ilişkin verdiği örnek ve anlatım şu şekildedir (Clarke ve Knake, 2011: 98):

> *"…Gerçek dünyada ABD neden olacağı karşı saldırının Amerikan ağları üzerindeki asimetrik etkisinden çekineceği için büyük ölçekli siber savaş başlatmayacaktır.*
>
> *…Ancak, 1960'lı yıllarda kitaplar yazmış olan Herman Kahn gibi stratejistlerin teorilerinin aksine, siber savaş caydırıcılığı çok daha değişik olasılıklar içermektedir. Nükleer silahlara ilişkin bütün ayrıntılar bilinmektedir. Siber silahların ise ne yapacağı şu ana kadar dünya devletleri tarafından gözlenmemiştir.*
>
> *…Nükleer savaşta iki tarafın da saldırı kabiliyetleri bilindiği için, ortada bir sır yoktu ve herhangi bir saldırı anında büyük bir olasılıkla dünyadaki tüm yaşamın yok olacağını herkes*

[40] *"Cyber War, The Next Threat to National Security and What to Do About It"* adlı kitabın da yazarı olan Clarke, *"Siber Savaş"* olarak adlandırdığı çekişme alanıyla ilgili ABD'de bağımsız bir merkezin de yürütülmesinde önemli görevler almıştır.

bilmekteydi. Siber savaşta ise, saldırının gücü bir sır olarak kalmaya devam ediyor. Etkin bir savunma kurma olasılığı var. Bu yüzden, hiçbir ulus bir kriz halinde caydırıcılıktan dolayı siber silah kullanmazlık etmeyecektir."

1.2.5. Siber Savaşlar Gerçek mi?

Toplumlararası ilişkilerin doğası çatışmaya dayalıdır. Bu çatışma, bazı dönemlerde bariz bir hal alırken, bazı dönemlerde kendisini gizlemiştir. Uluslararası ilişkiler çalışmaları adına kırılma noktası olan I. Dünya Savaşı'nın da öncesinde; 1815 Viyana Kongresi sonrasında Avrupalı güçler arasında hakim olan hava, artık Avrupa coğrafyasında bir savaş olmayacağı, ortaklıklara daha fazla vurgu yapılacağı yönündeydi (Toptaş, 2009: 15). Fakat 20. yüzyıl içerisindeki başdöndürücü gelişmeler tarihin gördüğü en büyük iki savaşı beraberinde getirmiştir.

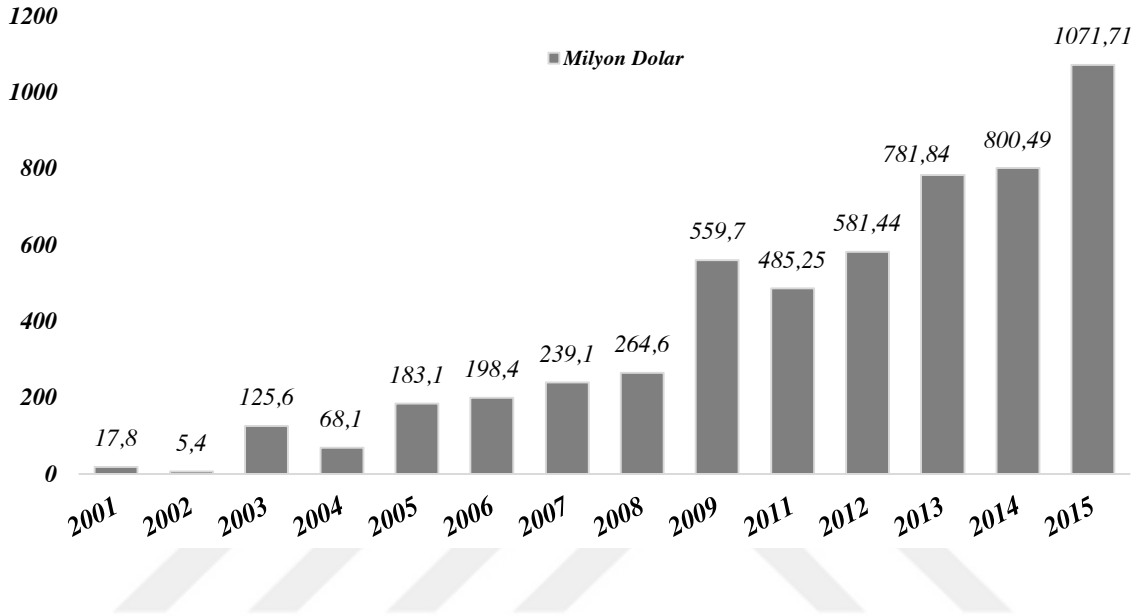
Yaşanan iki savaş ve çıkarılabilecek derslerin aksine; değişimin getirmiş olduğu imkanlar ve stratejiler askeri unsurların yıkıcı özelliklerini inanılmaz boyutlara taşımıştır. Bu durumu göze almak istemeyen aktörler, birbirlerini caydırmada ve etkilemede farklı saldırı ve savaş tekniklerini geliştirmeye başlamıştır. *Siber savaş* olarak adlandırdığımız gücün göreceliği üzerine kurulu küresel mücadele beraberinde ciddi bir karmaşıklığı da beraberinde getirmiştir.

Küresel mücadeledeki karmaşıklık ve değişim aslında önemli bir teorisyen olan Kenneth Waltz'un 1954'te vurguladığı verileri destekler niteliktedir. *"Man, State and the War"* adlı eserinde savaşın nedenleri ve gelişimi ile ilgili görüş ayrılıklarını ortaya koymaya çalışan Waltz, filozoflar arasındaki görüş ayrılıklarının aslında belirleyici olmadığını, sadece zamanın ve uygulamanın değiştiğine dikkat çekmektedir. Aslında kendi zamanından örneklerle yola çıkan Waltz, farklı teorilerin farklı yaklaşımları beraberinde getirdiğini, eğer ortada bir çatışma varsa bunun niteliğinin değişebileceğini vurgulamaktadır.

Niteliksel olarak bu değişim sadece savaş alanlarına ve cepheye ilişkin verilerle evrimini devam ettirmemiştir. Siber savaşın maddi ve fiziksel olarak etkisi ciddi bir maliyeti de beraberinde getirmiştir. Grafik 4'te IC3'e raporlanan maddi kayba ilişkin verilerde son 15 yılda yaşanan değişim 60 kata kadar çıkmıştır. Uluslararası sistemde toplam maliyetin

uluslararası aktörler bazında, ne kadar olduğuna ilişkin kesin veriler olmasa da siber savaşın kapasitesi ve etkisine ilişkin değerler mücadelenin yönünü ortaya koymaktadır.

Grafik 4: 2001-2015 Yılları Arası Siber Saldırı ve Suçlardan Dolayı IC3'e Raporlanan Maddi Kaybın Değişimi[41]



Kaynak: The Statistics Portal, 2016a

1.2.5.1. Asimetrik Savaş[42]

Özellikle 11 Eylül sonrası dönemde kendisine yoğun biçimde referans verilmeye başlanan *"Asimetrik savaş"*[43] kavramı kimilerine göre yeni bir savaş mantığına karşılık gelmekte kimilerine ise yeni bir terör türü olarak karşılık gelmektedir. Tarafların aynı kuvvet unsurlarını kullanmasıyla karşımıza çıkan simetrik savaşa karşın asimetrik savaşta düşmanın

[41] *IC3 (Internet Core Competency Certification)* bilgisayar olayları üzerine; yazılım, donanım, network ve uygulama sistemleri bazında derecelendirme ve belgelendirme yapan küresel bir oluşumdur ve Certiport tarafından yönetilmektedir *(Bkz. www.certiport.com)*.

[42] *Asimetri* Brockhaus sözlüğünde *"eşitsizlik, simetri eksikliği"* olarak tanımlanmaktadır. Asimetri, eşitsizlik ve nispetsizlik bağlamında uluslararası ilişkilerde hemen hemen sisteme dair bir olgudur. Aktörler arasındaki yaygın ayrım da; süper güç, bölgesel güç, küçük-orta ölçekli devletler olarak eşitsizlik üzerinedir (Bkz. Ergün, 2014)

[43] Asimetri; farklı düşünerek, farklı örgütlenerek, farklı hareket yöntemleri seçerek, mevcut dengeyi bozmaktır. Var olan dengenin bir dengesizlik üzerinde kurulduğu düşünülecek olursa yürütülen mücadele yöntemlerinin anlayışsal boyutu tartışma konusudur.

dengesini kaybettirme adına tarafların tekinde olmayan farklı unsurlar karşımıza çıkabilir. Bu yönüyle asimetrik savaş, benzeşmeyen güç unsurlarının, muharabe yöntemlerinin, vasıta ve silahlarının kullanıldığı savaştır (Varlık, 2013: 125). Asimetrik güç etkinliği teknolojik üstünlük, nitelik, sevk ve irade, komuta-kontrol, disiplin-moral ve motivasyon üstünlüğü gibi kuvvet çarpanı olabilecek herhangi başka bir unsurun devreye girmesiyle ortaya çıkmaktadır.

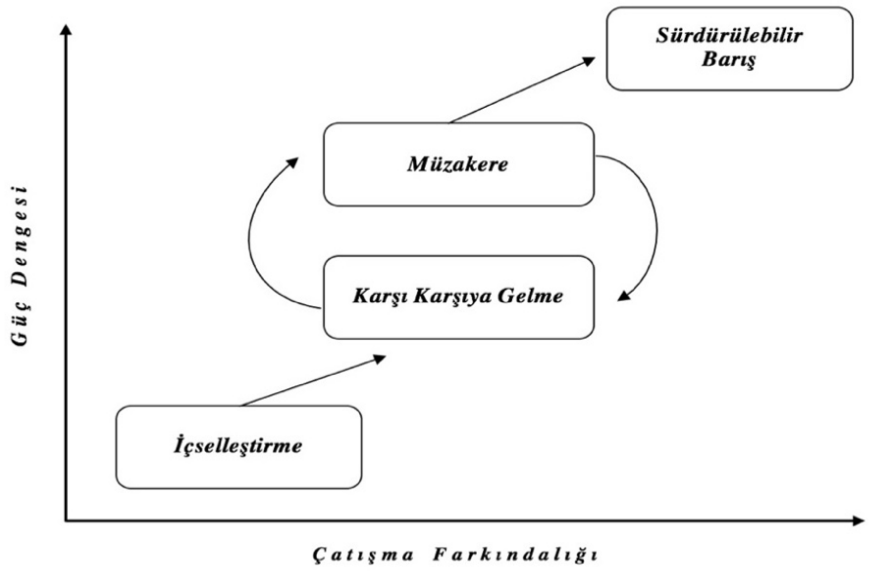
Farklı unsurların ortaya çıkışıyla asimetrik savaş adına rakip hedeflere yönelik zararın kapsamı farklı niteliklerle artmıştır. Düşmanın modern koşullar altında giderek *"görünür"* niteliğinin kaybolması, saldırgan duygusunu ortadan kaldırmaktadır. Asimetrik unsurlarla savaşın devamlılığı *"ölçülülük"* düşüncesini de ortadan kaldırmaktadır ve savaşın ruhuna yeni bir boyut katmaktadır. Özellikle konvansiyonel silahların değişimi ile birlikte askeri kayıpların yanında, inanılmaz boyutlardaki sivil kayıpları da savaşın olumsuz şekillerde ve asimetrik ölçülerle devam ettiğini ispatlamıştır (Aral, 2007: 60).

Savaşın kendi içerisindeki evrimine ilişkin asimetrik savaş kavramı dahilindeki değişimin 11 Eylül saldırıları ile uluslararası toplumun gündemine taşındığı kabul edilmektedir (Bendrath ve diğerleri, 2007: 71). Fakat Soğuk Savaş sonrası uluslararası güvenlik ortamında yaşanan değişimlerin bir sonucu olarak, devlet ve devlet dışı aktörler tarafından uygulanabilecek bir savaş anlayışı olduğunua ilişkin yaklaşımlar da asimetrik savaş adına mevcuttur. Bu anlayışa siber saldırılar anlamındaki taktiksel unsurları ve gelişmeleri de dahil edebiliriz.

Gelişen silahlar ve savaş teknolojisindeki değişim ile birlikte oluşan kayıplara ilişkin, gücün yapısı ve çatışma arasında bir değişim gözlenmektedir. Özellikle asimetriyle birlikte taraflar arasındaki çatışma yapısı ile barışın sürdürülebilirliği ve bir çıktı olarak bu durumla karşılaşılması oldukça güçleşmektedir.

Şekil 11'de görüldüğü üzere, yapısal olarak ortaya koyulan asimetrik çatışma sürecinde güç ve çatışmaya ilişkin taraflar arasındaki müzakere kültürü barışın sağlanmasında önemi bir basamaktır. Güç dengesi ve çatışma farkındalığı ekseninde ele alınan asimetrik çatışmanın evreleri sürdürülebilir barış noktasında kesişim olarak en üst dereceyi oluşturmaktadır.

Şekil 11: Yapısal Olarak Asimetrik Çatışmanın Evreleri



Kaynak: Gallo ve Marzano, 2009

Propaganda ve bilgi savaşına dayandırılan psikolojik harekatlar da asimetrik savaş kavramı içerisinde siber güvenlik alanına ilişkin bir parametre olarak ele alınabilir. Herhangi bir savaş alanına ihtiyaç duymadan gerçekleştirilebilen psikolojik harekatların ihtiyaç duyduğu, kimi zaman manipülasyon ve bilginin yayılması sürecindeki siber ortam asimetrik savaş açısından ihtiyaç duyulan harekat alanını taraflara sunmaktadır.[44]

1.2.5.2. Siber Savaş

"Siber Savaş" kavramını; "*ulusal bir hedefi gerçekleştirmek ya da süregelen bir savaşı desteklemek amacıyla, bir ülke tarafından veya inisiyatifinde, diğer bir ülkenin askeri ve sivil her türlü bilişim sistem ve altyapısının işlevselliğini engellemek, imha etmek ve kendi çıkarları doğrultusunda kullanmak için siber savaş yöntemlerinin kullanılması ve buna karşı koyacak tedbirler veya süreçler"* şeklinde tanımlamak mümkündür (Bayraktar, 2015: 48).

[44] Kavramsal temeller ve asimetrik yaklaşımları değerlendiren bir taraf, güçlü rakibin bir yandan zayıf yönlerini alışılmadık taktiklerle saptarken, diğer yandan da kamuoyunda şok ve ani psikolojik etki yaratmayı ve bu güçlü tarafın kurumlarına duyulan güveni zayıflatmayı amaçlayabilir. Böylelikle rakibin toplumsal yapısında, özellikle ekonomisinde ve motivasyonunda negatif etki yaratarak toplumsal özgürlüklerin kısıtlanmasına bile neden olabilir.

Masrafsız bir savaş vizyonuna sahip olan siber savaş, saldırının hangi tarafında bulunduğunu göre algısal bir farklılık temelinde kavramsal bir bütünlüğe sahiptir (Rid ve McBurney, 2012: 7).

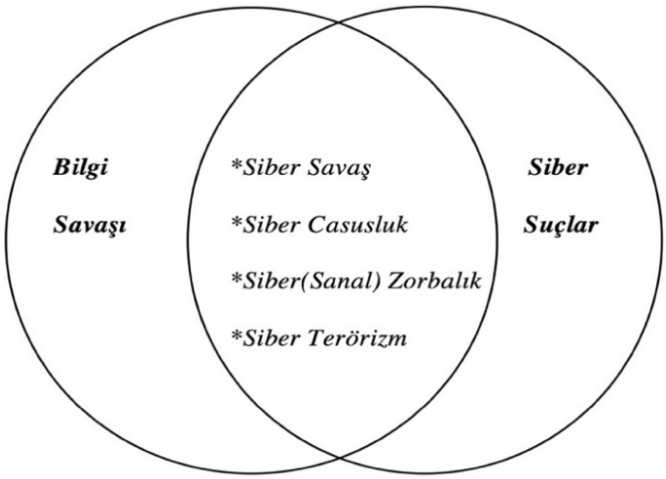
Richard Clark'ın kavramsal olarak siber savaşa yüklediği anlam, *"Bir devletin, başka bir devletin bilgisayar sistemlerine veya ağlarına hasar vermek ya da kesinti yaratmak üzere gerçekleştirilen sızma faaliyetleridir."* şeklindedir ve kapsamı dar tutulmuştur. Bunun en önemli sebeplerinden birisi enformasyon sahibi olma veya çalınması şeklindeki yaklaşımın tanımsal olarak genişliğidir. Richard Clarke, siber savaşın tanımını yaptıktan sonra, siber savaşa ilişkin şu tespitleri yapmıştır (Çifçi, 2013: 5):

> - *"Siber savaş gerçektir. Şimdiye kadar yaşananlardan daha kötüsü de yaşanabilir. Saldırganlar en gelişmiş yöntemleri açığa vurmak istememektedir.*
> - *Siber savaş ışık hızında gerçekleşmektedir. Saldırı paketleri, kablolardan ışık hızıyla akmaktadır. Saldırının başlangıcı ve etkisi arasındaki zaman aralığını ölçmek imkansızdır.*
> - *Siber savaş küreseldir. Herhangi bir siber çatışma küresel niteliktedir ve birçok ülke etkilenir ya da devreye girer.*
> - *Siber savaş, geleneksel savaş alanından önce gelmektedir.*
> - *Siber savaş artık başlamıştır. Çatışmayı bekleyen ülkeler, hazırlıklarını yapmıştır. Birbirlerinin altyapı ve ağlarına sağldırmakta, barış zamanalarında tuzak sistemleri ve arka kapıları yerleştirmektedir."*

Siber savaş bilgi teknolojilerine bağlı olarak ve siber suçlardaki farkındalığın artışıyla çıkarsal amaç içerisinde hareket eden aktörlerin ilgi alanına girmesiyle bugünkü küresel niteliğine ulaşmıştır. Bilgi teknolojilerindeki gelişmeler paralelinde, ülkeler güvenlik stratejilerini teknolojik tabanlı bir savaşa dayandırma arayışına girmişlerdir.

Şekil 12'deki kombinasyon dahilinde *bilgi savaşı* ve *siber suçlar*; *siber savaş*, siber casusluk, *siber zorbalık* ve *siber terörizm* gibi unsurları karşımıza çıkarmıştır. Bilgi savaşı ve siber suçlar uluslararası alana ilişkin sorunsal bütünlüğü artırırken diğer yandan teknolojik gelişmelerin gelişmesinde/geliştirilmesinde dinamo görevi üstlenmektedir. Devletlerin savaş, casusuluk, terörizm gibi unsurların karşılanmasına ilişkin algıları, AR-GE faaliyetlerini siber alana kaydırmaktadır. Bu konuda devletlerin özel sektörle olan birlikteliği yapısal olarak çeşitli düzeylerde spekülasyonları da beraberinde getirmektedir.

Şekil 12: Geleneksel Bilgi Savaşı ve Siber Suç Kombinasyonu Olarak Siber Savaş[45]



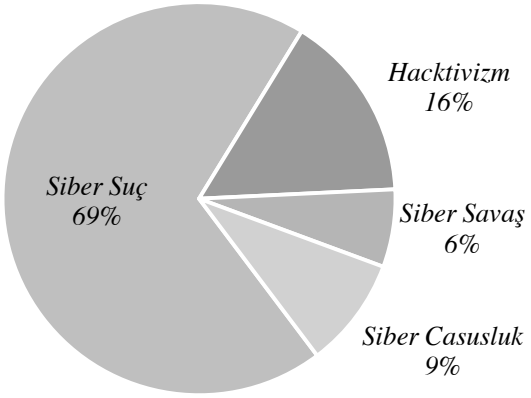
Kaynak: Merrick ve diğerleri, 2016: 5

Bilgi savaşı ve siber suçlara yapılan atıfların yanında küresel olarak siber savaşın gelişimine ilişkin bazı yaklaşımlarda siber suçlar direkt olarak adres gösterilmektedir. Carr (2012: 5) *"Inside Cyber Warfare"* adlı çalışmasında sorunun askeri bir problem olduğunu ve derlediği diğer çalışmalara ilişkin, hukuksal bazı zorlayıcı unsurlarla siber savaşın bir kombinasyon içerisinde değerlendirilmesi gerektiğini vurgulamaktadır. Siber suçlar yazılımsal olarak bazı zararlı unsurların hareketliliği ile geliştmekte, siber savaş ise test edilebilen unsurlarla evrimini sürdürmektedir.

Her ne kadar siber savaşa ilişkin gerçeklik ve gelişen olaylar yukarıda belirtilen tespitlere ilişkin süregelse de, özellikle siber suçlara ilişkin ve iç hukuktan dolayı sonuç doğurabilecek gelişmeler siber savaş algısının önünde gözükmektedir (Rawnsley, 2008: 83). Grafik 5'te görüleceği üzere, siber savaşın sahip olduğu motivasyon düzeyi saldırıların kaynaklandırılış şekline göre oldukça düşük bir yüzdeye sahiptir. Siber savaşın motivasyon düzeyinde düşük olmasına rağmen etki alanının belirginliği ve genişliği diğer unsurlara göre değişkenlik göstermektedir. Özellikle bireysel olarak, çoğu zaman maddi kazançların sağlanması siber suçları oldukça öne taşımaktadır.

[45] Yılmaz (2006: 615) bilgi savaşını; *"karşı tarafa ait, bilgi tabanlı işlemcileri, bilgi sistemlerini, bilgisayar tabanlı network sistemlerini etkileyecek bir hareket gerçekleştirmek ve kendi sistemlerini korumak"* şeklinde tanımlamıştır. Bilgi savaşı; askeri bir boyutu olmasıyla beraber daha çok bilgi sistemlerini çökertmeye yönelik, internet savaşlarını tanımlayan bir üst kavramdır.

Graifk 5: Saldırıların Motivasyonu[46]



Kaynak: Passeri, 2016

Siber savaş amaçlanılan unsur ve kapsamına göre stratejik ve operasyonel olmak üzere ikiye ayrılmaktadır. Stratejik siber savaşlar amaçlarına, olanaklarına, sınırlarına ve yürütülme şekline göre operasyonel siber savaşlardan daha geniş bir alanda kendini göstermektedir.

1.2.5.2.1. Stratejik Siber Savaş

Libicki (2009: 117) stratejik siber savaşı bir devlet veya onun toplumuna karşı yürütülen fakat birincil amaç olarak devletin davranışını etkilemeyecek bir siber saldırı bütünü olarak tanımlamıştır. Saldıran birim devlet veya devlet dışı bir aktör olabilmektedir. Özellikle devlet dışı aktörler açısından, saldırılan itibariyle karşılık bulma ve tepki daha güç ve karmaşık bir hal almaktadır. Devletler ise saldırılan ülke açısından diplomatik ve ekonomik birtakım yaptırımlarla karşılaşabilir.

Devletler stratejik siber savaşlarda provokasyon ve tırmandırma şekilleriyle farklı yollardan taktiksel unsurları benimseyebilir. Saldırılan aktör ise karşılıklı tırmandırma yoluyla çatışmanın boyutunu farklılaştırabilir. Bu durumda siber savaşın sınırlarının ne

[46] *Hackmageddon; Information Security Timeline and Statistics*'ten alınan verilere göre aylık olarak dalgalanmalar belirgin şekilde, dört unsur dahilinde değişmektedir. Veriler Haziran 2016 dönemine aittir. Mayıs 2016'ya göre siber suçlar %66.7'den az bir artışla, %69'a; hacktivizm %20'den düşerek %16 değerinde ifade edilmiştir.

olduğu konusu gündeme gelmektedir. Her ne kadar nükleer tırmanmada pratik bir husus olan ikinci vuruş yeteneği tartışılsa da, siber savaşlarda da ikinci vuruş yeteneği olarak saldırı metotlarının ele alınması yakın gelecek için önemli bir husustur. Her iki taraf açısından, yönetimsel olarak diplomatik tercihlerin mi kullanılacağı ya da kriz yönetimi kapsamında mı adımlar atılacağı farklı tercihler olarak da masa üzerinde yer alacaktır.

Rusya'nın 2007 Estonya ve 2015 yılı Ukrayna'ya karşı yürütmüş olduğu müdaheleler stratejik siber savaşa tipik örnekler olarak karşımıza çıkmaktadır. Stratejik siber savaşlar açısından devlet içi sistemin aksatılması ve toplumsal olarak psikolojik harekata örnek oluşturabilecek bu türden olaylarda kısa dönem ve uzun dönemde devlet altyapılarında hasarların onarılması, nükleer ve konvansiyonel unsurların bıraktığı yıkıcı etkilere göre daha kolaydır.

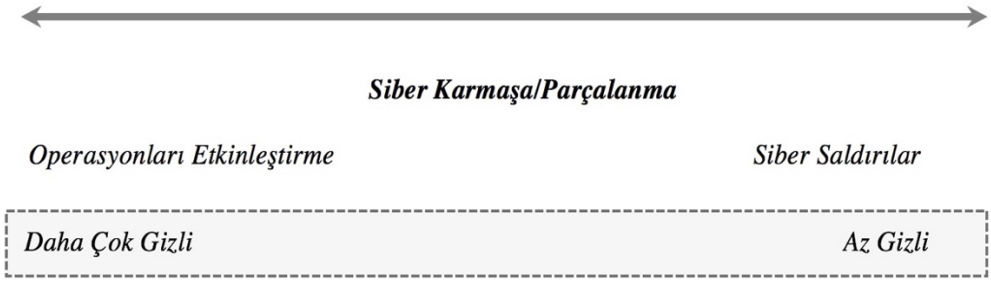
1.2.5.2.2. Operasyonel Siber Savaş

Libicki (2009: 139) operasyonel siber savaşı, askeri hedeflere ve askeri bağlantılı sivil hedeflere savaş zamanı yürütülen siber saldırılar olarak tanımlamıştır. Profesyonel bir müdaheleyi içeren saldırılarda, dikkatli ve eksiksiz bir şekilde, zamanında uygulanan güç unsurları olmalıdır.

Operasyonel siber savaş düzleminde eş zamanlı müdahele çeşitleri olduğu için operasyonların etkinleştirilme safhaları gizlilik bütünlüğü dahilindedir. Şekil 13, siber çatışma spektrumunda görüldüğü üzere *"siber saldırı"* olarak ele aldığımız kavram boyutsal ve niteliksel olarak daha düşük seviyeler taşıyabileceği için gizlilik konusunda çoğu zaman plan ve program içermeyebilir. Operasyonel siber savaşı da bu bu bağlamda adeta bir askeri çıkarma ya da bir gece yarısı askeri operasyonu gibi algılayabiliriz.

Siber çatışma spektrumu, aynı zamanda operasyonel boyut içindeki gizliliğin, siber saldırıların yönüne göre daha da gizlilik içerdiğini bizlere sunmaktadır. Siber alanda çatışmanın yaşandığı boyut, savaşın niteliğine göre değişkenlik göstermektedir. Askeri olarak konvansiyonel içerikli müdahelelerde benzer bir gizliliğin olduğu gözlerden kaçırılmamalıdır. Siber müdaheleler artık benzer bir organizasyonel altyapı gerektirmektedir.

Şekil 13: Siber Çatışma Spektrumu



Kaynak: Brown ve Tullos, 2012

Operasyonel siber savaşlarda müstakil bir savaş kombinasyonu yoktur ve tekil bir amaç dahilinde karakteristik özellikler mevcut değildir. Bir konvansiyonel savaşta, müdahele ya da askeri bir amaç güdülecekse fonksiyonel olarak siber unsurlarla destek gözetilmelidir. İlerleyen bölümlerde ele alınacak Körfez Savaşı ve 2008 yılında Güney Osetya Savaşı esnasında Rusya'nın Gürcistan'a yürütttüğü eş zamanlı siber müdaheleler operasyonel siber savaşların tipik örnekleri arasındadır.

1.2.5.3. Hibrit Savaş

Elektronik savaşın tekniklerinden daha fazlasına ihtiyaç duyulan, geleneksel savaşla birlikte de sürdürülen bileşke savaş tarzına *"Hibrit savaş"* adı verilmektedir. Özellikle NATO, Soğuk Savaş sonrasındaki güvenlik ortamının belirsizliği nedeniyle ve örneklerden çıkarılan dersler ışığında geleneksel savaş imkanlarını bırakmadan yenilerine sahip olmayı düşünerek hibrit savaş yöntemini tercih etmiş ve bu konuda farklı raporlar ortaya koymuştur (Bıçakçı, 2012: 210). Çoğu uluslararası ilişkiler çalışmalarında hibrit savaş, operasyonel siber savaş yerine de kullanılmaktadır fakat hibrit savaş, siber savaş başlığı altında incelediğimiz operasyonel siber savaşa göre daha özel durumları ve müdahale biçimine de işaret etmektedir.

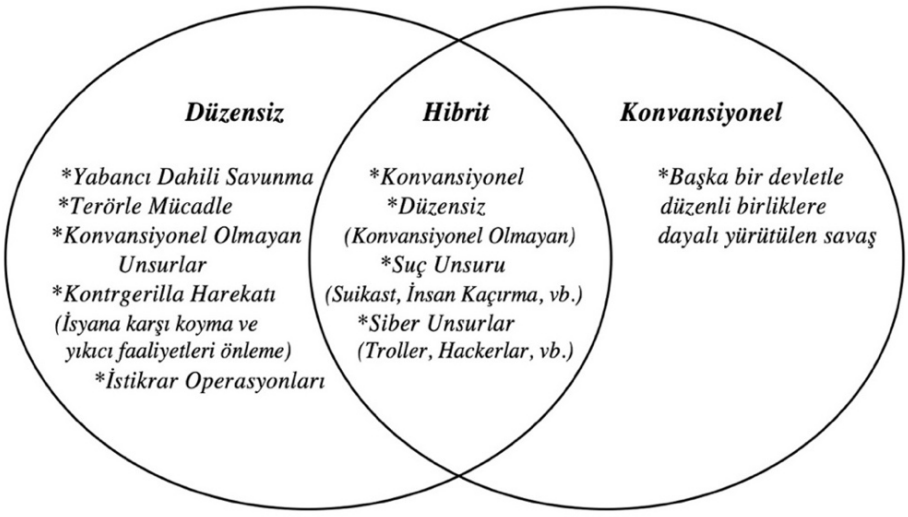
Savaşın evrimi ve özellikle asimetrik olarak gelişen unsurlar, farklı devletler ve NATO gibi örgütler bazında bu konunun tartışıldığı boyutu ortaya çıkarmıştır. Karma savaş olarak da vurgulanan terimsel ifadelerde, konvansiyonel kuvvet ve harekat yöntemleri ile *bilgi harekatı, bilgi tabanlı (cyber) faaliyetler, gayrinizami harekat, kitle imha silahları* ve

suç örgütlerinin kullanımı gibi geleneksel dışı kuvvet ve yöntemlerin kullanıldığı bir muharebe stratejisi tanımlanmaktadır (Varlık, 2013: 125).[47]

Hibrit savaş mantığına göre devletler kendilerini, kasıtlı bir tahrikten veya gerginliğin artmasından sonra bir siber savaş içinde bulabilmektedirler. Bir devlet, diğerine karşı kendini avantajlı duruma geçireceğine inandığı için siber saldırıda bulunabilir. Şekil 14'te düzensiz ve konvansiyonel unsurların bileşkesinde hibrit savaşın neleri kapsadığı sunulmuştur. Burada dikkat edilmesi gereken hibrit savaş içerisindeki unsurların gayri nizami nitelikler de taşıyabileceğidir. Suç unsuru oluşturabilecek ve siber unsurlarla birleştirilecek manevralarda amaç rakibi yıpratmaktır.

Hibrit savaş yaklaşımıyla yürütülen harekatlarda rakibin tamamen devre dışı bırakılması pratikte imkansız gözükmektedir. Bunun tek yolu rakibin tüm konvansiyonel unsurlarının siber ortama bağlı olması ve bir anda devre dışı bırakılabilme olasılığıdır. Hibrit savaşta asıl hedef, bir bölgeyi ele geçirmek veya kontrol etmek değildir.

Şekil 14: Hibrit Savaşın Temel Unsurları



Kaynak: Briefing to the Subcommittee on Terrorism, Unconventional Threats and Capabilities, Committee on Armed Services, House of Representatives, 2010: 16

[47] Askeri yazında "karma savaş" terimi henüz yerleşmemiştir. Bunun yerine, İngilizcede karma ya da melez anlamına gelen "hybrid" sözcüğünün okunuşundan "hibrit savaş" terimi Türkçeye aktarılmıştır.

Rakibi yıpratmaya yönelik ele aldığımız hibrit savaşta uzun süreli planlar yapılabilir ve zamana yayılabilir. Kısa sürede kesin sonuçlar beklemek hibrit savaşlar açısından gerçekçi durmamaktadır. Rusya'nın 2014 yılında Ukrayna'daki faaliyetleri yine Doğu Avrupa açısından Rusya'nın her fırsatta hibrit savaşı bir harekat biçimine dönüştürebileceği gerçeğini ortaya koymuştur. Karar alıcılar açısından yeni bir konseptin önlerinde olduğunu ortaya çıkaran benzer müdaheleler NATO gibi örgütlenmelerin de ajandalarında ilk sıralara yükselmiştir.[48]

1.3. Siber Güvenliğin Uluslararası İlişkilerde Etki Araçlarına Dönüşmesi

Siber güvenlik; kurum, kuruluş ve kullanıcıların varlıklarına ait güvenlik özelliklerinin siber ortamda bulunan güvenlik risklerine karşı koyabilecek şekilde oluşturulmasına ve idame ettirilmesine yönelik kendi içerisinde birtakım araçlara sahiptir. Bu araçlar karşısında değişen ve gelişen siber ortamda etki oluşturmak adına saldırı türleri çeşitlenmiş ve sonuç olarak siber politikalar üretilmeye başlanmış ve uluslarası ilişkiler içerisinde tüm bireylerin ve aktörlerin etkileşimde olduğu bir alan yükselişe geçmiştir.

Siber uzayın tartışıldığı ve konumlandığı alanda artık siber müdahele araçları olarak siber saldırı yöntemleri, siber silahlar geliştirilmiştir. Siber silahların kullanımına ilişkin verilerin toplanması, bunların politik boyuta taşınmasıyla birlikte siber istihbarat dediğimiz bir çalışma alanı oluşmuş ve bu alanda nitelikli personele ihtiyaç duyulmaya başlanmıştır. Siber saldırıların hazırlık ve savunma aşamalarına ilişkin ise devletler kimi zaman iş birliği içerisinde hareket ederken, kimi zaman da kendi öz imkanları ve kabiliyetleri doğrultusunda bu alanda etkili olmaya çalışmaktadır.

1.3.1. Genel Olarak Siber Silahlar

Siber saldırının hangi tür yazılım ve donanımlar ile gerçekleştirileceği konusunda, bir başka deyişle ne gibi zararlı bilişim unsurlarının siber saldırı silahı olarak nitelenebileceği hakkında literatürde kesin mutabakat sağlanmış değildir. Bunun bir nedeni, muhtemelen,

[48] Özellikle Rusya, hibrit savaş uygulamalarıyla ile birlikte, Soğuk Savaş sonrasında son 15 yılda gücünden söz ettiremezken yeniden atağa geçmiştir. Rusya'nın özellikle Estonya ve Ukrayna gibi ülkelerde açığa çıkan saldırıları ve faaliyetleri bölge ülkelerini de tedirgin etmeye başlamıştır.

bilişim alanındaki gelişmelerin olağanüstü hızı ve silah olarak sınıflandırılabilecek yazılım ve programların konvansiyonel silah sistemlerine göre resmi şekilde açıkça tasnif edilmemiş olmasıdır (Çelik, 2013: 141). Her ne kadar bu tasnif, nitelendirme olarak siber silah algısını geliştirmemiş olsa da uluslararası alandaki olayların seyrine etki eden bu türden araçlar alanın müdahele unsurları haline dönüşmüştür (Peterson, 2013: 121).

Siber silaha örnek olarak, zararlı yazılımlar; bakteri, solucan, virus, Truva atı, arka kapı ve sistemleri etkilemeye yönelik saldırılar; hizmet dışı bırakma saldırıları verilebilir. Başka programlarla ilişkili olup olmamasına bağlı olarak da gruplandırmalar yapılabilir. En temel siber silahları gelişmişliği ya da geçmişine bakılmaksızın şöyle gruplayabiliriz (Çifçi, 2013: 150):

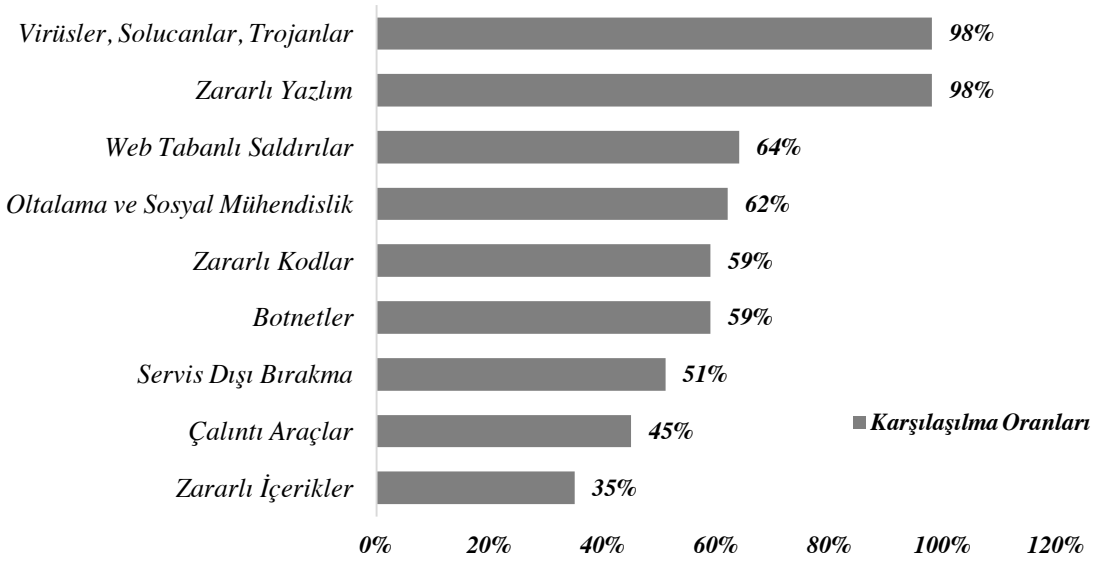
- *Bakteri: Bakteri, bağımsız, kendi kendine çoğalabilen, bir bilgisayarda birçok versiyonlarını kendi kendine yaratabilen bir programdır; çoğalan versiyonlarını çalıştırırken, daha fazla disk alanı ve işletim zamanı işgal ederler.*
- *Solucan (Worm): Kurt da denmektedir ve bağımsız, kendi kendine çoğalabilen, ağda bir bilgisayardan diğerine yayılma yollarını araştıran ve yayılan bir programdır. Saniyeler içinde milyonlarca bilgisayara ulaşabilir.*
- *Virüs: Başka programlara bağımlı, kendi kendine çoğalabilen, yerleşebileceği bir programa ihtiyaç duyan bir programdır. İçine gizlendiği program çalıştırıldığı anda veya sistemde istenen herhangi bir işlemin yapılmasından sonra başka programlara bulaşır.*
- *Truva Atı (Trojan horse): Normalde yararlı bir program gibi gözüken, ancak gizli bir şekilde, yerleştiği bilgisayara zarar vermeye yönelik olarak kullanılan programlardır. Truva atı, genelde kötü niyetli fonksiyonu harekete geçirmek için duruma bağlı bir test içerir.*
- *Mantık Bombası (Logic Bomb): Belirli bir zamanda veya belirli bir durum oluştuğunda çalışan programlardır. Mantık bombası, bilgisayarda gizli bir şekilde çalışacağı günü bekleyebilir veya kullanılan bir programda, zamanı geldiğinde zararlı işlemleri yapacak şekilde ayarlanabilir.*
- *Arka Kapı (Backdoor, Trapdoor): Tuzak kapı olarak da bilinmektedir. Sadece saldırgan tarafından bilinen, normal kimlik kontrol mekanizmalarını kullanmadan*

karşıdaki sisteme gizli bir kanalla ulaşmayı sağlayan yöntem veya giriş noktasına verilen isimdir.

- *Köle Bilgisayarlar (Botnet, Zombie): Bilgisayarlar, yüklenen bir program vasıtasıyla uzaktan kontrol edilebilmektedirler. Kullanıcı, bilgisayarına gizlice yüklenen ve saldırganın hedef sistemi, internet bağlantısı üzerinden uzaktan kontrol edilmesine imkan sağlayan programlar aracılığıyla köle bilgisayarlar kontrol edilir.*
- *Kök Kullanıcı Takımı (Rootkit): Bilgisayarda çalışan işlemleri, dosyaları veya sistem bilgilerini işletim sisteminden gizlemek suretiyle varlığını gizlice sürdüren zararlı programlara verilen isimdir. Genellikle işletim sisteminde çekirdek düzeyinde (kernel level) çalıştıkları için, tespit etmek ve kurtulmak çok zordur.*
- *Tuş Dinleyiciler (Keylogger): Temel olarak klavyede basılan tuşları, sürekli olarak kayıt etmekte ve bunları belli bir metin dizisi haline getirerek, ağ üzerinden saldırgana iletmektedir. Tuş dinleyiciler özellikle siber istihbaratçılar tarafından kullanılmaktadır.*
- *Script: Scriptler, web sayfalarında çalışan kod topluluklarıdır. Bot desteği ile scriptler kullanılarak toplu saldırılar gerçekleştirmek mümkündür.*
- *Sahte web sitesi: İnternette popüler web sitelerinin birebir kopyalarının yapılması ve benzer adlarıyla yayınlanan web siteleridir. Sahte web sitelerindeki hareketler izlenerek kişisel verilere ulaşılabilmektedir.*
- *Taklit e-posta hesabı: Taklit hesaplarla istihbarat çalışmaları yapılabilmektedir.*

Siber silahların kullanımında amaç ve hedeflenilen bir yer genelde mevcuttur. İstisnasını özellikle virüs, solucan ve trojan gibi zararlı yazılımların yayıldığı türler bozsa da bazı çalışmalarda karşılaşılma sıklıkları ile ilgili veriler de mevcuttur. Grafik 6'da siber saldırı türlerinin karşılaşılma sıklığına ilişkin oranlar verilmiştir. Karşılaşılma sıklığı açısından karakteristik olarak en yüksek oranlara sahip olan virüs, solucanlar, trojanlar ve zararlı yazılımlar ön planda olsa da verdikleri zarar açısından diğer siber saldırı türleri spesifik olaylarda ön plana çıkabilmektedir. Bu spesifik olaylardaki maddi kayıplardan ve zararlardan bireyler, kar amacı güden unsurlar ve uluslararası aktörler etkilenebilmektedir. Devletlerin operasyonel unsurlarını oluştururken bu türden saldırı türlerinden hangilerine başvuracaklarına ilişkin bir tasnif bulunmamaktadır. Bu durum siber saldırılara ilişkin teorik çalışmalarda sorun oluşturmaktadır.

Grafik 6: Siber Saldırı Türlerinin Karşılaşılma Sıklığı[49]



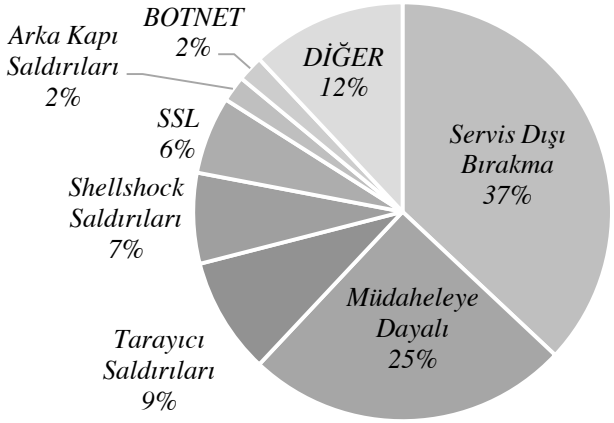
Kaynakça: Ponemon Institute, 2015a: 11

Farklı güvenlik firmalarının yaptığı tespitler siber ortamın, siber silahlar olarak adlandırdığımız unsurlardan farklı şekillerde etkilendiğini ortaya koymaktadır. Siber ortamda internet altyapısı ve ağı, bu unsurlardan farklı oranlarda etkilenmektedir. Bu etkilenme oranlarının dağıldığı yönün, kurumların, uluslararası aktörlerin tek tek belirlenmesi ise imkansıza yakındır.

Grafik 7'de ise 2015 yılı genelinde, en yüksek ağ saldırı türü olarak servis dışı bırakma saldırıları ön planda gözükmektedir. Daha önce vurguladığımız hususlar arasında birimlerin işleyişini bozmak ve yeri geldiğinde psikolojik bir harp stratejisi izleme adına tercih edilen servis dışı bırakmada maddi kayıplar da doğabilmektedir. Devlet kurumlarının çevrimiçi erişim kanallarına yönelik tercih edilen servis dışı bırakma saldırılarında ciddi bir prestij kaybı da doğabilmektedir. Her ne kadar bu konuda önlemler alınsa da hangi kurumun, ne zaman ve ne şekilde bu türden bir saldırıya uğrayacağı kestirilmesi imkansız bir durumdur. Kritik kurumların bu konuda tedbirli olması yerinde olacaktır. Bu tür saldırıları örgütleyen devletler, genellikle kendilerine yönelik benzer saldırılara ilişkin daha az mağduriyet yaşamaktadır.

[49] Grafik 6 üzerindeki veriler, 252 şirket üzerinden ölçülerek elde edilmiştir. Dağılım olarak saldırı türlerinin sıklığı ve oranları bu şirketlerlerden elde edilen verilere dayandırılmıştır.

Grafik 7: En Yüksek Ağ Saldırı Türü Oranları



Kaynak: McAfee Labs Threats Report, 2015: 44

Siber silahlar açısından bugün ortaya çıkan silahlanma yarışları Soğuk Savaşa dönemine benzerlikten uzaktır. Siber silahların gelişimi bakımından kıyaslandığında, özellikle siber silahların kullanımına ilişkin ilk adımlarda, ilk evreler benzer şekilde tehlikelidir. Siber silahlara ilişkin herhangi bir yarışta büyük stratejik üstünlükler kısa süreli olabilmektedir. Bunun en önemli sebeplerinden biri karşı tarafın kullanacağı siber silahlara ilişkin manevraların beklenmedik bir şekilde gerçekleşmesidir (Singer ve Friedman, 2015: 218).

1.3.2. Siber İstihbarat ve Siber Casusluk

İstihbarat günün şartlarına uygun olarak gelişmektedir ve çeşitli sözlüklerde *"akıl, zeka, malumat, haber, bilgi, havadis, bilgi toplama, haber alma"* şeklinde tanımlanmaktadır.[50] Teknolojinin gelişmesiyle ise sadece bilgisayarlar değil; telefonlar, tabletler, evdeki televizyonlar ve hatta buzdolabı gibi eşyalar dahi siber uzaya bağlı hale gelmiştir ve tüm bu dijital verilere ulaşmak amacıyla yapılan istihbarata *siber istihbarat* adı verilmektedir (Keleştemur, 2015: 74). Siber istihbaratın tanımsal özelliklerinde bu faaliyeti

[50] CIA resmi sitesindeki açıklamada istihbarat, basit ve ilginç bir şekilde; *"Ulusumuzun liderlerinin, ülkemizi güvende tutumak için duyduğu bilgi."* olarak tanımlanmıştır. Siber istihbarat ile elde edilen bilginin genişliği teknolojik gelişmelerle birlikte ciddi bir öneme sahip olmuştur.

kimin yürüttüğü ve neyi amaçladığı belirleyici olmaktadır ve kavramın kapsayıcılığını genişletmektedir. Uluslararası hukukun da dahil olduğu siber istihbarat faaliyetleri, BM Sözleşmesi'nin 2. Maddesi'ndeki egemenlik ve iç işlerine dair hususlarla birlikte tartışma konusudur (Ekstedt ve diğerleri, 2012: 157).

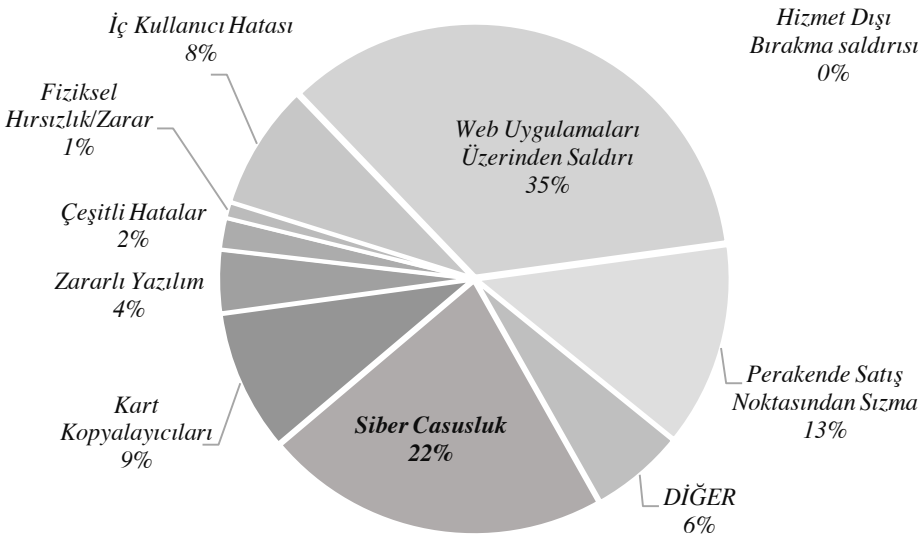
Dijital verilere ulaşılmasındaki nihai amaçlar siber savaş perspektifinde kişisel, ekonomik politik veya askeri avantaj sağlamak olarak özetlenebilir. İletişim ağları veya bilgisayarlara yasa dışı sızarak, şahıslardan, rakiplerden, gruplardan veya düşmanlardan onların haberi ve izni olmadan verisel avantaj sağlamak siber savaş alanındaki gelecek kurgusu haline gelmiştir.

İstihbaratçıların işini de sokaklardan masa başlarına ve bilgisayar ekranlarına taşıyan bu gelecek kurgusu olmuştur. Bilgisayarların istihbarat ve araştırma yapmalarını olanaklı kılan teknolojik gelişmeler, bunun baş döndürücü hızına ivme katmıştır. Günümüzde küresel iletişim ağlarından yararlanan gizli servisler, neredeyse istedikleri bütün kapalı veri bankalarına girerek gizli ve özel bilgilere ulaşabilmektedirler (Yılmaz ve Salcan, 2008: 18).[51] Birçok güvenlik lavoratuvarının yapmış olduğu testler ve analizlerde, saldırı merkezlerinin kesin tespitleri oldukça zordur. Modern terörizmin, yıkıcı etkiler bırakacak saldırıların yanında para, silah, bilgi ve doküman transferleriyle ilgilinerek verilere yönelmiş olması istihbaratın karakteristik niteliğini değişime uğratmıştır. Gerek 11 Eylül saldırıları esnasında, gerekse yükselişe geçtiği dönemde El-Kaide terör örgütünün internet, hackleme teknolojilerinde ciddi bir yol katetmesi dikkat çekicidir (Vellone, 2006: 119).

Siber istihbarat açısından uluslararası aktörlerin caydırılması amacıyla bir tercih önceliğine dönüşen, siber saldırılara ilişkin *siber casusluk* veri kaybının oluşumunda, Grafik 8'de de görüldüğü üzere önemli bir orana sahiptir. Siber casusuluk alanına ilişkin veriler, fiziksel birtakım unsurlara göre daha çok başvurulur olmuştur. Devletlerin nitelikli personel ihtiyacı ve bu konuda kurumsallaşmaya gidilmesi gibi hususlar, benzer örneklemlerle de çoğaltılabilir. Özellikle savunma kısmında ise devletlerin veya mağdurun eli oldukça zayıflamaktadır. Gelişen saldırı biçimleri ve anlık olarak güncellenebilen siber silahlar bu konudaki en büyük açığı oluşturmaktadır.

[51] Örneğin, elektronik istihbarat dünyasının en gizli ve en çok konuşulan sistemi Echelon, sinyal ve görüntü istihbaratı yapan bir ağ olarak; 100'ün üzerinde irili ufaklı uyduyu da kullanmakta ve yönlendirmektedir.

Grafik 8: Veri Kaybına Yol Açan Saldırıların Dağılımı



Kaynak: Başaran, 2014

Önceleri kişisel maksatlarla yapılan siber casusluk zamanla bireysel çerçevesinden çıkmış ve ekonomik, politik, askeri avantaj sağlamak amacıyla kullanılmaya başlanmıştır. Yasadışı faaliyet olarak yapılan siber casusluk, rakip ülkenin iletişim ağları veya bilgisayarlarına yasal olmayan yollarla sızarak grup ya da devlete ait gizli bilgilerin sızdırılması eylemi haline dönüşmeye başlamış ve uluslararası aktörler açısından, kurumlar ve birimlerin oluşturulmasını gerekli kılmıştır. Oluşturulan birimler, teknik içerikli önlemlerin yanında casusluk faaliyetlerine ilişkin bir uzmanlaşmayı da beraberinde getirmiştir.

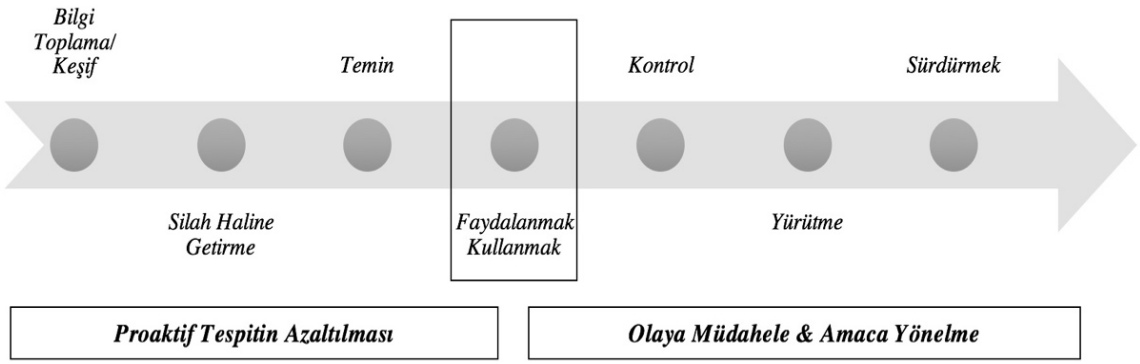
Farklı kurumlar ve birimlerin oluşturulmasıyla savaş zamanında casusluğa benzer biçimde, siber casusluk da farklı değerlendirmelere tabi tutulmuştur. Siber savaş alanında önemli çalışmalardan biri olan *Talin El Kitabı (Tallinn Manual)*, siber casusluğun insancıl hukuka aykırı olmadığını, siber casusların da savaş esiri statüsünü kaybedeceğini belirtmektedir. Uzaktan bilgi toplama operasyonu düşmanın kontrol ettiği bölgenin dışında gerçekleştirildiği için siber casusluk rejimi burada uygulanmayacaktır (Albayrak, 2015: 29). Siber istihbarata yönelik uluslararası uygulamalarda ve devletlerarası boyuttaki gelişmelerde hukuki düzenlemelere bu yüzden ihtiyaç vardır. Yapılacak düzenlemelerin uygulanabilirliği konusunda tartışmalar, düzenlemelerin niteliğinden daha çok tartışılmaktadır.

1.3.3. Siber Saldırılarda Hazırlık Aşaması

Siber saldırı, siber korsanlar tarafından yapılabileceği gibi, yetkili hükümet organları tarafından da gerçekleştirilebilmektedir. Dolayısıyla siber saldırılar gerek yasal anlamda gerekse teknik anlamda farklılıklar gösterebilmektedir. Siber saldırı, siber ortam üzerindeki yazılım, donanım ve altyapıları hedef almaktadır. Saldırılar amaçlarına, saldırı şekillerine, etkilerine göre farklılık içermektedir. Kimi saldırgan, ideolojik ya da tamamen kişisel tatmin amaçlı saldırılar düzenleyebilmektedir. Tüm bu saldırı tiplerine ve saldırgan karakterlerine göre bir analiz yapılmakta ve buna göre saldıran kişi ve grupların kimler olduğu tespit edilebilmektedir (Keleştemur, 2015: 267). Siber saldırıların hazırlık aşaması bu noktada genelde saldırıyı düzenleyecek birimin hedeflerine göre şekillendirilmektedir.

Siber saldırıların hazırlık aşaması, saldırı sürecinin aldığı yolu belirleyici en önemli unsurdur. Sürekliliğin kalitesi, bu süreçte hazırlık aşamasındaki ciddiyete bağlıdır. Şekil 15'te siber saldırının yaşam döngüsü gösterilmiştir. Siber saldırılardaki keşif, unsurların siber silah haline getirilmesi ve oluşturulabilmesi sürecin faydaya dönüşmesindeki ilk unsurlardır.

Şekil 15: Siber Saldırı Süreci/Yaşam Döngüsü (Lifecycle)



Kaynak: Barnum, 2014

Her grubun farklı bir saldırı becerisi bulunmaktadır. Uluslararası anlamda bireyler ya da devletlerin, kar amacı güden grupların bu konuda çevrimiçi halde devamlı olarak iletişimde olduğu bir gerçektir. Siber saldırıların ortaya çıkışında karşı tarafa zarar verilme

istemi haklı veya haksız olsun, iş birliği yapanlar açısından belli düzeyde samimiyet ve güvene de ihtiyaç duymaktadır. Bu yüzden saldırıların niteliğine ilişkin samimiyetin yanında elde edilecek kazanç, sürekliliği beraberinde getirebilmektedir.

Siber saldırıların ortaya çıkışında ve hazırlanışında, siber uzayın zayıf olanın güçlü üzerinde üstünlük kurabileceği gibi garip bir avantajı beraberinde getirdiği söylenebilir, fakat siber saldırı yeteneklerinin geliştirilmesine yönelik engeller oldukça düşüktür. Örneğin; insansız uçak sistemi ABD'ye yaklaşık 45 milyon dolara ve kayıtlarının aktarıldığı uzay uydu şebekesi milyarlarca dolara mal olmuştur. Bu sistemleri çökertmek için *skygrabber* olarak bilinen bir program 25.95 dolara mal olmuştur. Diğer taraftan ABD gibi devletler için gerçek kaygı, diğerlerinin artık siber tehdit oluşturabilmeleri değil, geleneksel kuvvetlerin siber hassas noktalar oluşturmalarıdır (Singer ve Friedman, 2015: 205).

Siber saldırıların hazırlık aşamasında birimler ya da aktörler tekil hareket etmenin yanında ortak harekat kabiliyetine de sahiptir. Siber ortamın dünyanın heryerinden ulaşılabilirliği bu alana ilişkin saldırıların hazırlık boyutunu ve birimlerin birbilerine ulaşma alanını sınırsız hale getirmektedir. Keleştemur (2015), siber saldırı yapanları sahip oldukları kapasite açısından ayırtetmeksizin şöyle gruplandırmıştır:

- *Bilgisayar korsanları*
- *Siber teröristler*
- *Organize suç örgütleri*
- *Endüstri casusları*
- *İstihbarat mensupları*
- *Kurum içindeki casuslar*
- *Yabancı ülkeler*

1.3.4. Siber Savunma ve Tehditler

Bir tehdit ile başa çıkabilmenin birinci şartı onu doğru tanımlayabilmekten geçmektedir. Herhangi bir siber tehdidi tanımlayabilmek için öncelikle saldırıyı kimin yaptığını ve nasıl bir saldırı olduğunu belirlemek gerekmektedir. Siber tehditler, bilişim teknolojisi kullanılarak bir toplumun iç ve dış düzenini muhafaza etme refleksini zayıflatmak

veya tamamen yok etmek amacıyla kullanılmaktadır. Dünyanın herhangi bir yerinden başka bir bölgeye yönlendirilen saldırı, küreselleşme sonucunda sınırların ortadan kalkması olgusunu pekiştirmektedir (Altunok ve Kaya, 2009: 138). Verilerin toplamda her yönüyle birbirine bağlı olduğu siber ortam bu sınırları boyutsuzlaştırmıştır. Siber politikalarda temel dikotomi "saldırı" ve "savunma" ikisilinde, siber saldırı ve siber savunmaya ilişkin politikaların oluşturulması hususunda tartışılmaktadır (Klimburg ve Healey, 2012: 74).

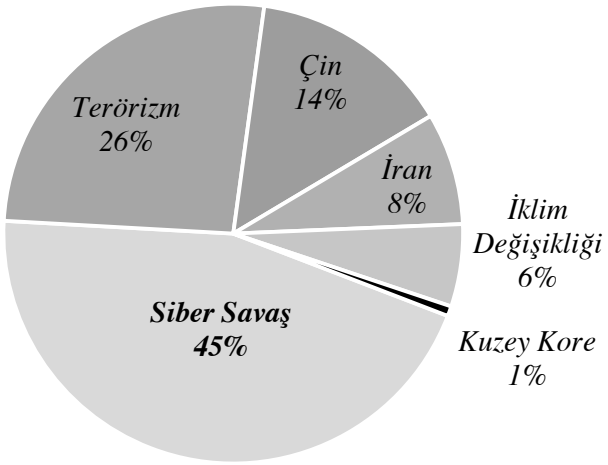
Siber savunmaya ilişkin genel sorun problemin boyutlarının doğru olarak tespit edilmemesiyle ilişkilidir. Diğer savunma boyutlarına ve suçlarına karşın köklü bir geçmişi olmayan siber alanda işlenen suçlar ve saldırılara ilişkin kesin istatistiklere ulaşmak mümkün değildir. Bu boyutun doğru tanımlanamayışı, tespitinin güçlüğü de savunma oluşturulmasında gereken önemin oluşmasında engelleyici bir durum oluşturmaktadır.

Siber ortamın merkezi ve sınırları olmayan ağ biçimindeki yapısı, onun herhangi bir devletin veya herhangi bir hukuk düzeninin altında yer almasına engel olmaktadır. Siber ortamda hakimiyetin kimlerin elinde olacağı veya egemenlik yetkisinin sınırlarının nasıl çizilebileceği sorusu karışık ve yanıtlanması zorunlu bir soru olarak karşımıza çıkmaktadır.

Siber ortam, ulusal güvenlik ve siyasi iktidarların askeri saldırıları için bir ortam olarak da kullanılabilmektedir. Siber ortam teröristler açısından propaganda aracı olarak da kullanılabilmektedir. Tüm bu unsurlar içerisinde savunmaya yönelik karşı hareketler zorunlu hale gelmektedir (Avcı ve Altunok, 2009: 215). Harekatın boyutları ele alınırken kaçırılmaması gereken nokta, ön savunmanın oluşturulması gerekliliğidir. Siber saldırılara ve tehditlere karşı ön savunmanın teknik zemini, kesin ve net bir çerçeve ile oluşturulamasa da olası saldırı türlerine karşı tedbirler her zaman mümkün gözükmektedir.

Tehdit olarak algılanan siber saldırılar birçok toplum için diğer tehdit algılarının da önüne geçmiştir. Grafik 9'da görüldüğü üzere siber savaş tehdidi ABD toplumu için terörizm, Çin, İran gibi unsurların da önündedir ve savunma sistemi oluşturulması açısından bu algının yönlendirilmesi önemli bir göstergedir. ABD'de çoğu zaman ciddi sıkıntılara yol açan iklimsel sorunlar dahi siber savaş tehdidi yanında tehlike boyutu açısından daha az bir algı düzeyi oranına sahiptir.

Grafik 9: ABD'nin Çıkarları Açısından Hangisi Daha Tehlikeli?[52]



Kaynak: Pizzi, 2014

Farklı tehditler ve siber savunma açısından diğer bir tehdit gelişimi ise siber uzaya artan bağımlılık ve hem devletlerin, hem de bireylerin bu konudaki bilinçsiz davranışlarıdır. Karar alıcılar açısından iyi oluşturulmamış kurumsal bir yapı ciddi bir sorunsala dönüşmektedir ve tehdit oluşturmaktadır. Verilerin korunmasına ilişkin alınabilecek tedbirlerde prosedürel bir yaklaşım yoktur, fakat özellikle fiziksel çevrenin temel unsurları haline gelen iletişim ağları ve bunlara bağlı cihazların etkinliği her geçen gün artmaktadır. *"Siber alana artan bağımlılık düzeyi"* olarak da adlandırabileceğimiz bu durum devletlerin korkulu rüyası haline gelmektedir. Siber alandaki altyapının anlık değişimler göstermesi bu durumun oluşmasında temel neden olarak dikkat çekicidir. Artan bağımlılık düzeyi kısa ve uzun vadede geri çekilememektedir.

Siber savunma açısından fiziksel çevrenin temel unsurları haline gelen iletişim ağlarında birçok kurumun, devletler bünyesinde hazırlıksız olduğu da bilinen ve tartışılan bir gerçektir. Devletlerin uluslararası alanda kimi zaman politika oluşturulmasına dair verileri, siber savunma kültürlerinin olmayışı ve siber tehditlerin ikinci plana atılmasından dolayı istenmeyen kişilerin eline geçmektedir. İletişim ağlarına bağımlılığı artan tüm devletler ve kurumlar ise bu durumla daha çok karşı karşıya kalmaktadır.

[52] Toplam 293 katılımcının yer aldığı araştırmada *Siber Savaş* ilk sırada yer almıştır. Kendisini *"Demokrat"* olarak tanımlayanlar *İklim Değişikliği* tehdidini ikinci sıraya koyarken herhangi bir siyasi yaklaşımdan bağımsız düşünenler *Terörizmi* seçmiştir. *"Cumhuriyetçiler", Terörizm* ve *Siber Savaşı* eşit tehditler olarak görmüşlerdir.

1.4. Uluslararası Aktörler ve Siber Mücadeledeki Yerleri

Uluslararası politikada aktörler veya temel aktör olma sorunu küreselleşen dünyada belirginsizliğini daha çok hissettirmeye başlamıştır. Uluslararası politika adına analiz düzeyi ve teorik sorunlar da eklenince yeni ve eklektik bir düzeyi alana katan siber politikalar, aktörler arasındaki uyum ve anlayış sorununu da beraberinde getirmiştir.

Siber güvenlik alanında politika oluşturma ve bu politikalar üzerinden etkileşime dair uluslararası aktörlerin kesin bir şekilde sıralanması yakın gelecek açısından oldukça zor gözükmektedir. Bireylerin siber ortamdaki müdaheleleri ve etkinlikleri dahi herhangi bir devlet içerisinde ciddi karışıklığa sebep olacakken kesin bir sınıflandıma yapmak algı sorununu beraberinde getirecektir.

Uluslararası politikada devletlerin aktör olarak vasıfları ve temel aktör olduğu yönündeki görüşler halen hakimken, hükümetleri temsil etmeyen uluslararası nitelikli aktörleri devletlerle eşit şekilde inceleyen uzmanlar da bir hayli fazladır. Devletlerin kendi içerisinde oluşturdukları siber ordular ve uzmanlaşmış personeller siber güvenliğe ilişkin yeni aktörlerdir ve adeta devletler için vazgeçilmez unsurların başında gelecektir. Uluslararası alandaki yapılanmalar ise daha çok illegal gruplanmalara kaymıştır ve çıkarsal anlamda iş birlikleri oluşmuştur.

1.4.1. Devletler

Aktör kavramı uluslararası politika alanına davranışçı yaklaşım terminolojisi çerçevesinde girmiştir. Devletlerin aktör olarak tartışıldığı boyut egemenlik ve dış politika çıktılarına ilişkindir. Uluslararası boyutta var olan resmi tüm adımlarla gerçekliğini koruyan devletin siber uzayda temel aktör olup olmadığı uluslararası politikaya nispeten tartışmalı bir husustur.

Günümüzde savaş teknolojisindeki gelişmeler ve siber uzaya artan bağımlılık, ülkesel devletin siyasal sınırlarının geçit vermezliğini ve bu sınırlar içerisinde söz konusu

olan mutlak egemenlik olgusunu aşındıran sonuçlar doğurmuştur.[53] Gelişmişlik düzeylerine göre devletlerin kendi aralarındaki karşılıklı bağımlılık olgusu, ulusal devletin klasik özellikleri üzerinde bazı önemli değişiklikler meydana getirmiştir (Sönmezoğlu, 2000: 34).

Bu değişiklikler içinde özellikle siber ortamın, kendi yapısal özellikleriyle birlikte devletlere zarar vermesi belirleyici olan kıstastır. Karşılıklı bağımlılık, egemenlik haklarına müdahele eden saldırgan bir boyuta ulaşmıştır. Siber uzayın nüfuz etme ve sanallaştırma karakteri, geleneksel olarak belirli bir arazinin kontrolünden türemiş olan devlet güçlerinin gerçek sınırlarının olduğu anlamına gelmeye başlamıştır.[54]

Karşılıklı bağımlılık ve egemenlik konsepti içinde ise devletlerin aktör olarak belirginleşmeye başladığı siber uzayda güç tam olarak hesaplanıp tahmin edilememektedir. Kimin daha güçlü olduğunun belirlenmesi adına ortaya çıkan savaşlar öncesinde taraflar kendini güçlü görüp, baskın olacağını hissettiği için girişimlerde bulunmaktadır. Devletler siber güvenlik ortamında, yine siber savaşlar bağlamında benzer bir düşünceyle hareket etmektedirler (Roskin ve Berry, 2014: 29).[55] Devletler, siber ortamda karşılığın nasıl ve ne şekilde olacağını kestiremedikleri için kapasite hesaplaması ve rakibi tanıma gibi unsurları masaya koyamamaktadır.

Daha önce değindiğimiz siber savaş konsepti içinde günümüz için devletlerin temel aktör olduğu ya da baskın bir tarzda savaş etkileşimi içerisinde olduğunu söylememiz çok güçtür. Bunun en önemli sebebi sorunların çözümünde devletler arasında ciddi bir gelişmişlik farkı ve güven eksikliği yer almaktadır. Özünde çatışmalı olan uluslararası

[53] Egemenlik kavramı zamanla iç hukukta söz konusu olduğu biçimde, uluslararası hukuk ve uluslararası siyaset alanına nakledilince, birçok devletin bulunduğu uluslararası sistem gerçek bir arenaya dönüşmüştür ve rekabet ortaya çıkmıştır. 20. yüzyılda uluslararası hukukta ortaya çıkan yeni tabii hukukçuluk, realist doktrin, normcu görüş gibi eğilimleri temsil eden birçok ünlü hukukçu, egemenliğin bu şekilde yorumlanmaya ve uygulanmaya çalışılmasına karşı çıkmışlardır.

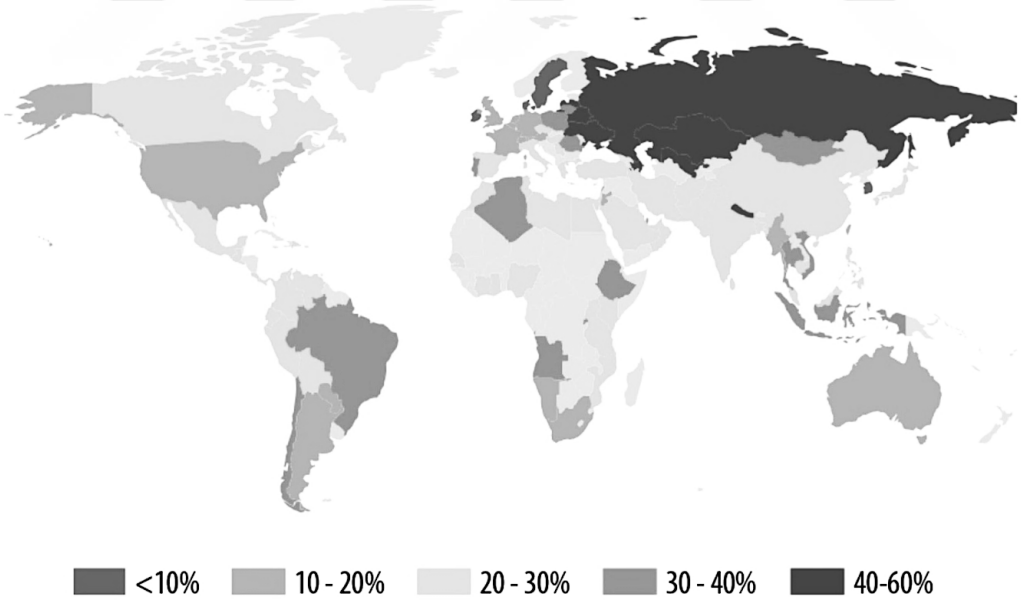
[54] Örneğin, korsan platformlar vasıtasıyla veri transferini olanaklı kılan birçok web sitesi mevcuttur. Dünya çapında birçok verinin birbirleri arasındaki bağlarla paylaşılması, devletlerin bunun karşısında etkisiz kalması ve müdaheleci olamayışı fiziki ve sanal sorunları oluşturmaya başlamıştır. Hiçbir devlet uluslararası alanda kendi sınırlarında faaliyet gösteren bu tarz yapılanmalara el koyamamıştır.

[55] Bu duruma örnek olarak ABD ve yönetiminin savaşlara ilişkin yaklaşımında güçlü bir orduya güvendiği tezi gösterilebilir. Askeri gücün sadece bir faktör olduğu gözlerden kaçırılmamalıdır. Güçlü ordulara sahip olmalarına rağmen İngiltere, Rusya ve ABD Afganistan'da tam bir hakimiyet kuramamışlardır. Siber güç açısından durum farklıdır ve daha da karmaşıktır.

sistem, geçmişi bilinmeyen ve geleceği tahmin edilemeyen bir ortamda daha da şüpheci hale gelmektedir.

Devletler kendi aralarında olmasa da, farklı aktörlerin devreye girmesiyle siber ortamdan etkilenmekte ve bu düzey siber ortama bağlılık düzeyine göre farklılık göstermektedir (Klimburg ve Healey, 2012: 68). Şekil 16'da devletlerin web tabanlı saldırılardan etkilenme dağılımı verilmiştir. Uluslararası ilişkiler açısından sınırları belirli olan devletler etkilenme açısından coğrafi, kültürel, sosyal unsurlara bakılmaksızın ciddi bir farklılığa sahiptir. Bu saldırılardan etkilenme oranlarının birbirleri arasındaki çatışma kültürüyle doğrudan alakalı olmadığı dağılımın yüzdeleriyle de açıkça ortaya çıkmaktadır. Rusya ve çevresindeki devletlere ait oranların yüksek olmasında bankalara saldırılar, devlet kurumlarına ait verilere ulaşılmaya çalışılması, illegal faaliyetlerin siber ortamda yoğunlaşması gibi unsurlar belirleyici olmuştur.

Şekil 16: Web Tabanlı Saldırılarda Devletlerin Küresel Etkilenme Oranları[56]

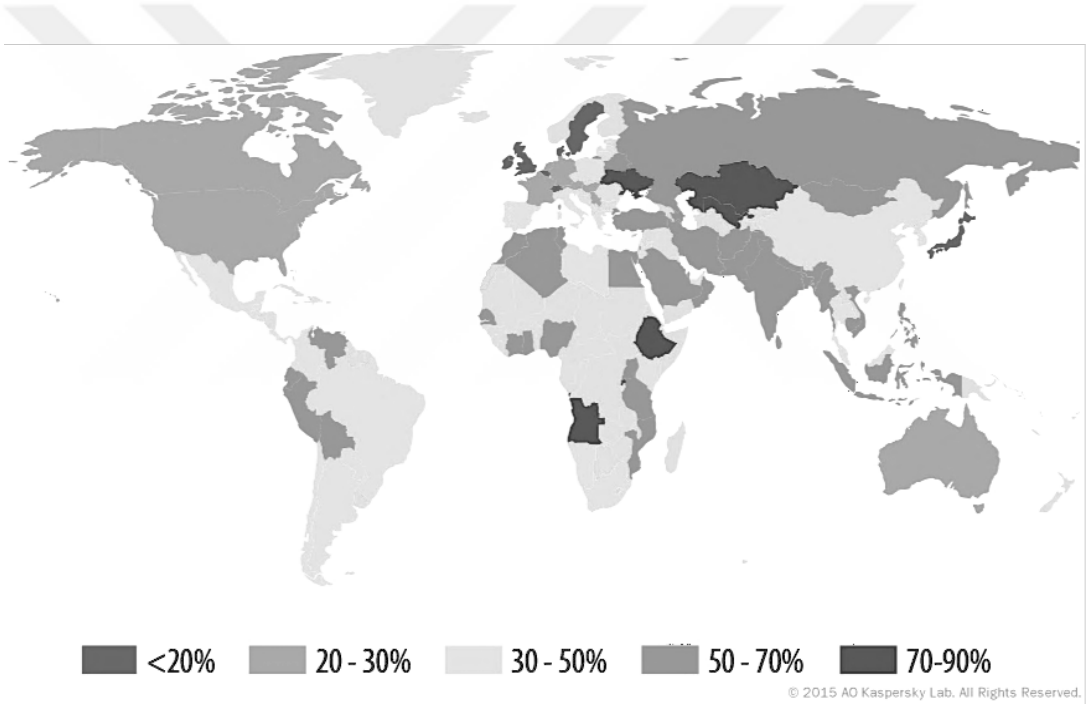


Kaynak: Kaspersky Security Bulletin, 2015: 31

[56] Kaspersky Laboratuvarlarının ölçümlerine göre 2015 içinde her üç bilgisayardan (%29) biri, bir veya daha fazla web tabanlı saldırıya uğramıştır. Genel olarak yüksek oranlara sahip zararlı programlar rapor içerisinde ayrıca belirtilmiştir.

Uluslararası alanda güç ilişkisinin herşeyiyle etkili olmadığı siber ortam sadece dış dinamiklerin etkisiyle devletler üzerinde baskı oluşturmamaktadır. Küresel bir aktör olarak devletin sınırları içerisinde olan ve dolaşan siber tehditler farklı fiziki araçlarla da etkinliğini arttırabilmektedir. Şekil 17'de yerel siber tehditlerin küresel dağılımı devletlere göre oransal olarak verilmiştir. Web tabanlı saldırılara göre yerel siber tehditler etkinlik açısından daha dengeli durmaktadır. Bunun en temel sebebi fiziksel olarak devletlerin bağlı olduğu teknolojik araçlar ve altyapı her geçen gün etkinliğini arttırmaktadır ve bu araçların varlığı kimi zaman bir caydırıcılık dahi oluşturmaktadır.

Şekil 17: Yerel Siber Tehditlerin Küresel Dağılımı[57]



Kaynak: Kaspersky Security Bulletin, 2015: 32

Farklı güvenlik şirketlerinin yaptığı araştırmalar devletlerin küresel bir aktör olarak, siber güvenlik konsepti içinde maruz kaldıkları etkinin güç ilişkisiyle bağlantılı olmadığını gözler önüne sermektedir. Özel olarak belirli hedeflere yönelmiş devletler veya diğer

[57] Kaspersky tarafından test edilen tehditler her ülkenin kurumsal kullanıcılarının yüzdeleriyle elde edilmiştir. *Antivirüs tespit dosyası*, kurumsal bilgisayar kullanıcılarının %41'inden etkilenmiştir. Tespit edilen unsurlar bilgisayarların yanında, *flaş bellekler, hafıza kartları, telefonlar, harici diskler* ve *network araçları* üzerinde konumlanmıştır. Genel olarak yüksek oranlara sahip zararlı programlar ve virüsler rapor içerisinde ayrıca belirtilmiştir.

aktörler, amaçladıkları sonuçlar ve etki açısından farklılık göstermektedir. Son yıllarda artan siber suçlar ve saldırılar, siber güvenlik adına en önemli aktörlerden biri haline gelen devletleri uluslararası politika açısından ön plana çıkarsa da, temel olarak belirli sınıflandırmalardan kaçınmak ve zayıf-güçsüz ayrımına gidilmemeyi gerektirmektedir.

Devletler bu güç mücadelesi içindeki farklılık dahilinde, siber mücadeleye ilişkin emir-komuta sistemleri kurmayı ve siber olayları, savaşı takip etme adına harp teknikleri geliştirmeye başlamıştır. Klasik ordu yapılanmalarından bazı temel özellikleriyle farklılaşan siber ordular en çok dikkat çekenler arasındadır.

1.4.1.1. Siber Ordular

"Siber Ordu", ülkeyi ya da kurumu siber dünyadan gelebilecek tehdit ve saldırılara karşı koruyacak ve gerektiğinde karşı siber saldırılar gerçekleştirebilecek yetenekteki bilgi güvenliği uzmanlarından oluşturulmaktadır. Siber ordunun mensupları hem saldırı hem de koruma yöntemlerini çok iyi bilmek zorundadırlar. Bu konuda önde gelen ülkelerde genelde iki tür siber ordu bulunmaktadır;[58]

- *Devlet eliyle yetiştirilen ve resmi olarak kullanılan birimler,*
- *Devlet tarafından desteklenen, gönüllülerden oluşup resmi olmayan birimler.*

Devletin kendi eliyle oluşturdukları ordular için de geçerli olan durum saldırı yapabilmek için çok pahalı ve karmaşık silah sistemlerine ihtiyaç duyulmamaktadır. Resmi olmayan gruplar olsun, devletlerin resmi siber orduları olsun bazen, bir adet bilgisayar ve basit bir yazılım dahi bir grup için, ordu için yeterli bir strateji aracı olabilmektedir. Orduların kapasitelerini de ölçmek bu yüzden bir o derece zorlaşmaktdır (Çifçi, 2013: 23). Siber alandaki değişimin anlık olarak nasıl takip edildiği ve ordu düzeyinde nasıl programa alındığı bu hususta belirleyici olmaktadır.

[58] İlk siber ordu yıllar önce ABD tarafından gizli olarak kurulmuştur. ABD savunma bakanlığı Pentagon siber uzayın kara, hava, deniz gibi yeni bir savaş alanı olduğunu doktrin olarak kabul etmektedir. ABD'de bu alandaki en önemli darboğazın bilgisayar güvenliği uzman sayısındaki yetersizlik olduğu vurgulanmaktadır. ABD, mevcut bir kaç bin civarında olan uzman sayısını 20-30 binlere yükseltmek için gerekli eğitim programlarını uygulamaya almıştır.

Özellikle siber orduların kapasitesi nasıl ve ne güçte olursa olsun, klasik anlamda savaş anlayışının ve orduların bilgi teknolojilerine bağımlı hale geldiği bir gerçektir. Komuta kontrol sistemleri, silah sistemleri, istihbarat, keşif ve gözetleme sistemleri, savaş sistemleri gibi sistemlerin tamamı elektronik ortamda ve iletişim altyapısı üzerinde çalışmaktadır (Al-Rawi, 2014: 421).

Geniş bir şekilde askeri kabiliyetlerin parçası olan sayısal ve elektronik ortamın korunması ve gerekli müdahelelerin yapılması adına atılacak adımlar devletler adına, nizami bir ordu oluşturulması açısından zorunluluk haline gelmiştir. Dünyada yüzden fazla askeri örgüt ve istihbarat birimi, çok sayıda birey, suç ve terör örgütü bilgi sistemlerinden veri çalmaya, bu bilgi sistemlerini çalışamaz hale getirme adına faaliyetlerini sürdürmektedir.[59]

Birçok devletin yine *"5. muharebe alanı"* olarak ilan edilen siber alanda güçlü olabilmek adına siber ordular yanında, caydırıcılık gücünü artırmak için özel sektörle de iş birliği halinde olduğu görülmektedir. Bu devletlerin başında ABD gelmektedir.[60] Siber orduları sadece nitelikli personel ile başbaşa bırakmama arzusu içinde olan ABD gibi ülkeler farklı çıkarsal konularda birleştikleri özel sektör güçleri ile ortak projelere imza atmaktadır ve ordularını takviye etmektedir. 2009 yılında ordu bünyesinde siber bir birim oluşturduğunu ilk olarak açıklayan NATO üyesi Almanya, 76 kişi ile başlayan çalışma ve iş birliğini, günümüzde 6 bin kişilik bir siber ordu kapasitesine eriştirmiştir (Çelik, 2015: 32).

Siber savunma kapasitesi ve yöntemi açısından bir tercih halinden çıkıp zorunluluk haline gelen siber ordulara ilişkin yapılanmalar ülkelerin gelişmişlik düzeyiyle ilgilidir fakat başarısı ve sahip olduğu güç bu düzeyi geçersiz kılmaktadır. Ülkelerin kapasiteleri ve sahip

[59] Halen dünyada en güçlü siber ordulara sahip ülkeler olarak ABD, Çin, Rusya, Kuzey Kore, İran ve İsrail öne çıkmaktadır. Bu ülkeler arasında bir siber savaşın olduğu da herkes tarafından kabul edilmektedir. Özellikle ABD ile Çin arasında süren, siber casusluğu da içinde barındıran bir siber savaşın uzunca bir zamandır sürmekte olduğu çeşitli olaylarla ispatlanmıştır. NATO'nun 50 yıllık stratejik savunma konsepti, 2010 sonrasında radikal bir değişime uğramıştır. 1960-2010 döneminde "*çift kutuplu, simetrik, kinetik, konvansiyonel ve nükleer savaş tehdit algılaması*" şeklinde özetlenebilecek olan savunma konsepti yerini, 2011-2020 dönemi için "*çok kutuplu, asimetrik, konvansiyonel, nükleer ve siber tehdit algılaması*"na dönüştürmüştür. Artık siber tehditler de savaş nedeni olarak kabul edilmektedir.

[60] Siber saldırılar sonucu ticari anlamda 400 milyar dolar zarara uğradığını iddia eden ve siber saldırıları terörizmden daha ciddi bir tehdit olarak niteleyen ABD, siber güvenlik alanında en dikkat çekici yatırımları yapan ülkelerin başında gelmektedir.

oldukları yapılanmalara ilişkin gelişim ve tarihi süreç, 2. bölüm içinde daha detaylı ele alınmıştır.

1.4.2. Devlet Dışı Uluslararası Aktörler

Uluslararası ilişkilerin tartışma alanına ilişkin devlet dışı aktörlerin siber güvenlikte nasıl ve ne şekilde yer edindiğine dair tespitler ve açıklamalar siber saldırıların ve gelişmelerin müdahil olabildiği alanla ilgilidir. Özellikle hükümetleri temsil etmeyen bireyler ve gruplar bu aktörler içinde belirleyici olandır ve inceleme konusudur. Hükümetlerin temsil edilmediği alana ilişkin ise özellikle uluslararası uzmanlık kuruluşları ve çok-uluslu şirketler uğradıkları mağduriyete illişkin gündemle söz konusudurlar.

Uluslararası politikanın analiz seviyesinde, birey/grup ve uluslararası kuruluşlar düzeyinde analiz yapabilmek için siber saldırılar sonucunda tarafların kazançları ve kayıplarına ilişkin elimizde kesin veriler olması gerekmektedir.[61] Uluslararası politika analizlerinde, genel geçerliliği konusunda herkesin üzerinde anlaştığı genel, hatta kısmi bir teorik yaklaşımdan bahsetmek zaten güç bir husustur. Diğer taraftan devletlerin kazanç sağlamaya çalıştığı siber müdahelelerde bu durum daha da güçleşecektir. Bu süreç, devlet dışı uluslararası aktörler olarak baskın bir şekilde illegal yapılanmaları ve manipülatif birimleri karşımıza çıkaracaktır.

1.4.2.1. Uluslararası İllegal Yapılanmalar

Aktör olarak illegal-yasadışı yapılanmaların varlığı ve uluslararası alandaki baskınlığı, devlet dışı gruplar olarak bir faaliyet alanı oluşturmuştur. Bilgisayar ve haberleşme teknolojileri alanında bilgi sahibi olan ve bu konularda aynı zamanda standardın üzerinde beceriye sahip olan yapılanmalar devletler ve kimi özel kuruluşlar ile iş birliği halinde uluslararası sistemin aktörleri haline gelmişlerdir (Broadhurst ve diğerleri, 2014: 3).

[61] Analiz düzeyi sorununun uluslararası politika disiplini içerisinde bir inceleme başlığı olarak yer alması, farklı yaklaşım ve çalışmalarla, dolaylı ve direk olarak kimi çalışmalarda açıklığa kavuşturulmaya çalışılmıştır. Kenneth Waltz, *"Man, The State and War: A Theoretical Analysis"* adlı çalışmasında savaşın sebeplerini, birey, devlet ve uluslararası sistem olmak üzere üç ayrı düzeyde analiz etmiştir. Özellikle birey ve devlet ilişkilendirilmesinde savaşın çehresinin değişimine ilişkin tespitler yakın dönemde birçok özel olaya ışık tutar niteliktedir (Bkz. Waltz, 1959).

Son dönemde yaşanan siyasi olaylarla birlikte farklı gruplar, gündemde sıkça adından söz ettirmeye başlamıştır. Son zamanlarda Anonymus gibi yapılanmaların faaliyetleri, Wikileaks ve Panama belgelerinin sızdırılmasına ilişkin olaylarda farklı grupların faaliyetleri, devletler ve bireylerle olan işbirlikleri ciddi yankı bulmuştur. Sıradan birine sorulduğu zaman bile akıllara gelebilecek RedHack ve Anonymus gibi grupların kendi içerisinde dahi kimi zaman bölünebildiği ve farklı olaylarla ilişkilendirdiği bilinmektedir.

Başta NATO olmak üzere, ABD gibi ülkelerin de uluslararası illegal yapılarla mücadele ve eylem planlarına ilişkin söylemler ve askeri açıdan atılan adımlar siber ortamda mücadele alanı oluşturan aktörler açısından önemli bir yere sahiptir. Uluslararası yapılanmaların faaliyet alanları ve kapasitesi bu önemi ve gerçekliği de gözler önüne sermektedir. Kimi zaman yerel, kimi zaman uluslararası alanda ses getiren yapılanmalar şu şekilde sıralanabilir:

- *Anonymous: 2006 yılından beri aktif olan bir gruptur ve adından sıkça söz ettirmektedir. Bilinen bir merkezi ya da yöneticisi olmayan grubun 2009 yılında İran'a yönelik seçim protestosu saldırısı ve 2012'de Go Daddy'ye yaptığı saldırı dışında Julian Assange'a Wikileaks belgelerini temin etme konusunda yardım ettikleri doğrulanmıştır.*
- *Redhack: Türkiye'de de son dönemde adından söz ettiren grup 12 kişilik bir çekirdek kadro tarafından yönetilmektedir. Devlet kurumlarına yaptıkları protesto saldırıları ve ele geçirdiği gizli belgeleri yayınlamalarıyla tanınmaktadır. Türkiye'de resmi olarak terör örgütü kabul edilmiştir.*
- *LuizSec: Kısa ömürlü olmasına rağmen adından oldukça söz ettirmiş ve etkili bir hacker grubu olarak yerini almıştır. ABD ve Avrupa'da polisin sıkı takibine uğrayan grubun birçok üyesi tutuklanmıştır. Geriye kalan üyelerin Anonymus gibi gruplarda aktif olarak faaliyetlerine devam ettiği bilinmektedir.*
- *The Chaos Computer Club (CCC): En eski ve köklü gruplardan biridir ve Almanya merkezlidir. Gri şapkalı olarak bilinse de kimi eylem ve olaylarda grup üyelerinin adı geçmektedir. Eylemlerini "Halkı devlete karşı koruma" olarak tanımlamıştır.*
- *Honker Union: Çin'in bilinen en eski gruplarından olan Honker Union, 1999 yılından sonra faaliyetine başlamıştır. Çin hükümeti ile bağlantıları ortaya çıkan*

örgütün başta ABD ve Japonya olmak üzere askeri hedeflere saldırılar düzenlediği bilinmektedir.

- *Red Hackers Alliance: Çinli hacker gruplarının ortak birliği olan RHA, oldukça ciddi ve tehlikeli bir bir grup olarak kabul edilmiştir. 80 bin civarında üyesi olduğu tahmin edilmektedir ve Çin Komünist Partisi tarafından finanse edildiğine dair deliller de ortaya çıkarılmıştır.*
- *GhostNet: Başka bir ünlü Çin hacker grubu olan GhostNet, 2009 yılında ortaya çıkarılmıştır. Çin hükümetiyle bağlantılı olduğu bilinen grup farklı ülkelerin diplomatik misyonlarına yaptığı saldırılarla gündeme gelmiştir.*
- *Cult of the Dead Cow: ABD karşıtı ülkelere yönelik faaliyetleriyle dikkat çekmektedir ve ABD hükümeti ile ilişkilerinin olabiliceği ihtimalleri tartışılmaktadır. Grup ayrıca genç hackerlar için bilgilendirici ve eğitici faaliyetler de yürütmektedir.*

1.4.2.2. Manipülatif Birimler ve Söylemler

Son yıllarda siber güvenliğe ilişkin gelişmelerden en önemlisi uluslararası alanda yaşanan manipülatif gelişmeler ve doğurduğu sonuçlar olmuştur. Endüstriyel sistemlerin güvenlik zafiyetinin daha fazla ortaya çıkmasının ardından kurumların sahip olduğu verilerin de değiştirilerek geri dönülmez saldırıların yaygınlaşması beklenmektedir. Özellikle devletlerin günümüzde kırılgan noktaları olan krizler ve krizleri doğuran olaylara ilişkin manipülatif anlık söylemler ciddi maddi kayıplara da sebep olmaktadır.[62]

Krizlerin gelişiminde siber saldırı araçları ve hizmetleri her geçen gün olağan bir hal almaktadır ve herhangi bir organizasyona saldırmanın maliyeti önemli ölçüde düşmekte ve bu da birincil odak noktası olarak daha fazla sayıda saldırının yapılabilmesini sağlamaktadır. Devletlerin verecekleri alana ilişkin kararlar bu gelişme dahilinde işlemektedir. Veriler bilinçli ya da bilinçsiz olarak manipüle edilirse söz konusu kararlara ilişkin yanlış adımlar atılabilir ve zorlayıcı unsurlara da başvurulabilmektedir. Kontrol sistemleri ve üretim süreçlerindeki verilerin yanlış yorumlanması durumunda yıkıcı sonuçlar doğabilir (Nath, 2012: 314).

[62] EMC'nin güvenlik birimi RSA'in Başkanı Amit Yoran, 2015 yılında güvenlik sağlayıcılarının gelişmiş tehditlere karşı koruma sağladığı iddialarına ilişkin, aslında bunun tersinin olduğunu belirtmiş ve somut veriler ortaya koymuştur.

Devletler ve sahip olduğu verilere ilişkin karar alıcıları zorlayabilecek, hatta etki altına alabilecek manipülatif gelişmeler medyanın değişimi ve siber ortamdaki etkinliği ile söylemler boyutuyla uluslararası arenayı zorlamaktadır. Sosyal ağlar ve siber ortam üzerinden etkililiğini artırmaya çalışan medya ve illegal yapılanmalar manipülasyon ile kaos ortamı oluşturabilir ve hatta finansal krizlere neden olabilir. Günümüzde siber ortam araçlarıyla uluslararası sisteme etki edebilecek ve toplumları etkileyebilecek bir algı operasyonunun varlığı her fırsatta dile getirilmektedir. Farklı terör yapılanmalarının da bu algı operasyonlarını kullandığı bilinmektedir. Bilişim teknolojilerinin en belirgin değişimi devletlerin ciddi güvenlik sorunlarıyla karşı karşıya kalmalarıdır.

1.4.3. Siber Savaşçılar

Genel anlamda siber alt yapıları, konvansiyonel silahlar bünyesindeki sibernetiğe bağlı tüm sistemleri koruyan, siber güvenlik ve siber saldırı konularında uzman, bu saldırı ve savunma kabiliyetlerine sahip kişilere siber savaşçı denmektedir. Kara, deniz ve hava kuvvetleri unsurlarının yanında, başta NATO olmak üzere birçok ülke siber alanı yeni bir çatışma alanı olarak kabul ederek siber savaşçıların bu düzlemdeki önemi ve varlığını da kabul etmişlerdir.[63]

Siber savaşların harekat yönünde ve kazanç elde edilebilmesinde gerek yasal, gerekse yasa dışı yollarla bireyler farklı amaçlarla uluslararası arenada yer almaktadır. Özellikle siber anlamda harekatların yürütülmesinde karşı tarafın olanakları ve kabiliyetleri tam olarak bilinemediği ya da tespit edilemediği için ortak hareket edilecek bireyler veya grupların karakteristik özellikleri doğru tahlil edilmedilir. Bu grupları şekilde özetleyebiliriz (Keleştemur, 2015: 209):

- *Hacker'lar: Yaptıkları saldırılar neticesinde hedef bilgisayardaki verileri okuyabilir, kopyalayabilir ve değiştirebilmektedirler. Farklı topluluklar oluşturabilen hacker'lar bireysel ve gruplar halinde çalışabilmektedirler. Sürekli*

[63] NATO, 8 Temmuz 2016 tarihli Varşova Zirvesi'nde *"siber alanı"* yeni harekat alanı olarak ilan etmiştir ve ittifakın savunulacağı bir boyut olarak belirlemiştir. Siber saldırıların sadece devletlerden değil; bireyler, organize suç örgütleri ve terör örgütlerinden de organizasyonel bir şekilde uyarlanabileceği özellikle vurgulanmıştır. Kara, deniz ve hava mücadele alanlarından sonra siber alanın da resmi savaş alanı olarak ilan edilmesi siber savaşçıların ve orduların bir zorunluluk olarak teşkilatlandırılmasını gündeme getirmiştir.

olarak işletim sistemleri, yazılımlar ve internet teknolojilerinde açık arayan hacker'lar buldukları anda durumdan faydalanarak saldırılarını gerçekleştirebilmektedir.

- *Siyah Şapkalı Hacker'lar: Kötü amaçlı olarak sistemlere sızan, genelde kişisel bilgileri ele geçirmek, tamamen yok etmek gibi saldırgan faaliyetler yürüten hacker'lardır.*
- *Gri Şapkalı Hacker'lar: Sistemlere sadece merak amaçlı sızmakta, herhangi bir kötü amaç taşımamaktadırlar, fakat yine de yapılan suç teşkil edebilmektedir.*
- *Beyaz Şapkalı Hacker'lar: Siyah şapkalı hacker'ların yapacakları potansiyel tehditleri savuşturmakla yükümlüdürler.*

➢ *Siber Casuslar: Siber casuslar aslında birer hacker türevidir. Klasik istihbarat yöntemleri ve anlayışıyla hareket edip siber uzayda etkili olmaya çalışmaktadırlar. Siber casuslar sızdıkları sisteme zarar vermemekte ve bağlı oldukları yere hizmet etmektedirler.*

➢ *Toplum Mühendisleri: Toplum mühendisleri ya da sosyal mühendisler olarak da bilinen kişiler ileri seviyelerde psikoloji ve sosyoloji bilgisine sahiptirler. Genellikle istihbarat servisleri tarafından tespit edilmiş kişilere yönelmektedirler. Toplum mühendisleri daha çok yazılımsal alandan daha fazla insanlar üzerindeki açıklara yönelmektedirler.*

➢ *Kripto Analizciler: Kriptografik sistemleri ve algoritmaları analiz etmekle görevlidirler.*

➢ *Network ve Sistem Uzmanları: Bir kurum içinde tesis edilmiş olan ağ ve sistemlerin etkin ve sorunsuz çalışmasından sorumlu olan kişilerdir. Bu kişiler aynı zamanda herhangi bir problem olması durumunda problemin kaynağını tespit etme ve kısa sürede çözüm bulma özelliklerine sahiptir.*

Siber savaşçılar konusunda en profesyonel girişimler geliştiren ülkelerin başında ABD gelmektedir. 2012 yılında hackerlerın ABD merkezli enerji şirketlerinin bazı kilit mekanizmalara girişi düzenleyen şifreleri elde etmek amacıyla saldırılar düzenlediği ortaya çıkmıştır (Charmonman ve Trichachawanwong, 2014: 8). Hackerların, sözkonusu şifrelerle hayati önem taşıyan endüstriyel altyapı sistemlerinin kontrolünü elde etmeyi amaçladığı belirlendikten sonra bütçe planlarında ciddi bir değişikliğe giden ABD siber savaşçı statüsünde istihdam edilen personel sayısını kademeli olarak artırma yoluna gitmiştir.

1.5. Siber Güvenlik ve Uluslararası Hukuka İlişkin Sorunlar

Uluslararası hukuk, devletler arasındaki ilişkileri düzenlemeye yönelik bir ilkeler bütünü olarak ifade edilmektedir ve farklı kişi veya okulların hemen hepsinin, farklı uluslararası hukuk tanımlarına rastlamak mümkündür. Uluslararası hukukun özüne ilişkin tanımlamalar yapılırken ve eksikliklerine vurgular yapılırken siber güvenliğe ilişkin olaylar ve gelişmeler karşısında eksik kaldığı yadsınamaz bir gerçektir.

Devletlerin temel olarak uluslararası hukuk kurallarına uymalarının çeşitli nedenleri vardır. Devletler, kısmen bir alışkanlık çerçevesinde uluslararası hukuka verilen değerden dolayı, kısmen de söz konusu kuralların olmaması halinde ortaya çıkacak kaostan duydukları endişe dolayısıyla uluslararası hukuk kurallarına uymaktadırlar (Sönmezoğlu, 2000: 644). Ne olursa olsun, bireyin doğal olarak kendi özünde yönetimsel anlamda kurallar bütününe ihtiyaç duyması, siber uzaya ilişkin hukuksal bir yaklaşımı ve kimi zaman sorunları beraberinde getirmiştir.

Bilişim suçları da iç güvenlik açısından sorunsal oluştururken, siber uzaya ilişkin uluslararası hukukun eksik kaldığı noktalar, farkındalık oluşturma ve belli antlaşmalarla aşılmaya çalışılmaktadır. Bu başlık altında temel olarak uluslararası hukukun niteliği ve siber güvenlikteki yeri hususunda konu detaylandırılmaya çalışılmıştır.

1.5.1. Bilişim Suçları

Kişisel verilerin hukuksuz olarak ele geçirilmesinden siber suçlara, siber terörden siber savaşa ve uluslararası bazda siber istihbarata kadar birçok siber güvenlik olayı bireyleri, toplumu ve devleti tehdit etmektedir. Geçmişte meydana gelen geleneksel güvenlik tehditlerinin ve suç korkusunun yerini siber uzayda meydana gelebilecek korkular almıştır (Yeşilyurt, 2015: 16). Farklı tehditler ve araçlar beraberinde yasa dışı faaliyetlerle birlikte farklı ve yeni bir suç grubunu oluşturmuştur. Bu gelişmelerle birlikte yasal düzenlemeler de gecikmemiştir. Yasal düzenlemeleri zorlayan unsur, siber uzayın tanımlanmasına ilişkin uluslararası toplumun yaklaşımı olmuştur (Schmitt, 2012: 17).

Bilişim suçu olarak isimlendirilen eylemler bilgisayar üzerinde veya bilgisayar olarak nitelendirilmemekle birlikte bilgileri otomatik olarak işleme tabi tutabilen ya da veri iletişimi sağlayabilen diğer elektronik, manyetik veya mekanik araçlarla bunları veri iletişimi için birbirine bağlayan soyut ya da somut ağlar üzerinde işlenebilmektedir (Erdağ, 2010: 279). Yasal düzenlemelerin boyutu iç güvenlik ve dış güvenlik açısından sonuçlar doğurabilmektedir. Uluslararası alanda yapılan bir dizi hukuki düzenleme olsa da sınırlar arasındaki sorunlarda devletler ciddi bir koordinasyon eksikliğine sahiptir.

Tablo 5'te siber uzaya bağımlılığın arttığı ülkelerde bilişim suçları sıralamasında ilk 20 ülke yer almaktadır. Bilişim alanında temel gelişmişliği sağlamış olan başta ABD olmak üzere birçok ülke bilişim suçlarının işlenebilirliği açısından ilk sıralarda yer almaktadır. Bunun temelinde yatan en önemli husus kaynakların ne kadarının siber ortama bağlı olduğu ile ilgilidir. Türkiye bilişim suçları açısından dünya sıralamasında 9. olarak ciddi bir orana sahiptir ve bu konuda yapılan yasal düzenlemeler yetersiz kalmaktadır.

Tablo 5: Bilişim Suçları Sıralamasında İlk 20 Ülke

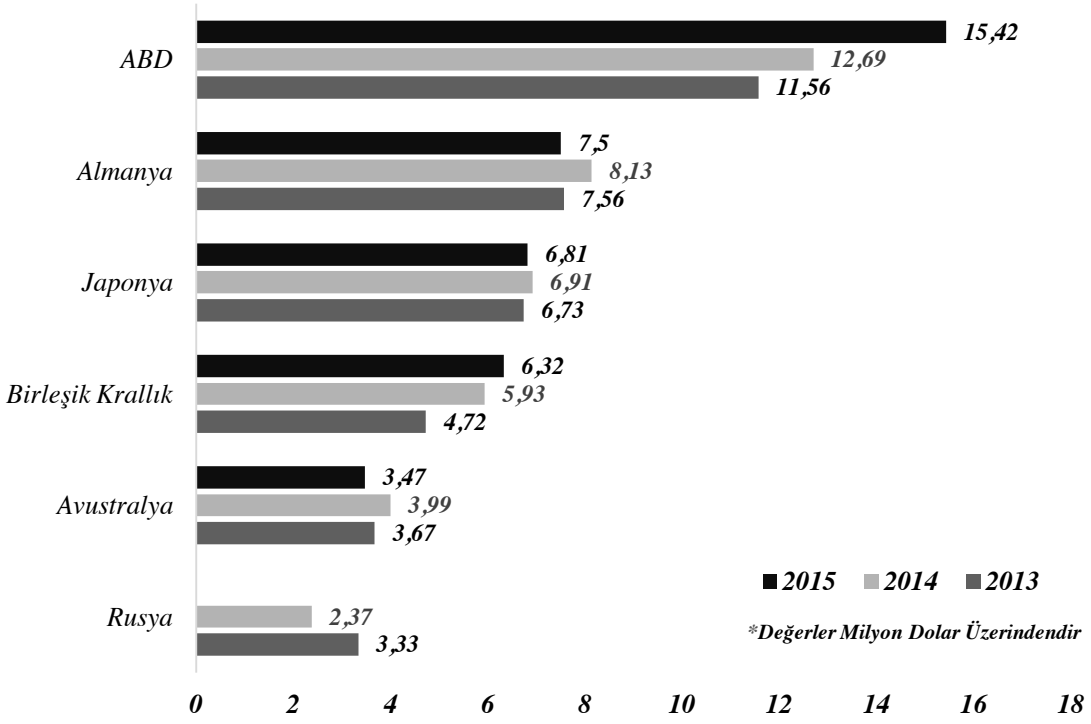
Sıralama	***Ülke***	***%***	***Sıralama***	***Ülke***	***%***
1	*ABD*	*23*	***11***	*Hindistan*	*3*
2	*Çin*	*9*	***12***	*Rusya*	*2*
3	*Almanya*	*6*	***13***	*Kanada*	*2*
4	*Birleşik Krallık*	*5*	***14***	*Güney Kore*	*2*
5	*Brezilya*	*4*	***15***	*Tayvan*	*2*
6	*İspanya*	*4*	***16***	*Japonya*	*2*
7	*İtalya*	*3*	***17***	*Meksika*	*2*
8	*Fransa*	*3*	***18***	*Arjantin*	*1*
9	*Türkiye*	*3*	***19***	*Avustralya*	*1*
10	*Polonya*	*3*	***20***	*İsrail*	*1*
DİĞER ÜLKELER					*19*

Kaynak: Saygılı, 2015

Bilişim suçları sadece ülkelerin iç güvenlik ve dış politika çıktıları açısından sorun oluşturmamaktadır. Küresel çapta bu suçların ülkelere maliyetleri de faturayı

kabartmaktadır. Verilerin kaybı ve çoğu zaman kurumların işlerliğindeki yavaşlama veya durma, bankalar üzerinden yapılan faaliyetler her bir devlet için maliyet yükü oluşturmaktadır. Grafik 10'da siber suçların devletlere maliyetlerinin son yıllarda değişimi gösterilmiştir ve artan orandaki değişim ile rakamların ciddi boyutlara ulaşması oldukça düşündürücüdür. Bu konuda devletler tedbir olarak siber suçlara karşı anlık hareket edememekte ve maliyet her geçen gün artmaktadır. Siber suçların, ABD'ye 2013-2015 yılı içinde maliyeti 30 milyon doları bulmuştur.

Grafik 10: Siber Suçların Global Düzeyde Bazı Ülkelere Maliyetleri



Kaynak: Ponemon Institute, 2015a: 10

Bilişim suçlarında maddi boyutların ciddi rakamlara ulaşmasında ve suçların uluslararası boyut kazanarak devletleri etkilemesinde siber suçlunun ya da suçluların koordineli olduğu durumlarda saldırganların amaçları, kararları ve araçları belirleyici olmaktadır. Siber suçlar açısından en sık karşılaşılan suç türü genel olarak DDoS saldırılardır.[64] Bu tarz saldırı türleri, internet üzerinden virus bulaştırmak suretiyle dizayn

[64] DDoS saldırıları temel olarak 2 şekilde gerçekleştirilmektedir. Bunlardan birinde çok sayıda farklı kullanıcının; sosyal medya, forum, IRC gibi kanallar üzerinden organize olarak aynı anda bir sisteme erişmeye

edildiğinden hacker tarafından sisteme giriş yapma zorunluluğu bulunmamaktadır (Darcan, 2015: 325).

1.5.2 Siber Uzayda Sanal Saldırı Ağı ve Uluslararası Hukukun Yetersizliği

Siber savaş alanı aslında günlük hayatta kullanılan cihazlar ve bunları birbirine bağlayan diğer öğelerden ibaret gözükmemektedir. Siber uzaydaki saldırı ağının içerisinde bilgisayarların içerisindeki işlemciler, cihazları birbirine bağlayan ve yer altından geçen kablolar ve fiber optik kablolarını taşıyan boru hatları da yer almaktadır. Bu noktada dolaylı olarak uluslararası hukukun ilgi alanına giren nokta siber uzaydaki tüm bigisayar ağları ve bu ağlara bağlı olan cihazlarla, onların kotrol ettiği unsurlar bulunmaktadır (Keleştemur, 2015: 195).[65] Bu unsurların kendi içerisinde oluşturduğu bilgi savaşı tüm aktörlerin yer aldığı uluslararası sistemde, çıkarsal bütünlük ile teknolojik gelişmenin buluştuğu noktada daha büyük bir etkileşimi ve bilişim kavramını ortaya çıkarmaktadır (Delibasis, 2008: 95).

"Bilişim" kavramı kontol edilen unsurlar ile ilgili olarak saldırı ağına yönelik ortaya çıkarılmış bir kelimedir. Günümüzde bilgisayar dışında yazılımla çalışan, verileri depolayan, işleme tabi tutan ve ileten elektronik cihazların çeşitlenmesi ile birlikte bilgisayara oranla daha kapsayıcı olan bilişim kavramı ortaya çıkmıştır. Uluslararası hukukun bilişim suçlarına ilişkin tepkisel olarak nasıl bir yol izlediği ve devletler arasındaki uyum eleştiri noktasını oluşturmaktadır.

Siber suçlarla mücadelede duyulan ihtiyaçlara paralel olarak hukuk sisteminde yapılan iyileştirmeler ile beraber yasal mevzuat etkin ve hızlı bir reaksiyona imkan sağlasa da internetin tasarımından kaynaklanan açıklar iz sürmeyi ve planlamayı güçleştirmektedir. Gerek ulusal anlamda, gerekse uluslararası hukukun ihtiyaçlarını giderme adına internetin güvenilir bir kullanıcı grubuna hizmet edeceğinin düşünülmesi nedeniyle, IP paketleri içerisindeki bilgilerin orijinal halinin korunmasına yönelik bir şifreleme önlemi alınmamıştır

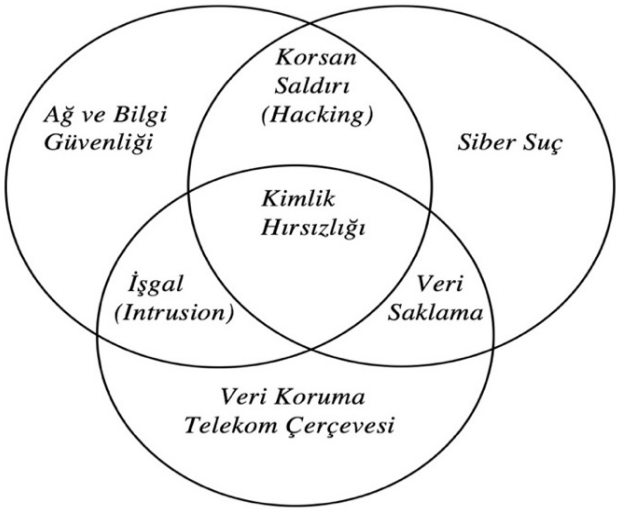
çalışması şeklinde olmaktadır. Diğerinde ise Botnet üyesi olan zombi makinelerin bilinçsizce sisteme erişimi şeklinde gerçekleşmektedir.

[65] Siber uzayın sadece internetten ibaret olmadığını kavramak ilk başlarda zor gelebilmektedir. Ancak internet, herkesin kolayca girebileceği, birbirine bağlı olan ağlardan oluşan açık ağdır. İnternette bulunan, bu ağa bağlı herhangi bir cihazla iletişim kurmak mümkündür. Ancak siber uzay içerisinde, internet ile birlikte internetten erişilemeyen, farklı ağlar da bulunmaktadır.

(Bayraktar, 2015: 99). Bu gibi durumlarda ilk kaynağa ulaşma gibi hususlar zorlaşmaktadır ve uluslararası hukukun alana ilişkin yorumu yetersiz kılmaktadır. Gelişen ülkeler için bu durum daha da çok hissedilmektedir (Shalhoub ve Al Qasimi, 2010: 36).

Uluslararası alanda yapılan düzenlemeler ve saldırı ağlarına ilişkin ortak politikalar oluşturma, konvansiyonel ve nükleer hususlarda dahi ortak anlaşmalara varılamamışken kısa vadede zor gözükmektedir. Bilgi güvenliği politika alanlarına ilişkin hangi temel çerçevenin baz alınacağı ve kapsayıcı olduğu tartışma konusu olacaktır ve devletlerin gelişmişlik düzeyi ile tarihi süreç bu konudaki samimiyeti azaltmaktadır.

Şekil 18: Bilgi Güvenliği Politika Alanları ve Etkileşim



Kaynak: Commission of the European Communities, 2001

Uluslararası hukukun etkileşim boyutu açısından siber ağları tamamen güvenli hale getirmek bir ütopya gibi görünse de siber saldırıları engellemek için küresel anlamda iş birliğine ihtiyaç olduğu bir gerçekliktir. Devletlerin siber tehditlere karşı yaklaşım ve yorumları farklı olduğu için, hukuki anlamda ortak bir çözüm zorlaşmaktadır (Yayla, 2013: 217). Siber alanın fiziksel alanda sonuç doğurduğu noktalarda saldırganın tespiti, saldırgan aktörün niteliği gibi hususlar uluslararası alanda ortak bir yaklaşımı daha da zorlaştırmaktadır ve bu konuda atılan adımlar oldukça yetersizdir. Bu konuda belli düzeylerde devletler ve uluslararası kuruluşlar nezdinde samimi adımlar da yok değildir.

1.5.3. Siber Güvenlik Antlaşmaları ve Uluslararası Düzenlemeler

Devlet örgütlenmesi ile birlikte oluşan iç hukukta, yasa yapıcı bir yasama organı, hukuk sistemi içerisindeki tutum ve davranışları bu yasalara uygunluk açısından denetleyen mahkemeler ve yasaların uygulanması açısından gerektiğinde önlemler alan kolluk kuvvetleri bulunmaktadır. Uluslararası hukukta da aynen iç hukuktaki benzer yapılanmayı bulmak mümkün değildir fakat uluslararası hukukta da konulara ilişkin benzer fonksiyonlar gören öğelerden söz edilebilir (Sönmezoğlu, 2000: 644). Bunlar arasında en önemlisi uluslararası antlaşmalardır. Malcolm N. Shaw (2008: 944), uluslararası antlaşmaların düzenlendiği alana bakılmaksızın *jus cogens* konseptine aykırı olmamasını ve sonuçlarının da gözetilmesini özellikle vurgulamaktadır.

Uluslararası hukuk açısından siber güvenliğe kaynak oluşturabilecek başlıca kaynaklardan olan antlaşmalar haricinde; teamül, genel hukuk ilkeleri ve uluslararası hukuk yazarlarının doktrinleri oldukça geri planda kalmaktadır. Bunun temel sebepleri özellikle siber terörizm ve siber savaşa ilişkin başlıklarda özetlenmişti. Antlaşmaların siber güvenliğe ilişkin düzenlemelerde baskın bir şekilde ön plana çıkmasının temel sebebi karşılaşılan bir sorunda nasıl bir karşılık verileceği ile ilgilidir.

Uluslararası düzenlemeler içerisinde, savaşa ve silahlı çatışmalara ilişkin düzenlemeler yapılırken, siber güvenliğe ilişkin yaklaşımda silahlı bir cevap verilip verilemeyeceğine dair bir kesinlik yoktur. Bu noktada atılan adımlar siber suçlarla mücadeleye ilişkin düzenlemelerle sınırlı kalmaktadır. Fakat devletler siber saldırılar sonrasında ciddi mağduriyetler de yaşamaktadır. Bu noktada oluşturulabilecek politikalara ilişkin teorik düzlem çalışmanın 3. bölümünde oluşturulmaya çalışılmıştır.

Uluslararası anlamda eskiye oranla daha ciddi ve somut adımların atıldığı siber güvenlik ile ilgili düzenlemelerde karşılıklı güven ilişkisine dair ciddiyet eksikliği halen devam etmektedir. Siber güvenliğe ilişkin yapılmış uluslararası antlaşmaları ve düzenlemeleri şöyle özetleyebiliriz:

- *Talin El Kitabı (Tallinn Manual):* Orijinal adı *"Tallinn Manual on the International Law Applicable to Cyber Warfare"* olan *Tallinn Manual,* bağlayıcılığı olmayan

akademik bir çalışma olarak uluslararası hukukun siber savaş ve çatışmalara uygulanabilirliğini tartışan bir çalışmadır. 2009-2012 arasında NATO tarafından davetli yaklaşık 20 uzmanın hazırladığı el kitabı, 2013 yılında Cambridge University Press tarafından yayınlanmıştır. Söz konusu çalışmaya Kızıl Haç Uluslararası Komitesi, NATO ve ABD Siber Komutanlığı da gözlemcilik yapmıştır. Çalışmada günümüz uluslararası yasalarının siber ortamda nasıl uygulanacağına yönelik yorumlar mevcut olup ilave yasa maddesi önerilmemektedir. Türkiye'de MGK tarafından resmi sitede yer verilen kitap, siber savaşta BM'nin siber saldırılara karşı uluslararası askeri operasyon dahil önlemleri alabilmesine imkan tanımaktadır.

➢ *Avrupa Konseyi Siber Suçlar Sözleşmesi:* Bilgisayar ve internet suçları ile ilgili düzenlemeler getiren ve *Budapeşte Sözleşmesi* olarak da bilinen çalılşma 1 Temmuz 2004 tarihinde yürürlüğe girmiştir. 48 maddeden oluşan sözleşme özellikle telif haklarının ihlalleri, bilgisayarlarla ilgili sahtekarlık eylemleri, çocuk pornografisi ve ağ güvenliğine ilişkin suçları tanımlamaktadır.

➢ *Siber Suçlara Karşı BM Kararları:* BM siber suçlarla iligli etkin bir çalışma içindedir. Bu konuda iki karar ön plana çıkmaktadır.

- *57/239(2002) numaralı BM kararı: Siber güvenlik konusunda bir kültür oluşturmaya yönelik dokuz kıstas tanımlanmıştır.*[66]
- *58/199(2004) numaralı BM kararı: Siber güvenlik küresel kültürünün geliştirilmesi ve kritik altyapıların korunması üzerine odaklanmaktadır (Çifçi, 2013: 104).*

➢ *Bilgisayarla İgili Suç: Yasal Politikanın Analizi Raporu (Computer Related Crime: Analysis of Legal Policy):* OECD tarafından 1986 yılında yayınlanarak üye ülkelere hangi ihlallere cezai yaptırım uygulaması gerektiğinden bahsedilmektedir.

➢ *Ülkelerarası Organize Suçlarla Etkin Mücadelede Tavsiyeler Raporu:* G8'in Fransa Zirvesi'nde 40 temel noktanın üzerinde durulmuştur. Ülkelerin iç hukuklarını modern teknoloji ihlallerini cezai müeyyide ile karşılayacak şekilde yeniden düzenlemeleri belirtilmiştir (Çakmak ve Katman, 2009: 178).

[66] Bunlar; *farkındalık, sorumluluk, mukabele, ahlak, demokrasi, risk değerlendirmesi, güvenlik tasarımı ve gerçekleştirimi, güvenlik yönetimi* ve *yeniden değerlendirmedir*. BM kararlarının, farklı kıstaslarla gündeme getirmeye çalıştığı siber güvenlik çalışmalarında yaşanan temel sorunsal devletlerin alana bakış açısının ciddi derecede farklılık içermesidir. Tüm üye ülkeler açısından konunun ele alınışındaki ciddiyet aynı derecede ortak bir tavır alınışında gerekli potansiyele ulaşamamıştır.

Siber güvenliğe ilişkin yapılan düzenlemeler ile ilgili, uygulama alanında yaşanan sorunlardan en temeli yargılama yetkisi sorunu ve ülkeler arasındaki uyumdur. Siber suçlar genellikle birden fazla ülkeyi ilgilendirecek bir nitelik sergilemektedir (Sandvik, 2012: 3). Uluslararası alanda düzenlemelerin uygulanmasına ilişkin diğer bir temel sorun ise fiziksel arama ya da haberleşmelerin takibi/dinlenmesi hususunda yasal sürecin başlatılması ve harekete geçilmesi yönündeki güçlüklerdir.

1.5.4. Karşılaşılan Hukuksal Güçlükler, Algının Kırılması ve Farkındalık

Uluslararası sistemdeki aktörlerin üzerinde uzlaştıkları bir siber alan tanımı yapılmamıştır. Bu durum, ülkelerin tanımlayama çalıştıkları siber alanın sınırlarının belirgin olmamasına neden olmakta ve siber alan üzerinden yapılan saldırılarda hukukun nasıl uygulanacağı konusunu bir sorunsal olarak ortaya çıkmaktadır (Bayraktar, 2015: 104).[67] Siber güvenliğin genel tanımında olduğu gibi siber alanın ve siber savaş kavramının tartışıldığı noktada uluslararası hukuk uzmanları arasında bir anlaşmazlık söz konusudur. *"Siber savaş"* kavramı yerine *"Siber Silahlı Çatışma"* kavramıyla da sıkça karşılaşılmaktadır (Schmitt ve Vihul, 2014: 8).

İnternet hizmetlerinde ve kullanımındaki artış, aktarılan bilgi hacmindeki yoğunluk suçların ve suçluların tespitinde yaşanan önemli bir güçlüktür. Uluslararası hukuk adına çoğu zaman devletlerin birbirlerine ilişkin söylemleri de iddia bazında kalmaktadır. Hukuksal anlamda izlenecek yol doğal olarak askıda kalmaktadır.

Gerek hukuksal anlamda, gerekse uygulamaların güvenilirliği açısından algı oluşturulması adına bilgi güvenliği ve siber sorunlara ilişkin bağlantıların yönü doğru algılanmalıdır. Algısal olarak siber güvenliğe dair karşılaşılan hukuki sorunlar sadece uluslararası anlamda değil, bireylerin yaşadıkları iç politika ve bunun devamındaki dış politika açısından önem taşımaktadır. Bilgi güvenliğinin uluslararası normlarla tartışılması, en azından siber ortama ilişkin, devletler arasındaki güven algısını arttırıcı bir etken olacaktır.

[67] Bir siber suçun failini tespit edebilmek için öncelikle suçlunun yerini bulmak, yani saldırı kaynağının IP adresini tespit etmek gerekmektedir. Bunun için izlenen yöntem hedeften geriye doğru yönlendirici takip etmektir.

İnternet hizmetlerinde ve kullanımındaki artış, aktarılan bilgi hacmindeki yoğunluk suçların ve suçluların tespitinde yaşanan diğer bir güçlüktür. Tüm suçlarda olduğu gibi siber ortamda gerçekleştirilen suçlarda, suçun oluşabilmesi için manevi unsurun bulunması, yani failin eylemi kasten veya taksirle işlemiş olduğunun ispatlanması gerekmektedir (Bayraktar, 2015: 105).

Siber ortamda suçlar, herhangi bir yere ve kimi zaman bir merkeze bağımlı olmadan dünyadaki ağ sistemleriyle başka herhangi bir yere kanalize olabilme özelliğine sahiptir. Saniyenin de daha az zaman dilimlerinde, ışık hızında müdaheleler dünyanın bir ucundan diğer ucuna gerçekleşmektedir. Sınır tanımayan siber saldırılar karşısında devletlerin iş birliği yapmaları gerekliliğine karşın bu konuda farkındalığın azlığı dikkat çekicidir (Çakmak ve Katman, 2009: 167). Uluslararası düzenlemelerin teknolojik gelişmelere adapte edilmesi gerekliliği vurgulanması gereken diğer bir husustur. Nükleer anlamda tesislerin kurulması ve nükleer geliştirmelere ilişkin uluslararası hukukta nasıl adımlar atılıyorsa benzer süreçler siber güvneliğe de uyarlanabilir (Chatterjee, 2014: 8).

1.5.5. Siber Saldırılar ve *Jus Ad Bellum-Jus In Bello*

Uluslararası hukukta, *kuvvet kullanma hakkı (jus ad bellum)* ile *kuvvete başvurulduğunda uyulması gereken çatışma kuralları (jus in bello)* arasında bir ayrım yapılmaktadır. Buna göre silahlı çatışma hukuku kurallarının uygulanmasının, bu hakka sahip olunup olunmadığı sorunundan tamamen bağımsız olduğu kabul edilmektedir (Yayla, 2013: 202).[68]

Siber saldırılar ve silahlı çatışma hukukuna ilişkin kurallar özellikle uluslararası düzenlemelerde netlik kazanmayan hususlar arasındadır. Kuvvete başvurma ve bu konuda kararlar alma uluslararası kamuoyunun ilgisi dahilindedir ve anlayış olarak somut bir siber saldırı çıktısı gözetilmektedir. Siber alanda yaşanan gelişmelere ilişkin kuvvete başvurma gibi tedbirlerin var olması gerektiği çoğu zaman belirli ülkelerle sınırlı kalmaktadır.

[68] Savaş hukuku incelenirken, kuvvet kullanılmasının hukuka uygun olup olmadığı hususu ile silahlı kuvvet kullanılması sırasında seçilen hedef, araç ve yöntemlerin hukuka uygunluğu hususunun birbirinden ayrı incelenmesi ve düşünülmesi gerekmektedir. Siber saldırı durumunda devletlerin buna karşılık verme hakkı, kuvvete başvurma hakkına ilişkin (jus ad bellum) kuralların incelenmesini gerekli kılmaktadır.

Siber saldırıların kaynağını bulmayı amaçlayan teknolojiler geliştiği ölçüde siber saldırıların kaynağını gizleyen teknolojiler de gelişme göstermektedir. Bir fiil ya da hareketsizliğin devlete atfedilebilir olması için söz konusu fiilin o devletin *de facto* ve *de jure* organları ya da ajanları tarafından yapıldığının ispat edilebilir olması gerekmektedir (Kurtdarcan ve Mumcu, 2014: 182). Siber saldırıların oluşturulması aşamasında siber harekatın yöneliş şeklinin temelinde yer alan siber casusluk ve siber suçların çıkış noktası karar alıcılar ya da bireyler olmaktadır. Siber harekat düzlemine göre siber müdahele ve siber saldırı şeklinde devam eden süreçte harekatın çıkış noktası doğru bir şekilde tespit edilebilirse *kuvvet kullanma hakkı (jus ad bellum)* işletilebilir (Melzer, 2011: 6).

Siber ortam, bir devletin kuvvet kullanımına varmayan harekatlara ilaveten ölümlü veya yaralanmalı sonuçlar doğurabilecek harekatlar yapmasına olanak sağlayabilir. Ölüm, yaralanma veya maddi kayıplara sebep olan siber eylemler, uluslararası hukuk açısından silahlı saldırı veya kuvvet kullanımı olarak değerlendirilebilir. ABD Siber Komutanlığı tarafından tanımlandığı şekliyle siber eylemler, siber casusluktan erişim operasyonlarına ve en son noktada ölüm veya maddi kayıplara sebep olan aktivitelere kadar yayılan geniş bir eylem spektrumu boyunca görülebilir.

Geniş eylem sürecine sahip olan siber ortam, kendi kapasitesinin başlangıcı itibariyle siber suç veya casusluğa yönelik olsa da özellikle kritik altyapılara ilişkin saldırılarda ve müdahelelerde fiziksel bir zarara ilişkin saldırı türüne dönüşmektedir. Caydırıcılık amaçlı olan ve daha az gizliliğe sahip olan fiziksel sonuçlu bu tür saldırılarda savaş hukukuna ilişkin süreç, klasik savaşa ilişkin uluslararası düzenlemelerde olduğu gibi sonuçlar doğurabilmektedir.[69]

[69] Uluslararası hukukta, meşru müdafaa haricinde kuvvet kullanmanın yasaklanması ile beraber *jus in bello,* haklı savaş teorisinden koparak kendine bağımsız bir alan kazandırmıştır. Bu bağımsız olma hali nedeniyle siber saldırıya ilişkin *jus in bello* kurallarını, *jus ad bellum* siber saldırı ilişkisine dair kurallardan farklı olarak ele almak gerekecektir.

İKİNCİ BÖLÜM

2. SİBER GÜVENLİK VE UYGULAMA ALANLARININ ULUSLARARASI İLİŞKİLERDE GELİŞİMİ

"Uzay konrolünün coğrafyası hakkında konuşmak ile uzayı kontrol edebilmek tamamen farklı şeylerdir. Düşman kuvvetlerinin uzaya çıkmasını engelleyecek silah sistemleri henüz geliştirilmedi…"

George Friedman

2.1. Siber Güvenliğin Politik Düzlemde Dönüşümü

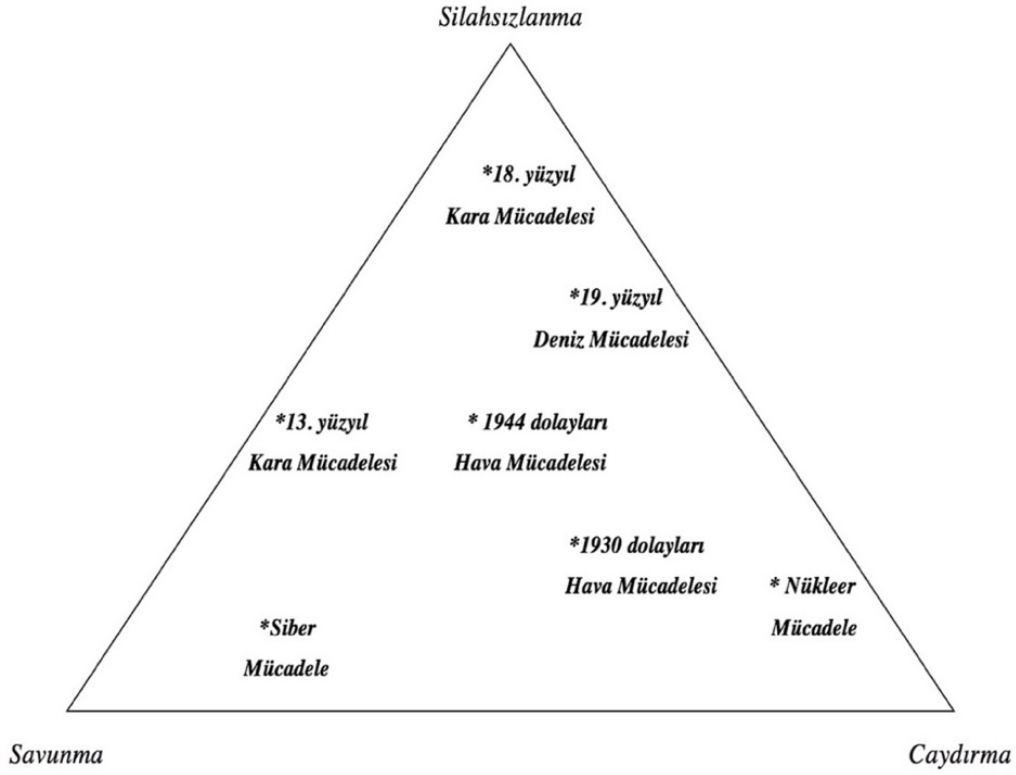
Fiziki dünyada, sanal dünya vasıtasıyla yapılabilecek yeni siber saldırı taşıyıcılarından kaynaklanan artan bir hassasiyet mevcuttur. Günümüzde savaşlar, sadece askerler ve askeri teknolojiler yardımıyla yapılmamaktadır. Kamu hizmetleri, ulaşım, iletişim ve enerji gibi kritik endüstrileri aksatan veya yok eden özenle silahlandırılmış bilgisayar programlarını uzaklardan serbest bırakan bir müdahele ile yapılmaktadır. Böyle saldırılar ilave olarak askeri unsurların hareketlerini, savaş uçaklarının rotalarını ve savaş gemilerinin komuta kontrolünü sağlayan ağları da etkisiz hale getirebilmektedir.

Etkisiz hale getirebilme ya da süreci aksatabilen unsurların ortaya çıkması, mücadele alanı arayan aktörlerin de zamanla iştahlarını kabartmıştır. Bilginin ve yönetimsel olarak verilerin sahip olunmasına ilişkin arzu, siber güvenlik kavramını uluslararası politika alanında daha belirgin kılmıştır. Devletler kendi içlerindeki yasal düzenlemeler gibi uluslararası alanda tüm konular üzerinde şeffaf ve adil olamamaktadır. Siber saldırıların ve terörizmin vermiş olduğu avantaj uluslararası güvenliğe ilişkin sorunları ve çalışmaları da artırmıştır. Siber güvenlik kavramı, politik bir düzlemde ilerlerken uluslararası bir boyut kazanımına ilişkin bir soru uluslararası güvenlik çalışmalarında artan bir hassasiyete sahip olmuştur. Bu sorunun temel olarak gelişiminde, özgün bir tarihi arka plan da mevcuttur. Teknoloji ve sibernetiğe ilişkin gelişmeler özellikle Soğuk Savaş dönemiyle birlikte bir devinim kazanmıştır.

Soğuk Savaş dönemindeki çekişme her alanda kendini hissettirirken gelecekle ilgili sibernetiğe ilişkin felsefi tartışmalar bu mücadelenin içinde yerini almıştır. Soğuk Savaş'ın sonra ermesi ve özellikle hegemon bir güç olarak ABD'nin siber uzaya ilişkin çalışmaları başdöndürücü bir şekilde gelişmiş ve günümüz siber politikaları ile igili çalışmaların temelini oluşturmuştur.

Libicki'nin (2009: 175) Şekil 19'da ortaya koyduğu caydırma-silahsızlanma-savunma üçgeninde, yakınlıkları açısından gruplandırdığı mücadele türleri konunun gelişimini açık ve güzel bir şekilde ortaya koymaktadır. Yakın dönemde özellikle siber mücadele ve nükleer mücadelenin tarihi olarak diğer mücadele türlerinden çok daha net bir şekilde savunma ve caydırma unsurlarına yaklaştığını görmekteyiz. Siber mücadele gelişim itibariyle, saldırıların bilinmezliği yönüyle savunma alanında paralel bir gelişmeyi sağlarken, nükleer gelişmeler caydırıcılık olarak en üst noktada bu kavrama yaklaşan mücadele türü olarak gelişimini sürdürmektedir.

Şekil 19: Mücadele Çeşitlerinin *Caydırma-Silahsızlanma-Savunma Üçgeninde* Duruşu



Kaynak: Libicki, 2009: 175

2.1.1. Tarihsel Olarak Siber Güvenlik Kavramının Uluslararasılaşması

Savaş ve şiddetin yok edilip edilemeyeceği sorunsalı, uluslararası ilişkilerin I. Dünya Savaşı'nın ardından sistematik bir akademik disiplin olmasından itibaren farklı çalışmaların merkezinde yer almıştır. Soğuk Savaş sonrası dönemin getirdiği yenilik, uluslararası ilişkiler literatürü üzerinde önemli bir etkide bulunan güvenliğin doğasına dair yeni yaklaşımlar oluşturmuştur (Baylis, 2008: 71).

Özellikle savaş teknolojilerindeki gelişim ve istihbarat yapısı ile ilgili genel değişim siber güvenlik kavramına ilişkin yaklaşımları ve uluslararası ilişkilerin bu yönüne ilişkin çalışmaları hızlandırmıştır. Son yıllarda uluslararası güvenlik konusunda farklı ve kendine özgü bir bakış açısı geliştiren normatif uluslararası ilişkiler yaklaşımlarıyla siber güvenliğe ilişkin teorik düzlem harmanlanmış ve siber güvenlik kavramının uluslararası alandaki belirginliği daha da artmıştır.[70]

Devletlerin çıkar amaçları yeni savaş ve saldırı yöntemlerini beraberinde getirmiştir. *"Siber Terörizm"*, *"Siber Saldırılar"*, *"Siber Caydırıcılık"*, *"Siber Güvenlik"* olarak ele alınan kavramlar farklı gelişmeleri ve uluslararası arenada farklı bir çatışma alanını ortaya çıkarmıştır. Hem mikro hem de makro düzeyde yapılan bu türden saldırılar maliyet açısından devletleri zorlamazken, saldırıları kimin yaptığına ulaşılamamaktadır. Bu da devletlerin elini güçlendirmekte ve önünü açmaktadır.

Nükleer caydırıcılığın aksine siber caydırıcılıkta taarruz kabiliyeti, yeri ve zamanı bilinmezken; telafi edilemez ekonomik kayıplar verdirilebilmekte ve can kaybı yaşanmamaktadır. Diğer taraftan hem saldırı hem de savunma ayağında daha etkili manevralar yapılabilmekte ve zarar en aza inebilmektedir. Fakat bu türden saldırıların veya terörizmin caydırıcılığı ancak ve ancak somut olarak uygulandığında gerçekleşebilmektedir (Güntay, 2015: 479). Caydırıcılık yönünün artmasıyla siber güvenlik uluslararasılaşan bir kavram haline dönüşmüştür. Her ne kadar tartışılabildiği boyut Soğuk Savaş döneminin

[70] Örnek olarak David Campbell, uluslararası ilişkilerin geleneksel söylemlerine paralel bir şekilde ittifak ile güvenliğin devlet tarafından kullanılacak bir dizi araçla sağlanacağını savunmaktadır ve genel olarak bu anlayış kabul görmektedir. Fakat savunma ve dış politika arasındaki bağlantı farklı bir şekilde anlaşılabilmektedir. Dış politikanın bir parçasını oluşturduğu güvenlik, her şeyden önce siyasi düzeni oluşturan bir söylem olarak karşımıza çıkmaktadır.

klasik caydırma teorileriyle açıklanamasa da süper güçlerin yükselişiyle etkisini artıran *"siber güvenlik"* kavramı 1939 ve öncesindeki uluslararası sistemde kendisine yer bulamamıştır (Zagare ve Kilgour, 2000: 4).

Siber güvenlik kavramının uluslararası ilişkiler alanında inceleme boyutuna sahip olmasının başında caydırıcılık ve uygulama alanına ilişkin somut olayların artması gelmektedir. Tablo 6'da siber olayların tarihsel gelişimine ilişkin süreç özellikle siber casusluk ve siber savaşa ilişkin parametrelerin artışıyla ortaya konulmuştur. Soğuk Savaş'ın bitişi ve bu parametrelerdeki gelişimin hız hazanması daha önce vurguladığımız siber terörizm, siber savaş ve siber güvenlik gibi kavramların devletlerarası ilişkilerde incelenmesini zorunlu hale getirmiştir. Siber savaşın yönü Soğuk Savaş sonrasında aynı hızıyla devam ederken, zararlı yazılım ve siber suçlara ilişkin uluslararası çapta etki yaratması ve olayların artışı devletlerarasında iş birliğini de gerekli kılmıştır.

Tablo 6: Siber Olayların Tarihsel Olarak Gelişimi

Zararlı Yazılım	*1*	*-*	*2*	*3*	*4*	*5*	*7*	*9*	*10*	*11*	*-*	*12*	*13*	*14*
Siber Suç Casusluk	*-*	*-*	*-*	*-*	*-*	*-*	*15*	*-*	*-*	*-*	*16*	*18*	*19*	*-*
Siber Savaş	*-*	*20*	*21*	*22*	*-*	*-*	*-*	*-*	*23*	*24*	*25*	*27*	*28*	*29*
YILLAR	***1988***	***1991***	***1998***	***1999***	***2000***	***2001***	***2003***	***2004***	***2007***	***2008***	***2009***	***2010***	***2011***	***2012***

Kaynak: Bakır, 2013

Siber olayların tarihsel gelişimi içerisinde güvenlik boyutuna dönüşmesi, 1960 ve 1970'li yıllar boyunca tartışılan bilgi devriminin kendi içerisindeki temel değişikliklerle gerek medya araçlarını gerekse inovasyon yönündeki unsurları etkilemesiyle de alakalıdır. Kimi halk hareketlerinde ve verilerin sızdırılması amacıyla gerçekleşebilecek anlık iletişimde siber araçlar etkin bir şekilde kullanılmaktadır ve devletlerin yakın takiplerindedirler (Cavelty, 2008: 13).[71] Bu takip içinde devletlerin adını tam koyamadağı

[71] Yapılan analizlerde sosyal medyanın ve siber kanallar vasıtasıyla oluşturulan haberleşme unsurlarının etkisiyle başta Arap Baharı olmak üzere birçok hareketin örgütlendiği tespit edilmiştir. Sosyal medya, Tunus'ta devrim günlerinde yaygınlaşmış ve devrimden sonra da etkileri hissedilmeye başlanmıştır. Fakat Mısır'da, Arap Baharı'ndan çok daha önceleri sosyal medya faaliyetleri organize olmuştur.

ve kimi araştırmacılara göre radikalleş(tir)me aracı olarak da kullanılan internet ve medya etkileşimi yeni bir savaş aracı olarak kabul edilmektedir. Özellikle toplumsal hareketlenmelerde bu durum daha da hissedilir bir hal almıştır (Hoskins ve O'Loughlin, 2008: 31).

2.1.2. Soğuk Savaş Dönemi Gelişmeleri Çerçevesinde Siber Güvenlik

II. Dünya Savaşı sonrası oluşan uluslararası sistemi tanımlamak için kullanılmış olan Soğuk Savaş, iki kutuplu sistem döneminde ABD ve SSCB'nin liderliklerindeki Batı ve Doğu Blokları arasında gerginlik ve kısmi çatışma biçiminde sürdürülen mücadele olarak karşımıza çıkmıştır. Ulusal güvenlik, Soğuk Savaş dönemindeki uluslararası sistemi şekillendiren ve ulus devletler arasındaki ilişkileri düzenleyen en temel unsur olarak belirginleşmiştir.

Soğuk Savaş döneminin güvenlik yaklaşımı perspektifinde siber güvenliğin günümüzdeki boyutuna ulaşmasında ciddi temeller oluşmuştur. Sönmezoğlu (2010: 719) bu durumun oluşmasında güvenlik yaklaşımına ilişkin üç belirleyici özelliği şu şekilde açıklamıştır:

> - *"İlk olarak NATO ile Varşova paktı gibi, güvenliğe ilişkin kararların alındığı iki merkezde süreç çatışmaya dönük bir görünümde seyretmiş ve savaş teknolojilerine ilişkin gelişmeler karşılıklı olarak izlenmiş, geliştirilmiştir.*
> - *İkincisi, bloklar ekonomik ve askeri yapılanmalarla üçüncü dünya ülkelerini kendi etki alanlarına sokmak adına uluslararası ilişkilerde çekişme içine girmişlerdir ve uzak coğrafyalara etki edebilme adına sibernetiğe ilişkin öz gelişim göstermiştir.*
> - *Üçüncüsü ise silahların kitlesel yok edici özelliği savaşları önleyici bir hal almış ve bu da yine müdahele anlamında farklı araçların gelişimini hızlandırmılştır. Sisteme ilişkin stratejik denge farklı unsurlarla oluşturulmaya başlanmış ve arayış içine girilmiştir."*

II. Dünya Savaşı sonrasında bu temel özelliklerin yanında istihbarata ilişkin, teknolojik verilerin artması siber güvenliğin bu süreçte yıldızını parlatmıştır. İstihbarat sadece savaş kazanmak için gerekli görülürken sinyal ve görüntü istihbaratına ilişkin önemin farkedilmesi teknolojik arayışları siber güvenliğin uluslararası ilişkiler boyutuna itmiştir. Çok kısa bir zamanda U-2 Keşif Uçakları, uzay programları, bilgisayarların en eski örnekleri

ve örtülü operasyonlar ile ilgili özel vasıtaların gelişimi konusunda önemli adımlar atılmıştır (Yılmaz ve Salcan, 2008: 25).[72]

Özellikle ABD'nin, Sovyet uydusu Sputnik'e karşılık olarak ileri bilimsel ve teknolojik projeleri hayata geçirmekle görevli ARPA'yı harekete geçirmesi 1958 yılını bir milat haline getirmiştir. 1969 yılına gelindiğinde Amerika'nın önde gelen üniversite ve enstitüleri kendi aralarında bilgi alışverişi sağlamak amacıyla ABD Savunma Bakanlığı tarafından desteklenen ve o güne kadar daha çok askeri amaçlı kullanılan ARPAnet ağına katılmışlardır.[73]

1974 yılına gelindiğinde Bob Kahn ve Vint Cerf adlı bilimadamları birbirinden bağımsız ağlardaki kullanıcıların iletişim kurabilmesi ve veri gönderimi sağlayabilen devrim niteliğindeki TCP protokolünü yazmıştır. Özellikle siber güvenliğin uluslararası alanda bahsedilmesi ve olayları etkilemesine ilişkin olaylar TCP'nin hızlı bir şekilde gelişmesiyle başlamıştır.

Sovyetler Birliği 1980'lerin ortalarına kadar bilgisayar teknolojilerinin tümünü KGB aracılığıyla batıdan çalmaya devam etmiştir. Sovyetler Birliği'nin bilgi alma operasyonları 1981 yılnda ABD ve Fransa'nın düzenlediği ortak bir operasyonla ortaya çıkmıştır.[74] Rusya'nın özellikle günümüze kadar uzanan bölgesel siber saldırganlığı ve hegemon bir bölgesel siber güç olarak bölge ülkeleri takibi 1980'lerdeki bu tür faaliyetlerine uzanmaktadır (Hansen ve Nissenbaum, 2009: 1169).

Soğuk Savaş'ın bitimine yakın devletlerin kendi altyapılarının da ciddi bir şekilde etkilendiği Morris virüsü, bilişimin karanlık boyutuna geçen bir çok yazılımcı açısından iştah kabartıcı olmuştur ve uluslararası alanda siber güvenliğe ilişkin verilerin önemine dair

[72] 4 Haziran 1956'da Sovyetler Birliği'nin üzerinde U-2'lerin ilk uçuşundan iki ay sonra bir keşif uydusu üretimi için operasyonel gerekçeler üretilmeye başlanmıştır. Uydular; görüntü elde etme, sinyal toplama, iletişim, erken ikaz ve diğer çeşitli istihbarat görevlerinin yerine getirilmesinde kullanılmıştır.

[73] 1968 yılında, Sovyet bilim adamları KGB'nin yardımları ile IBM'in o dönemdeki en güçlü modeli olan IBM System/360'ın bir benzerini yapmaya başlamıştır. Bu bilgisayar Ay'a ilk adım atılan projede kullanılmıştır.

[74] Sovyetler Birliği'ne ait verilerin alınmasında ve Soğuk Savaş'ta ABD'nin ciddi bir avantaj elde etmesinde ABD'nin bu konuya ilişkin planı dikkat çekicidir. CIA'in o dönemki başkanı olan Bill Casey, KGB'nin verileri çalmasına izin verilmesini fakat çalınacak şeylere hatalar yerleştirilmesini planlamıştır. KGB ajanları hatalı verileri ülkelerine götürmeye başlamış ve sistemsel sorunlar içine girmişlerdir.

ciddi bir gelişme olmuştur. Dijital saldırganlık ve yakın gelecekteki boyut adına ipuçları sunan, Soğuk Savaş'ın sonunda yaşanılan olaylar siber güvenliğin bilgi çağında hem teknik boyutuyla adından söz ettireceğini, hem de sosyal bilimler ve uluslararası ilişkiler adına yer edineceğini ortaya koymuştur.

2.1.3. Soğuk Savaş Dönemi Sonrasında Uluslararası Güvenlik ve Siber Güvenlik

II. Dünya Savaşı'nın sona ermesinin ardından Soğuk Savaş döneminin başlamasıyla birlikte yeni bir güvenlik rejimi ortaya çıkmıştır. Sıcak çatışmadan uzak kalınan bu dönemde, tedirginlik ve tansiyon hep yüksek olmuştur. 1989 yılında Berlin Duvarı'nın yıkılması sonrasında, 25 Aralık 1991'de Sovyetler Birliği'nin dağılmasıyla birlikte, uluslararası sistem için gerilimli bu iki kutuplu dönem yavaş yavaş sona ermiştir (Bıçakçı, 2012: 206).

Sovyetler Birliği ve liderliğini yaptığı Doğu Blok'unun ortadan kalkmasıyla birlikte somut bir düşman olarak karşı tarafını yitiren NATO'nun meşruiyeti sorgulanmaya başlamıştır. NATO'nun misyonunun artırılması ve ittifakın güvenlik alanının genişletilmesi için 1990 Londra Konferansı'nda yeni bir strateji geliştirilmesi kararı alınmış, 1991 Roma Zirvesi ile yeni stratejik konsept geliştirilmiştir (Bayraktar, 2015: 37). Siber güvenliğe ilişkin gerek politik düzlemde, gerekse yeni adımlarla NATO kendine ciddi misyonlar edinmiştir. Birbiri ardına gelen tatbikat ve zirvelerle siber güvenliğe ilişkin her adım NATO'yu bir adım daha öne taşımıştır (Healey ve Jordan, 2014: 3).

Soğuk Savaş dönemi boyunca simetrik bir düşmanı bulunan ve Ortodoks güvenlik anlayışıyla hareket eden NATO, Kosova Savaşı'nda maruz kaldığı siber saldırılar neticesinde bu anlayışını günümüze dek modernize ederek Soğuk Savaş sonrasında en ciddi atılımı yapan örgütlenme olmuştur. Özellikle sırasıyla 11 Eylül saldırıları ve bir NATO müttefiki olan Estonya'ya yönelik siber saldırılar, NATO ve üye ülkeleri siber tehditler ve siber güvenlik konularında daha fazla ihtiyatlı olmaya yöneltmiştir (Boyraz, 2015).

Soğuk Savaş süresince tartışılan ve uluslararası çalışmalarda önemli bir yere sahip olan konvansiyonel ve nükleer caydırıcılık yanına siber caydırıcılık kavramının eklenmesi ile devletler arasındaki yeni bir etkileşim doğmuştur. Siber caydırıcılığın da konvansiyonel

ve nükleer caydırıcılık gibi işlev göreceğine ilişkin somut veriler ortaya konulmaya başlanmıştır.

Siber caydırıcılığa ilişkin somut verilerin Soğuk Savaş sonrasında etkili oluşunda askeri-stratejik ortama ilişkin değişim etkili olmuştur. Tablo 7'de görüleceği üzere özellikle 2010 yılı başlarına kadar konvansiyonel unsurların etkililiğini koruması ve değişkenlerin sadece bu silahların etkinliğinin artırılması üzerine kurulması finansal olarak da kaynakları bu yöne kaydırmıştır. Son yıllarda yaşanan finansal krizler daha az maliyetle caydırıcı olabilme adına siber yeteneklerin ön plana çıkarılmasını bir gereklilik halinden çıkararak zorunluluğa dönüştürmüştür.

Tablo 7. Soğuk Savaş Sonrası Askeri Stratejik Ortamda Değişimler

1990-2001	***2002-2011***	***2012-2015***
Bölgesel Rekabet ve Tehditler	*Terörle Savaş/ Ayaklanmalar*	*Sürekli Gerilim/ Aşırı Şiddet*
Körfez Savaşı/Barışı Koruma Operasyonları	*Afganistan ve Irak Savaşları*	*Sürekli Savaş/Asya Pasifik'e Odak Kayması*
Çeşitli Askeri Operasyonlar	*Artan Operasyon Hızı ve Stres*	*Vekilli Savaşlar/Siber Yetenekler*
Azaltılan Finansal Kaynaklar	*Artırılan Finansal Kaynaklar*	*Azalan Finansal Kaynaklar*
Orduların İnsan Sayısının Artırılması	*Kara Kuvvetleri ve Özel Kuvvet Artışı*	*Küçülen Kuvvet Yapıları/Siber Ordular*
Teknolojiyi Entegre Etme	*Dönüşüm Kabiliyetleri*	*Dengeli Kabiliyet/Teknoloji*
Soğuk Savaş Kabiliyetinin Muhafazası	*Mevcut Kabiliyetleri İdame, Yenileme*	*Envanterden Çıkarma, Sıfırlama ve Yeni Yatırım*

Kaynak: Yılmaz, 2016

Siber yeteneklerin ön plana çıkarılması gelişmiş ülkelerle birlikte tüm ülkelerin öncelikli alanı haline dönüşmüştür. 1990'lı yılların ortalarında Çin, Körfez Savaş'ından çıkarttığı dersler doğrultusunda, kendi stratejisini değiştiren ülkelerin başında gelmiştir ve siber etki açısından Soğuk Savaş sonrasında ciddi anlamda yükselen bir güç olmuştur. Çin de ordusunu küçültüp, yeni teknolojilere yatırım yapan ülkeler arasına girmiştir (Clarke ve

Knake, 2011: 33).[75] Bu gelişmelerle güvenlik ikileminin askeri döngüsü siber savaş alanına kaymaya başlamıştır. İdeolojik yakınlıklar ile birlikte güçsüz ülkelerin birbirlerine olan yaklaşımının yakın gelecekte siber güvenliği canlı tutacağı ve farklı politik birliktelikleri beraberinde getireceği savunulan hususlar arasındadır (Hare, 2010: 216).

2.2. Siber Savaş, İstihbarat ve Uygulamalarına İlişkin Temel Olaylar

Siber uzaya artan bağımlılık ile birlikte, gelişen sistemlerden istifade etmenin yanında sistemlerin çalışmasını engelleyecek karşı girişimler de başlamıştır. İletişim ağını meşgul ederek karşılıklı iletişimi engelleme, zararlı yazılımlarla bilgisayar kayıtlarına zarar verme ve bilgisayar kaynaklarının kullanılması gibi eylemler temel parametreleri oluşturmuştur.

Siber savaş dahilinde gelişen olaylara dair sistem açıklarındaki güvenlik dahilinde, klasik savaşların gidişatını farklılaştırma, hem iç politika hem de dış politikaya ilişkin süreci manipüle etme amacıyla somut örnekler ortaya çıkmıştır. Sayıları hızla artan olaylar arasıdaki bazı temel olaylar bu bölüm dahilinde ele alınmıştır.

2.2.1. Çeçen Savaşı (1994-1996)

Soğuk savaşın bitmesinden kısa bir süre sonra Çeçenler Rusya'ya karşı bağımsızlık mücadelesine başladığında, Rus birlikler 1994 yılında Çeçenistan'ın başkenti Grozni'ye müdahalede bulunmuşlardır. Müdahale başlamadan önce Ruslar, Çeçenlerle başlayacak olan çatışmaların kısa süreceğini düşünmüşlerdir; ancak çatışmalar başladıktan kısa bir süre sonra Çeçen savaşçılar, öldürdükleri Rus askerlerin fotoğraflarını internete yüklediklerinde durum Rus birliklerinin düşündüğü gibi olmamıştır.

İnternette çocuklarının ölü fotoğraflarını gören Rus anneler vakit kaybetmeksizin bir araya gelerek bu çatışmaların durması için kamuoyu yaratmışlardır. Bu durumun faydasını fark eden Çeçen savaşçılar ise interneti her geçen gün daha kapsamlı kullanarak aslında

[75] Çin, ABD gibi 1990'lı yılların sonunda kalitatif askeri eksikliklerini giderme amacıyla siber savaş birlikleri kurmuştur. Çin, son yıllarda uluslararası alandaki mücadelesini deniz kuvvetlerine ve siber savaş alanındaki kuvvetlerine kaydırmıştır.

sosyal medyanın gücünü gösteren ilk olaylardan birini ortaya çıkarmıştır. Bu durum aynı zamanda NATO için önemli bir işaret olmuştur; çünkü statükocu Soğuk Savaş zihniyetinin izlerini taşıyan NATO, yakın zamanda somut bir düşmandan ziyade soyut bir düşman ile karşılaştığında ne yapacağına dair hazırlık yapmamıştır. Takip eden süreçte NATO'nun böylesi bir duruma hazır olmadığı Kosova Savaşı sırasında anlaşılmıştır (Boyraz, 2015).

2.2.2. Kosova Savaşı (1998-1999)

Rus birlikler ile Çeçen savaşçılar arasındaki çatışmadan sadece beş yıl sonra Yugoslavya Federal Cumhuriyeti'nden bağımsızlığını isteyen Kosovalılar ile Yugoslavya kimliği altında bunu durdurmaya çalışan Sırp güçler arasındaki çatışmanın giderek büyük bir felakete dönüşmesi üzerine NATO, 1999 yılının Mart ayında Sırp güçlere yönelik hava saldırılarına başlamıştır. 7 Mayıs 1999 tarihinde, ABD Hava Kuvvetleri tarafından düzenlenen hava saldırısında yanlışlıkla Belgrat'taki Çin Büyükelçiliği'nin vurulması üzerine üç Çinli gazeteci hayatını kaybetmiş, büyükelçilik binası ise hasar görmüştür.

Dönemin ABD Başkanı Bill Clinton, bu olayın bir kaza olduğunu belirtmiş ve Çin resmi makamlarından özür dilemişse de gerek Çin Hükümeti gerekse Çin kamuoyu bu olayın kasıtlı olduğunu düşünmüşlerdir. Takip eden süreçte hükümet destekli Çin Kızıl Hacker Grubu NATO'nun ve ABD'nin birçok önemli internet sitesine siber saldırıda bulunmuştur. Çinli hackerler kadar Sırp hackerler da ciddi siber saldırılarda bulunmuşlardır. Bu saldırılarda NATO'nun merkez karargahında, içinde e-posta sunucusunun da yer aldığı yaklaşık yüz sunucu kilitlenmiştir. Bu sebepten NATO ne kendi içerisindeki online koordinasyonu sağlayabilmiştir ne de üye ülkelerle olan online ilişkisini muhafaza edebilmiştir. Çinli ve Sırp hackerler tarafından, Kosova Savaşı'nda NATO merkezi sistemini hedef alan bu saldırılar NATO'yu doğrudan hedef alan ilk siber saldırılar olarak tarihe geçmiştir (Boyraz, 2015).

Bu saldırılar sonrasında NATO, ABD ve Birleşik Krallık içinde birçok bilgisayar etkilenmiştir. DDoS saldırıları ve farklı virüs çeşitleri bu savaş içinde devreye girmiştir. Daha sonra Birleşik Krallık saldırılardan bir dizi veri kaybının olduğunu kabul etmiştir (Geers, t.y.: 6). Bu gelişmeler sonrasında devletlerin siber saldırılara ilişkin açıklamaları önemli bir gelecek kurgusunun ilk verilerini ortaya çıkarmıştır.

2.2.3. Hainan Adası Olayı

1 Nisan 2001 tarihinde, bir Çin jeti ile ABD casus uçağı Güney Çin Denizi'nde çarpışınca, 80.000'den fazla bilgisayar korsanı *"ABD saldırganlığına karşı kendini savunma hareketi"* başlatmıştır. The New York Times gazetesi tarafından bu olay aynı zamanda *"World Wide Web War I"* olarak adlandırılmıştır (Çifçi, 2012: 164).

Hainan Adası Olayı yaşanan fiziki çarpışmalara veya gelişmelere ilişkin asimetrik bir harekat olarak siber saldırı anlamındaki karşılığa iyi bir örnektir. Konvansiyonel unsurların kendi başına bir baskı aracı oluşturduğuna ilişkin tezi çürüten bir olay olarak tarihe geçmiştir.

2.2.4. Titan Rain

2002 yılından itibaren Çin'de siber saldırılar sıklık kazanmış ve yoğunluktan dolayı Titan Yağmuru olarak adlandırılan *"Titan Rain"* olayı ortaya çıkmıştır. APT kavramı daha da belirgin bir şekilde ortaya çıkmıştır. Bu olayda NASA, ABD askeri kurum ve firmalarına ait bilgisayarlara siber saldırılar düzenlenmiş ve bu sayede 10-20 TB arasında gizli dosya ele geçirilmiştir (Keleştemur, 2015: 142).[76]

2008 yılına gelindiğinde ABD Savunma Bakanlığı, iletişim ağına bağlı bilgisayarlarda 46.880 zararlı faaliyet tespit edildiğini açıklamıştır. Titan Rain saldırıları sadece ABD devlet sitelerini değil, devletle iş birliği içinde bulunan ve önemli teknolojiler üzerinde çalışan özel sektörü de hedef almıştır.

2.2.5. Körfez Savaşı

2003 yılında ABD Irak'ı işgal etmeden önce, Irak'ın kapalı devre bilgisayar ağına sızarak, Irak Savunma Bakanlığı e-posta sistemi üzerinden binlerce Iraklı subaya, savaşa girmeden teslim olmaları için mesajlar gönderilmiştir. Birçok Iraklı subayın bu mesaja

[76] Bu olayın devamında *"Siber Savaş"* ve *"Siber İstihbarat"* kavramlarını ilk kullanan ülkelerin Rusya, Çin ve ABD olduğunu görmekteyiz. Daha sonra bu üçlünün içine Kuzey Kore, Hindistan ve İran gibi ülkeler de girmeye başlamıştır.

uyarak silahlarını bıraktıkları tespit edilmiştir. ABD'li bilgisayar korsanlarının Saddam'ın mali düzenini ele geçirmek için Irak ve başka ülkelerdeki bankacılık sistemlerine saldırmalarına Bush, başka ülkelerin bu eylemleri uluslararası yasaların çiğnenmesi olarak algılayabileceğinden dolayı istememiştir (Çifçi, 2012: 165).

Siber savaşın konvansiyonel savaş ile kullanıldığı ilk harekat olarak adlandırılan Körfez Savaşı aynı zamanda manipülatif girişim ve saldırı tekniğinin psikolojik harbe dönüştürülmesi açısından önemli bir örnektir. Savaşların boyutunun fiziki unsurların ötesine taşındığına ilişkin önemli bir uygulama örneğidir.

2.2.6. Orchyard Operasyonu

6 Eylül 2007'de Suriye topraklarında nükleer silah geliştirdiği iddiası ile bir tesis gece saatlerinde İsrail savaş uçakları tarafından imha edilmiştir. Bu operasyon siber saldırılar neticesinde hava savunma sistemlerine sızılması ile birlikte, çok daha etkili sonuçlar vermiştir. Türkiye'de bu olay, saldırıdan dönen İsrail uçaklarına ait yakıt tanklarının Türkiye sınırlarında bulunması üzerine gündemde olmuştur (Keleştemur, 2015: 144).[77]

Orchyard operasyonu özellikle Orta Doğu'ya ilişkin siber savaş taktikleri ve bölgesel baskınlık anlamında bir gözdağı olmuştur. Özellikle İsrail'in istenildiğinde siber strateji açısından vermiş olduğu mesaj süreç itibariyle etkisini göstermiştir (Follath ve Stark, 2009: 11). Siber saldırıların artık basit yazılımlarla dahi yürütülebildiği bir ortamda Orchyard Operasyonu özgün bir örnektir. Bilgi güvenliğinin sadece bilgisayarlarla sınırlandırılamayacağı hususunda bir farkındalık oluşturan bu operasyon farklı komplo teorileri ile adından söz ettirmiştir.

2.2.7. Estonya Siber Savaş Alanı

Estonya Siber Savaşı olarak da bilinen olayın temeli II. Dünya Savaşı yıllarına kadar dayanmaktadır. Estonya'nın Nazi istilasından korunması maksadıyla, SSCB'nin verdiği

[77] Suriye'nin kullandığı Rus yapımı sistemlerdeki bilgisayar programına, İsrail hesabına çalışan biri tarafından Truva atı adı verilen tuzak programı yerleştirilmiş ve heronlardan gönderilen bir sinyal sayesinde, bu tuzak kapısı etkinleşerek radar ekranlarında bir şey görünmemesi sağlandığı görüşü ağır basmaktadır.

mücadeleyi sembolize eden *Bronz Asker Anıtı*'nı 2007'de yerinden kaldırmasıyla olaylar büyümüştür. Rusya yanlısı gösteriler sürerken 27-29 Nisan 2007 tarihinde özellikle Estonya devlet sitelerinin ele geçirilmesi sebebiyle ulusal bilgi sistemleri çökmüş ve internet hizmet sağlayıcıları ve bankalar ciddi zararlar görmüştür (Keleştemur, 2015: 144). Her ne kadar Rusya hükümetinin olaylarla kesin ilişkisi olduğu saptanamasa da, *Russian Nashi* genç liderlerinden olan Konstantin Goloskokov, Duma üyesi Sergei Markov ile irtibatını daha sonra itiraf etmiştir.

Estonya'ya gerçekleştirilen saldırı dünyanın siber tehdit efsanelerini dikkate almasını sağlamıştır. Ülkeler kendi varlıklarını koruma adına daha etkin teknik ve hukuksal önlemler almaları gerektiğini görmüşlerdir. NATO, BM, Avrupa Birliği ve AGİT gibi birçok uluslararası örgütün güvenlik politikaları bu başlık altında revize edilmiştir (Yılmaz ve Sağıroğlu, 2013a: 159).

2.2.8. Gürcistan ve Rusya Mücadelesi, Güney Osetya'ya Müdahele

2008 yılında, Güney Osetya Savaşı zamanında, Gürcistan internet altyapısı çökertilmiş ve devlete ait web sitelerine saldırılarak propaganda görüntüleri yerleştirilmiştir. Gürcistan'ın devlet web siteleri ile birlikte, ABD ve İngiltere büyükelçiliklerinin web siteleri de siber saldırıya uğramıştır. Gürcistan, siber saldırıları durdurmak içi Rusya'dan gelen internet trafiğini bloke etse de farklı ülkelerdeki köle bilgisayarları kullanarak saldırıları devam ettirmişlerdir (Çifçi, 2012: 168).[78]

Gürcistan'a yönelik olarak düzenlenen siber saldırılardan çıkartılabilecek en önemli sonuç bunun gerçek bir hibrit savaş niteliği taşımasıdır. Geleneksel savaş yöntemini kullanan Rusya, eş zamanlı olarak siber saldırıları da başlatmıştır. Rusya'nın uyguladığı bu savaş düzenini hibrit savaş olarak tanımlamak mümkündür. Olayın bu şekilde gelişmesi NATO'nun da hibrit savaşa olan inancını desteklemiştir. Ancak siber savaş konusunda NATO'nun kavramsal tercihi *"Cyber Security"* olmuştur (Bıçakçı, 2012: 219).[79]

[78] Ruslar *www.stopgeorgia.ru* sitesini kurarak, herkesi gönüllü olarak saldırı yapmaya davet etmiş ve sıradan bilgisayar kullanıcılarının bile saldırı yapabilmesini sağlayan programları kullanıma açmıştır.

[79] Rusya'nın 2008 yılında Gürcistan'a ve 2014 yılında Ukrayna'ya olan müdaheleleri hibrit savaşın teoriği açısından öne çıkan olaylar olmuştur. Siber alanın etkisel yönünde, hem teknik boyuttaki müdahele hem de psikolojik harekat iki olay açısından özgün örneklerdir (Hunter ve Pernik, 2015: 3).

2.2.9. Conficker

Microsoft işletim sistemlerini hedef alan *Conficker* isimli solucan ilk olarak Kasım 2008 yılında tespit edilmiştir. Hızlı bir şekilde yayılan solucan kısa bir süre içinde dünya genelinde milyonlarca bilgisayara bulaşmıştır. Solucan, sadece askeri ve devlete ait bilgisayarları değil, bireysel kullanıcılar için de zararlı olmuştur (Keleştemur, 2015: 145). Conficker'ın halen en az 3 milyon bilgisayarı etkilediği yetkili kişiler tarafından dile getirilmektedir. Birçok uzman Conficker'ın saldırı çeşitlemesi açısından ilk evrelerde olduğunu belirtmesi düşündürücüdür (Krebs, 2009: 1).

Conficker virüsünün Çin hükümeti tarafından siber savaş testi yapma amacıyla yazıldığı da bir dönem tartışılmıştır. Kaspersky uzmanı olan Eugene Kaspersky bu solucanın Ukrayna kaynaklı olduğunu belirtmiştir. Conficker, güvenlik uzmanlarına göre arkasında 9.1 milyar dolarlık bir hasar bırakmıştır. Solucan hala aktiftir ve zararını devam ettirmektedir.[80]

2.2.10. Cast Lead Harekatı

2008 yılının sonlarına doğru İsrail, Gazze Savaşı sırasında Filistin'e *Cast Lead* isimli bir harekat başlatmıştır. İsrail savunma güçleri, Hamas'a ait Al Aqsa kanalını hacklemişler ve Hamas liderinin öldüğünü ilan etmişlerdir. Filistinli siber korsanlar ise İsrail'e ait birçok web sitesine saldırmış ve binlercesini hacklemiştir. Ele geçirilen web sitelerinin büyük bir kısmında İsrail aleyhine yazılar ve görseller yayınlanmıştır (Keleştemur, 2015: 145).

İsrail ve Filistin arasında, özellikle bu harekattan sonra siber savaşın başladığına dair ve mücadelenin yıpratmaya dönük boyutu gün yüzüne çıkmıştır. Psikolojik harekat açısından önemli bir yere sahip olan manipülasyon ve siber saldırılar bu gelişme sonucunda bir kez daha önemini artırmıştır. Psikolojik boyut açısından bir etki aracına dönüşen siber harekatlar sistematik bir saldırı yapılanmasını gerekli kılmıştır.

[80] 3 milyon 500 binden fazla IP'de Conficker tespit edildiği ancak birçok bilgisayar ağının dışarıya tek IP ile çıkış yaptığı düşünüldüğünde rakamın daha büyük olabileceği ortaya çıkmaktadır. Yayılmanın en büyük sebebi olarak kurumların prestijlerini korumak adına olayı gizlemesi, kişisel kullanıcılarınsa olayın farkında olmaması ya da virüsü temizleyecek bilgiye sahip olmaması gelmektedir.

2.2.11. GhostNET

2009 yılında ortaya çıkarılan bir olayda, 103 ülkeden çok sayıda bilgisayardan veri çalabilen, bilgisayarların mikrofon ve kameralarını açarak ses ve görüntü aktarabilen bir casus yazılım ortaya çıkarılmıştır. *GhostNet* adı verilen bu sistemin özellikle elçilik ve devlet kurumları bilgisayarlarına yüklendiği belirlenmiş, bilgilerin Çin'e gönderildiğine ilişkin tespitler yer almıştır (Çifçi, 2012: 172).

2007 ile 2009 arasında 22 aylık bir süreçte aktif olduğu düşünülen casus yazılım büyükelçilikler, dışişleri bakanlıkları gibi devletler arası ilişkilerin yönetildiği kurumları hedef aldığı ve 103 ülkede aktif olduğu ortaya çıkmıştır (Kaminski, 2010: 82). Çin hükümeti bu saldırıların yürütüldüğünden haberdar olmadığını belirtmiştir. Barbados, Malta, Portekiz ve Hong Kong gibi ülkelerden çalınmak istenilen verilerin hangi stratejik amaçlarla kullanılacağı açıklığa kavuşturulamamıştır. [81]

2.2.12. Stuxnet Olayı

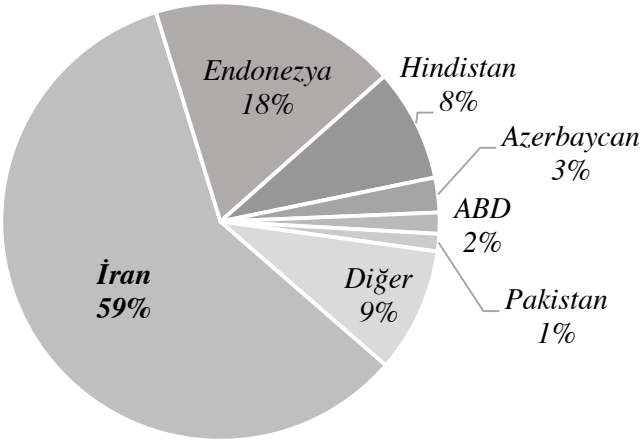
Stuxnet adlı bir solucanın Haziran 2010'da, İran'ın nükleer tesislerine sızıp etki yaptığı, nükleer çalışmaları sekteye uğrattığı rapor edilmiştir. Bu solucan özellikle Siemens üretimi kumanda sistemlerini etkilemiştir. Stuxnet solucanı siber saldırıların etkileri açısından en önemli olaylardan biridir ve SCADA endüstriyel kontrol sistemleri hedef alınmıştır.[82]

Virüsün varlığı ve saldırı hakkında ayrıntılı bilgiye saldırıdan yaklaşık bir sene sonra ulaşılabilmiştir. Stuxnet basitçe bir bilgisayar virüsü olarak anılsa da, esasen uzaktaki bilgisayar sistemlerine nüfuz etmesi ve bunları kontrol altına alması için tasarlanmış son derece kompleks bir bilgisayar programıdır (Çelik, 2013: 146). Temel olarak etkilediği altyapı SCADA vasıtasıyla birbirine bağlı olduğu için Grafik 11'de görüldüğü üzere başta İran olmak üzere, Endonezya ve Hindistan gibi birçok ülke bu olaydan etkilenmiştir.

[81] Bu olay dahilinde, Tibet'in sürgündeki lideri Dalai Lama'nın Hindistan, Brüksel, Londra ve New York'taki ofislerine ait bilgisayarların hemen hepsine sızılmıştır. Uluslararası güvenlik kurumları konuyla ilgili soruşturma başlatmıştır.

[82] SCADA, enerji üretim ve dağtımının kontrolü; su, doğal gaz, kanalizasyon sistemleri gibi kritik altyapıların kontrol edilmesi ve izlenmesinde kullanılmaktadır.

Grafik 11: Stuxnet'ten Etkilenen Ülkeler



Kaynak: Çifçi, 2012: 174

Stuxnet, sadece bilgisayarların değil, endüstriyel kontrol sistemlerinin ve dış dünyaya kapalı sistemlerin hedef alınması ve bunda başarılı olunması açısından çok önemli bir yere sahiptir. Stuxnet olayından sonra İran'da ciddi bir kurumsal yapılanma başlamış ve 2012 yılında ABD'ye karşı gerçekleştirilen saldırılarda İran'ın parmağı olduğu ileri sürülmüştür (Çifçi, 2012: 176).

2.2.13. Aurora Operasyonu

12 Ocak 2010 tarihinde Google, kendilerini ve bazı firmaları hedef alan oldukça karmaşık, koordineli siber saldırılara maruz kaldıklarını duyurmuştur. Bu saldırıların Çin tarafında kaynaklandığını ve sonucunda firmalardan bilgi sızdırıldığı açıklanmıştır. Yapılan siber saldırıda Microsoft internet tarayıcısı Internet Explorer'da var olan ve anti virüs tarayıcıları tarafından tespit edilemeyen sıfırıncı gün açıklığı[83] ile sistemlerine sızdıkları açıklanmıştır (Emre, 2012). Bu olay üzerine Google firması, Çin kaynaklı siber saldırıların kurbanı olduğunu ve Çin'deki şubesini kapatabileceğini duyurmuştur.

Operation Aurora gibi saldırıların gelecekte önlenmesi adına *Communitarian Policy Studies Enstitüsü*'nden Amitai Etzioni, Çin ve ABD gibi ülkelerin siber uzaya saygı

[83] Sıfır gün güvenlik açığı saldırısı (ZETA), yazılımda bir zayıflığın keşfedildiği gün gerçekleşir. Bu noktada, geliştirici tarafından bir düzeltme sunulamadan önce bu zayıflıktan faydalanılır.

duyulması adına mutabık olmalarını vurgulamıştır. Her iki ülkenin kendi savunmalarını oluştururken saldırı adımlarının da hesaplanması gerektiği konusunda ortak kaygılar dile getirilmiştir.

2.2.14. Night Dragon

2011 yılında enerji raporlarının sızdırılmasına ilişkin bu saldırıda petrol ve enerji firmalarından veri çalmayı amaçlayan siber casusluk saldırıları gerçekleştirilmiştir. Bu saldırıların arkasında Çin'in olduğu iddia edilmiştir. Öncelikle hedef alınan şirketin web sitesindeki açıklık kullanılarak içeri girilmekte, ele geçirilen bilgisayarlara casus yazılım yüklenmekte ve bu yolla diğer bilgisayarlara da ulaşılarak veriler çalınmaktadır (Çifçi, 2012: 176).

McAfee Uzmanı Dmitri Alperovitch mevcut kritik altyapı sistemlerinin bu saldırılardan oldukça etkilendiğini belirtmiştir. Çinli korsanların amaçlarına ulaşamadığı fakat başarı gösterdikleri belirtilmiştir. Bu olayda sadece bilgisayar sistemlerine sızmakla yetinilmemiş, Yunanistan, Tayvan, Kazakistan ve ABD'de bulunan üst düzey yöneticilere ve kurum çalışanlarına ait bilgilere de ulaşılmıştır.

2.2.15. RSA Saldırısı

Mart 2011'de, *RSA Security* adlı ABD kökenli güvenlik firması kapsamlı ve karmaşık bir saldırıya uğradığını duyurarak olaylar silsilesi başlamıştır. ABD'nin en saygın güvenlik firmalarından olan RSA, ürettiği parolaya ilave olarak kullanılan güçlü bir kimlik doğrulama mekanizması olan SecurID adlı ürünü zafiyete uğratabilecek kritik verilerin çalındığını belirtmiştir (Çifçi, 2012: 177).

Bu saldırı sayesinde istenilen bilgiler elde edildikten sonra, hiçbir şey olmamış gibi yeniden anlık verileri, eski hallerine getirmek mümkün olabilmiştir. Böylelikle ABD'nin internet alt yapısını kullanan tüm verilere ulaşmak, hepsine zarar verebilmek mümkün olabilmiştir.[84]

[84] Güvenlik alanında ciddi bir gelişime sahip olan firmaların özellikle bu tür olaylardan etkilenmesi savunma adına siber savaşın ne kadar anlık ve kolay kazanılabileceğini gözler önüne sermiştir.

2.2.16. Wikileaks Krizi

28 Kasım 2010 itibariyle ABD büroktratlarının birbirleriyle olan yazışmalarından oluşan belgeleri yayınlamaya başlayan Wikileaks oluşumu, ABD başta olmak üzere devletlerin gizli politikalarını dünya kamuoyu ile paylaşmayı amaçlamıştır. Bu belgeler devletlerin ulusal ve uluslararası gündemini uzun bir süre meşgul etmiştir. Her ne kadar etkileri azalsa da yayınlanan her yeni belge, dünya siyasetinde önemli bir yer tutmaya devam etmektedir (Turgut, 2011: 1).[85]

Olayların gelişimi itibariyle Anonymus, Wikileaks'e destek vermek amacıyla Mastercard, Paypal, Visa ve çeşitli devlet kurumlarının sitelerini hedef alan, karşı bir saldırı başlattığını duyurmuştur. Anonymus, gönüllü olarak herkesin bu saldırıları desteklemelerini istemiştir (Keleştemur, 2015: 148). Farklı grupların ve yapılanmaların gerek ABD, gerekse karşıt gruplar arasındaki mücadelesi önemli gelişmeler arasında yer almıştır. 1968-2010 yılları arasında yapılan yaklaşık 250.000 yazışmanın internete sızdırılması ve bunun duyurulmasını engellemek için Wikileaks sitesine karşı DDoS saldırıları düzenlenmeştir. Bu saldırılarla birlikte gündem bir anda değişmiştir.

Özellikle Wikileaks sonrasında dünyanın birçok ülkesi siber savunma konusunda ciddi yapılanmalara, düzenlemelere giderken, politika ve strateji geliştirme çalışmaları başlamıştır. Devletlerin özel verilerine ilişkin siber uzayda yer alan her verinin potansiyel bir manipüle aracı olduğu ve tehlikesi şiddetini daha çok belli hissettirmiştir.

Türkiye açısından, Ankara merkezli belgeler de oldukça yoğun bir şekilde Wikileaks belgeleri içerisinde yer alırken, siyasi ortam ve gelişmeler gündemde fazlaca yer edinmesini engellemiştir. Wikileaks internet sitesinin verdiği bilgilere göre, Türkiye 7918 belgeye kaynaklık etmektedir. İddialar incelendiğinde, bunların Türkiye'nin hem iç hem de dış politikasını etkileme potansiyeli taşıdıkları da ileri sürülebilir. Belgelerde Türk hükümetinin İslami kimliğine, İsrail ve ABD'li büroktratların Türkiye'de İslam'ın yükselişi ile ilgili

[85] Wikileaks belgelerinin ortaya çıkması farklı tartışma konularını beraberinde getirmiştir. Hızla gelişen iletişim teknolojisinin, kişilerin ve devletlerin gizli hayatlarını açığa çıkarmak amacıyla kullanılmaması gerektiğini ileri sürenler olmuştur. Diğer yandan halkların, devletlerin politikaları konusunda bilgi sahibi olmalarının engellenmesi gerektiğini iddia edenler, Wikileaks belgelerinin açığa çıkmasının uluslararası ilişkiler ve devlet-toplum ilişkileri açısından bir dönüm noktası olduğunu savunmuştur.

duyduğu endişeye ve Türk hükümeti liderleri üzerine görüşlerine, Türkiye'nin dış politika uygulamalarına ve Türkiye-İsrail, Türkiye-İran ve Türkiye-Azerbaycan ilişkileri gibi Türkiye'nin yakın çevre ülkeleriyle ilişkilerine yönelik konu başlıkları bulunmaktadır (Turgut, 2011: 20).

2.2.17. Panama Belgeleri

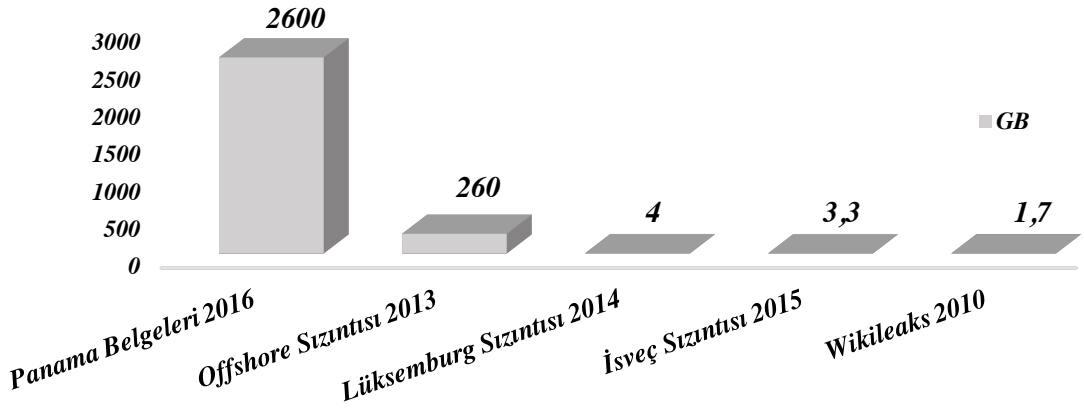
Panama merkezli Mossack Fonseca firmasının 1977'den bu yana tuttuğu müşteri kayıtlarına ulaşarak yayınlamaya başlayan *Uluslararası Araştırmacı Gazeteciler Konsorsiyumu (ICIJ)*, pek çok kişi, banka ve şirketin vergilendirilebilir gelirlerini gizlediğini ortaya çıkarmıştır. Henüz bir kısmı paylaşılan belgeler Avrupa ve dünya siyasetinde önemli bir yer tutmuştur. Vergi kaçakçılığıyla AB çapında mücadele yürütmesi beklenenlerin, vergi hileleriyle anılan üyelerin, hükümet mensupları olduğunun Panama belgeleriyle ortaya çıkması, vergi kaçakçılığıyla etkin şekilde mücadele edilememesinin nedenini kısmen de olsa açıklamıştır (Bilgen, 2016: 1).[86]

Açıklanan ilk belgeler arasında Rusya Devlet Başkanı Vladimir Putin'i, Ukrayna Cumhurbaşkanı Petro Poroşenko'yu, İzlanda (eski) Başbakanı Sigmundur Gunnlaugsson'u, İspanya (eski) Sanayi Bakanı José Manuel Soria'yı, İngiltere Başbakanı David Cameron'ı ve Fransa'daki Ulusal Cephe'nin lideri Marine Le Pen'i ilgilendiren belgeler bulunmuştur. Siyasetçilerin yanında kendini savunmak zorunda kalan ünlülerin hemen hepsi hukuksuz bir iş yaptığını inkar etmiş ve bunun bir itibarsızlaştırma kampanyası oluduğunu vurgulamışlardır.

Panama belgeleri tarihi olarak sahip olduğu kapsam ve içerik olarak yapılan inkarlarla birlikte tarihe geçmiştir. Mossack Fonseca'ya ait toplam 2.6 TB'lık yaklaşık 11.5 milyon belgenin gözler önüne serildiği içerik, Grafik 12'de görüldüğü üzere, daha önceki Wikileaks, Offshore Sızıntısı, Lüksemburg Sızıntısı ve İsveç Sızıntısı'na ait belgelerin toplamından daha da büyüktür.

[86] Panama belgeleri skandalı, küresel şirketlerin karlarını artırmak için maliyetleri düşürmek ve tüketimi artırmak gibi geleneksel yollardan daha fazlasına başvurduklarını göstermiştir. Panama belgeleri elde edilen kazancın bir şekilde vergiden muaf tutulabilmesini içeren son bir aşama daha olduğunu ve bu aşamanın nasıl gerçekleştiğini dünya kamuoyuna somut biçimde göstermiştir.

Grafik 12: Panama Belgelerinin Boyutu



Kaynak: Kılıç, 2016

Belgelerin uluslararası alanda birtakım siyasi sonuçları da olmuştur. Belgelerle birlikte kendisi ve eşinin denizaşırı şirket sahibi olduğu ortaya çıkan İzlanda Başbakanı Gunnlaugsson, ülkedeki protestoların ardından istifa etmek zorunda kalmıştır. Rusya Devlet Başkanı Putin'in, yakın arkadaşı üzerinden denizaşırı banka hesapları üzerinden vergi kaçırmak amacıyla gerçekleştirilen 2 milyar dolarlık para transferi ile bağlantılı olduğu iddiaları Kremlin'i zor durumda bırakmıştır. Çin'de ise Devlet Başkanı Şi Cinping'in ailesi ile çıkan belgeler üzerine Panam belgeleri ile ilgili haberler sansürlenmiştir (Kılıç, 2016). Bu gelişmelerle birlikte kendi ülkelerinde liderler kısmen de olsa güven kaybı yaşamışlardır.

2.2.18. Rusya'nın Ukrayna Müdahelesi

2014 Şubat'ında Rusya'nın Kırım'a müdahelesiyle başlayan olaylar, uluslararası toplumun tepkisini çekmesine rağmen Doğu Ukrayna'da yeni bir güvenlik tasarımı peşinde olan Rusya'nın faaliyetlerini bölgede artırmasıyla siber alana da taşmıştır. Rusya'nın Kırım'a müdahelesi itibariyle hedeflenilen durumun hem coğrafi açıdan, hem de iletişim ve siber ortamda dış dünyadan tecrit edilmesi olduğu gözlenmiştir.

Ukrayna iç güvenlik birimi SBU'nun başkanı Valenty Nalyvaichenko tarafından Şubat ayı sonuntan itibaren Ukrayna mobil telefon iletişim altyapısı ile internet altyapısının

saldırıya uğradığı ve bu alt yapıların büyük oranda çöktüğü, özellikle Ukraynalı bürokratlarla Ukrayna Parlamentosundaki milletvekillerine ait akıllı cep telefonlarının tamamının hedeflenerek hacklendiği ifade edilmiştir (Gürcan, 2016). Rusya'nın hedefi temel olarak ilk aşamalarda iletişim ağlarının zayıflatılması olmuştur. Ukrayna ise karşılık olarak Rusya'ya ait en büyük haber ajanslarından olan RT'nin sitesini kapatmıştır. İlerleyen süreçte yazılımlar ve sistemler üzerinden bürokratların, askerlerin ve Rusya aleyhine yazan gazetecilerin yazışmalarını ele geçiren Rusya, sık sık DDoS saldırıları ile Ukrayna'nın siber alanına müdahelede bulunmuştur.[87]

2016 yılı başlarında Ukrayna'nın başkenti Kiev'deki havaalanının bilgisayar sistemlerinde tespit edilen virüsün de Rusya kaynaklı olduğu duyurulmuştur. Ukraynalı yetkililer, Borsipil Havalimanı'nın, kontrol kulesi dahil olmak üzere iletişim sistemlerinde saptanan virüsün siber saldırı neticesinde Rusya Federasyonu merkezli olduğunu belirtmişlerdir. Zaman zaman yaşanan elektrik kaynaklarındaki problemlerin de benzer saldırılar sonucu Rusya Federasyonu kaynaklı olduğu Ukrayna'da ısrarla yinelenmektedir.[88]

2.2.19. ABD Başkanlık Seçimleri ve Rusya Krizi

ABD'de, 8 Kasım 2016'da düzenlenecek Başkanlık seçimi öncesi Demokrat Parti'den başkan adayı Hillary Clinton'ın kampanyası için kullanılan bilgisayarların Rus istihbarat servisleri tarafından saldırıya uğradığı iddiaları krize dönüşmüştür. Kremlin, Rusya'ya yöneltilen siber saldırı suçlamalarının, ABD seçim kampanyasının yerel kuvvetler tarafından manipüle edildiği gerçeğini gizlemek için tasarlanmış örtbas etme çabası olarak yorumlamıştır.[89] Böylece ABD ve Rusya arasında uzun süredir devam eden tartışmalara bir yenisi daha eklenmiştir.

---

[87] Daha önce Ukrayna ve Polonya'daki devlet kuruluşlarını hedef alan *BlackEnergy* siber saldırısını tespit eden ESET firması, 2015 yılı içinde Ukrayna hükümeti, askeri kuruluşları ve çeşitli Ukrayna haber ajanslarına odaklanan bir Truva atını tespit etmiştir. *Potao* adı verilen bu Truva atı, bir casusluk yazılımı işlevi görmektedir.

[88] Özellikle Rusya ve Ukrayna arasında gelişen sıcak gelişmelerden sonra NATO; Estonya, Letonya, Litvanya ve Polonya'daki dört tabur konuşlandırma kararının yanı sıra, siber savunmayı da operasyonel alan olarak değerlendirmeye almıştır.

[89] Kremlin Basın Sözcüsü Dimitri Peskov düzenlediği basın toplantısında, Clinton'un *"Saldırıların ardında Rusya var."* şeklindeki suçlamalarına *"somut bir içeriği olmayan, duygusal bir seçim öncesi retoriği"* şeklinde cevap vermiştir.

Wikileaks kurucusu Julian Assange, ABD başkan adayı Hillary Clinton'ın *Demokratik Ulusal Komite (DNC)* ve seçim kampanyalarına yönelik siber saldırılar karşısında Rusya ile ilgili yaptığı açıklamalara yönelik, Wikileaks dışında üçüncü bir aktörü devreye sokma çabası olduğunu belirtmiştir. Assange, Clinton'un açıklamalarının yayınlanan e-postaları eritme amaçlı olduğunu vurgulamıştır.

2.3. Örgütler ve Devletler Bazında Siber Güvenlik Yapılanmaları

Uluslararası sistemin getirmiş olduğu çok boyutluluk, orduların kabiliyetlerini ve ilgi alanlarını da değiştirmiştir. Komuta kontrol sistemleri, silah sistemleri, istihbarat, keşif ve gözleme sistemleri, muharebe sistemleri gibi sistemlerin tamamı elektronik ortamda ve iletişim altyapısı üzerinde çalışır hale gelmiştir. Gelişen olaylar ve siber savaşa ilişkin karakteristik ilerlemelerle birlikte örgütler ve devletler farklı yapılanmalar tercih etmişlerdir.

Siber güvenlik alanında, strateji geliştirme adına askeri nitelikli kurumlar oluşturmaya çalışan ülkelerin bir kısmı, internet altyapısının gelişmiş olmasıyla strateji oluşturma mantığını birbirine karıştırır hale gelmiştir. Ekonomik gelişmişlik ile telekomünikasyon sisteminin ileri bir yapıda olması, devletlere kurumsal nitelik anlamında stratejik bir ajanda sunmamaktadır (Spidalieri, 2015: 5).

Tercih edilen yapılanmalar yanında hukuki boyuta ilişkin, iç ve dış politikayı şekillendirecek, karar alıcıları doğru yönlendirecek temellerin oluşturulması adına devletler birtakım stratejik belgelere de imza atmıştır. Başta NATO ve bünyesindeki devletler olmak üzere oluşturulan belgelerde, iç güvenliğin ve bilişim alanındaki suçların önlenmesi adına stratejik bir ajanda çıkarmaya çalışan ülkeler, uluslararası kuruluşlarla da koordineli olma adına adımlar atmaya çalışmıştır. Tablo 8'de görüldüğü üzere siber güvenlik strateji belgeleri ortaya koyan ülkeler, siber alanda gelişmişlikten daha çok siber savunma gereksinimi duyan ve bu konuda farklı tecrübeler yaşayan ülkelerden oluşmaktadır. Dikkat çeken hususlardan diğeri siber güvenlik strateji belgeleri ortaya koyan ülkelerin birçoğunun teorik olarak hazırladıkları ajandaların pratiğe uyarlanamamasıdır. Siber güvenlik alanının teknik ve politik yönüyle harmanlandığı günümüz gelişmeleri, stratejik uyum ile teknik uyumu yakalayan ülkelerin bu konuda daha başarılı olduklarını ortaya koymaktadır ve bu konuda bir vizyon çerçevesi ortaya koymaktadır.

Tablo 8: Ulusal Siber Güvenlik Strateji Belgelerine İlişkin Örnek Ülkeler[90]

Devlet	*Yayın Tarihi*	*Öncülük Eden Kurum/Kişilik*	*İngilizce Versiyon*
ABD	2003 Şubat	White House	*The National Strategy to Secure Cyberspace (CNCI, HSPD-7, 60 day Review)*
Almanya	2011 Şubat	Federal Ministry of The Interior	*Cyber Security Strategy for Germany*
Avustralya	2009 Kasım	Attorney-General	*Cyber Security Strategy*
Birleşik Krallık	2011 Kasım	Cabinet Office	*The UK Cyber Security Strategy. Protecting and promoting the UK in a digital world*
Çek Cumhuriyeti	2011 Temmuz	Ministry of Interior	*Cyber Security Strategy of the Czech Republic for the Period 2011-2015*
Estonya	2008 Eylül	Ministry of Defence	*Cyber Security Strategy*
Fransa	2011 Şubat	General Secretariat for Defence and National Security	*Information Systems Defence and Security. France's Strategy*
Güney Afrika	2012 Mart	Department of State Security	*Notice of Intention to Make South African National Cyber-security Policy*
Güney Kore	2011 Ağustos	Korea Communications Commision	*Çevrimiçi olarak hiçbir versiyon yer almamaktadır.*
Hindistan	2011 Nisan	Ministry of Communications and Information Technology	*Discussion Draft on National Cyber Security Policy*
Hollanda	2011 Şubat	Ministry of Security and Justice	*The National Cyber Security Strategy (NCSS). Strength through Cooperaiton*
İspanya	2011 Mayıs	Spanish Government	*Part of Spanish Security Strategy: Everyone's responsibility*
İsviçre	2012 Haziran	Federal Department of Defence, Civil Protection and Sport	*National Strategy for Protection of Switzerland against Cyber Risks*
Japonya	2010 Mayıs	Information Security Policy Council	*Information Security Strategy for Protecting the Nation*
Kanada	2009 Ekim	Public Safety Canada	*Canada's Cyber Security Strategy: For a Stronger and More Prosperous Canada*
Litvanya	2011 Haziran	Government of The Republic of Lithuania	*Programme for The Development of Electronic Information Society (Cyber Security) for 2011-2019*

[90] *Sıralama ülkelerin isimlerine göre, alfabetik olarak yapılmıştır.*

Tablo 8 (Devamı)

Devlet	***Yayın Tarihi***	***Öncülük Eden Kurum/Kişilik***	***İngilizce Versiyon***
Lüksemburg	2011 Kasım	Government of The Grand Duchy of Luxembourg	*İngilizce çevrimiçi olarak yer almamaktadır.*[91]
Romanya	2011 Mayıs	Ministry of Communications and Information Society	*İngilizce çevrimiçi olarak yer almamaktadır.*[92]
Slovakya	2008	Ministry of Finance	*Slovak National Strategy for Information Security*
Türkiye	2013 Haziran	Ministry of Transport, Maritime Affairs and Communications	*National Cyber Security Strategy and 2013-2014 Action Plan*[93]
Uganda	2011 Kasım	Ministry of Information and Communication Technology	*National Information Security Strategy*
Yeni Zelanda	2011 Haziran	Ministry of Economic Development	*New Zealend's Cyber Security Strategy*

Kaynak: Lindstrom ve Luiijf, 2012: 53

Elektronik ortama ve iletişim altyapısına olan bağlılık ise askeri harekatlarda bulunabilecek örgütleri ve onların özelindeki devletleri kendi iç yapılarında çeşitlendirmeye götürmüştür. Çalışmanın bu bölümünde siber alanda faaliyetlerini artıran uluslararası yapılanmalar olarak NATO ve AB ile belli bazı devletlerin atmış olduğu adımlar temel nitelikleriyle irdelenmiştir.

2.3.1. NATO

Soğuk Savaş'ın sona ermesiyle birlikte, NATO üyeleri kendilerini mücadeleden galip çıkmış olarak tanımlamıştır. Soğuk Savaş döneminin güvenlik yapılanmasının başlıca ürünü olan NATO kendisini yeniden tanımlama ve yapılandırma ihtiyacı duymuştur. NATO'nun 1991 yılında yayınlanan strateji belgesinin önemli bir kısmında ortadan kalkan tehditler yer almıştır (Bıçakçı, 2012: 206). NATO bu belgede, birbiri ardına gelen

[91] Fransızca versiyon olarak anadilinde adı*: "Stratégie nationale en matiére de cyber sécurité"*.
[92] Rumence versiyon olarak anadilinde adı: *"Strategia de securitate cibernetica a Romaniei"*.
[93] Türkiye adına *2013-2014 Siber Güvenlik Eylem Planı*, tabloya yazar tarafından eklenmiştir. Belgenin Türkçe ve İngilizce olarak tam metnine, TC Ulaştırma Denizcilik ve Haberleşme Bakanlığı'nın çevrimiçi sitesinde yer alan *"http://www.udhb.gov.tr/h-12-siber-guvenlik.html"* bağlantısından ulaşılabilir. Yalnızca Türkçe versiyonunun yayınlandığı *2016-2019 Ulusal Siber Güvenlik Strateji Belgesi*'ne aynı bağlantıdan erişilebilir.

çözülmeler nedeniyle tehditlerin ortadan kalkışının yarattığı güvenlik ortamının sürdürülmesi konusundaki kararlılığını ortaya koymuştur. Yeni politik yapılanmaların oluşması sürecinde, Soğuk Savaş'ın dondurduğu çatışmaların yeniden ortaya çıkması ihtimali üzerinde durulmuştur.

NATO siber savunma ve bilgisayar olaylarına müdahele yeteneğinin, kurulucak bir teşkilat ve NATO kaynaklarının kullanılacağı bir proje ile ele alınması fikri ilk olarak, 2002 yılında Prag'daki NATO zirvesinde ittifak gündeminde yer almıştır. Siber savunma yeteneklerinin uygulanması adına bir çok faaliyet hayata geçirilmeye başlanmıştır. Bu faaliyetlerden en önemlisi *NCIRC (NATO Bilgisayar Olaylarına Müdahele Yeteneği)* programıdır. Bu program dahilinde üç aşamalı bir yetenek geliştirme yaklaşımı benimsenmiştir (Çifçi, 2012: 52):

- *Birinci Aşama (2003-2006): NCIRC'nin başlangıç seviye yeteneklere kavuşturulması.*
- *İkinci Aşama (2006-2012): Bilgi güvenliğine yönelik projelerin geliştirilmesi ve harekat yeteneğinin kazanılması.*
- *Üçüncü Aşama (2012-…): Yasal mevzuat ve kaynak konularını da içeren geniş çaplı siber savunma çözümlerinin hayata geçirilmesi.*[94]

Siber savunma fonksiyon yapısıyla dikkat çekici bir konuma gelen NATO'da özellikle saldırıların teknik boyutuyla ilgili de uzmanlaşmaya gidilmiştir. Şekil 20'de görüldüğü üzere özellikle teknik merkezin, koordinasyon merkezi ile iş birliği içinde olması ve atılacak politik adımlarda bir kanat olarak yer alması kayda değer bulunmuştur. Siber savunma fonksiyon yapısı açısından önemli bir dinamik haline gelen CDMA, çalışmaların niteliklerine ivme kazandırmıştır.

---

[94] *BİLGESAM, Dış Politika ve Savunma Araştırmaları Grubu* (2010), genel anlamda NATO'nun kuruluşundan günümüze kadar geçen dönemde, ittifakın stratejik yaklaşımının dört belirgin evreden geçtiğini belirterek siber güvenlik anlamındaki değişimle neredeyse paralel bir gruplandırma yapmıştır. Bu evreler şu şekilde belirtilmiştir:

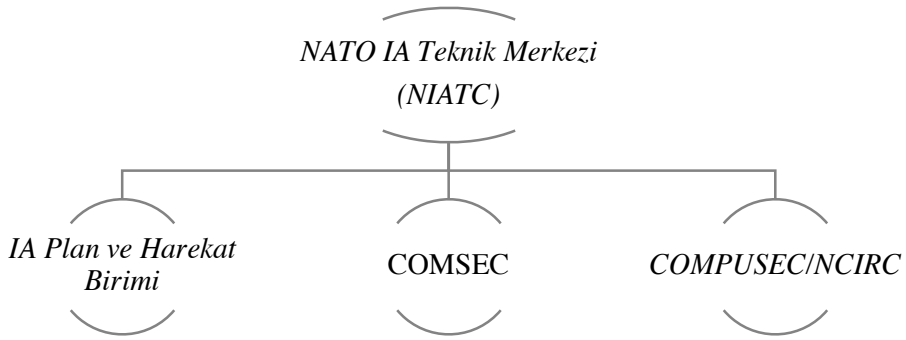
- *Soğuk Savaş dönemi (1949-1991),*
- *Soğuk Savaş sonrasındaki dönem (1991-2001),*
- *11 Eylül 2001 sonrası güvenlik ortamı (2001-2010),*
- *NATO'nun Lizbon Zirve deklarasyonu ve kabul edilen yeni stratejik konsept.*

Şekil 20: NATO Siber Savunma Fonksiyon Yapısı

Kaynak: Çifçi, 2012: 53

NATO kapsamında, siber savunma teşkilat yapısının geliştirilmesi amacıyla Danışma, Komuta ve Kontrol Teşkilatı (NC3A), 2012 tarihinde yaklaşık 58 milyon euroluk tarihinin en büyük siber savunma anlaşmasını imzalamıştır. Anlaşma kapsamında, NCIRC'nin tam harekat kabiliyetine erişmesi ve bilgi paylaşımıyla, talep edildiğinde üye ülkelerin siber saldırılara karşı desteklenmesi amaçlanmıştır. Bu doğrultuda NATO'da siber güvenliğe yönelik olarak yaklaşımlar, pro-aktif bir tutumdan daha çok re-aktif bir tutumla devam ettirilmiştir (Bayık ve diğerleri, 2013: 343). Siber savunma teşkilatlanma yapısı değişen tutumla birlikte uzmanlaşma kollarına ayrılmıştır.

Şekil 21: NATO Siber Savunma Teşkilat Yapısı



Kaynak: Çifçi, 2012: 55

Özellikle 11 Eylül sonrasından günümüze, uluslararası alanda NATO'nun bu denli hızlı bir şekilde kendini siber uzaya adapte etmesinde, NATO üyelerinden birine karşı

gerçekleşmesi mümkün olan *"Dijital Felaket"* senaryosu belirleyici olmuştur. Siber terör ve terörist grupların sanal ortamı kullanmaları ihtimali, muhtemel bir *Dijital Pearl Harbour* beklentisini yükseltmiştir. Devletlerin siber sistemlerine yönelecek saldırılarla ekonomik ve diğer kritik alt yapılarının vurularak etkisiz hale getirilebileceği, bunun da ülkedeki güvenliği derinden sarsacağı düşünülmüştür (Bıçakçı 2014: 119). Baskın bir güç haline gelen ABD ve diğer yükselen ülkelerin kritik altyapılarının bağlı oldukları sistemler siber alana ilişkin ortak hareket etme güdüsünü geliştirmiştir.

2016 Temmuz'unda düzenlenen Varşova Zirvesi'nde *siber alan,* ittifakın savunulacağı operasyonel alanlardan biri olarak tanımlanmıştır. Değişen güvenlik tehditlerine uyum sağlamak amacıyla atılan bu adım, herhangi bir NATO ülkesinin ciddi boyutlara ulaşan bir siber saldırıya hedef olunması halinde, kolektif savunma öngören NATO'nun 5. maddesinin işletilmesine, konvansiyonel silahlarla karşılık verilebilmesine yeşil ışık yakmıştır.[95]

2.3.2. Avrupa Birliği

AB, Şubat 2013'te hayata geçirilen *AB Siber Güvenlik Strateji Belgesi* ve ona eşlik eden *Network and Information (NIS) Direktif*'i ile siber güvenliği öncelikli alanlar arasında tanımıştır (Meulen ve diğerleri, 2015: 18). AB'de siber güvenlikten sorumlu teşkilat olan *Avrupa Ağ ve Bilgi Güvenliği Teşkilatı (ENISA),* 2004 yılında kurulmuş ve 2005 yılında tam harekat kabiliyetine kavuşmuştur. ENISA, AB içerisindeki iletişim ağlarının kurulması, güvenliğinin sağlanması ve ilgili personelin bilgilendirilmesi hususunda çalışmalar yapmaktadır (Keleştemur, 2015: 192).

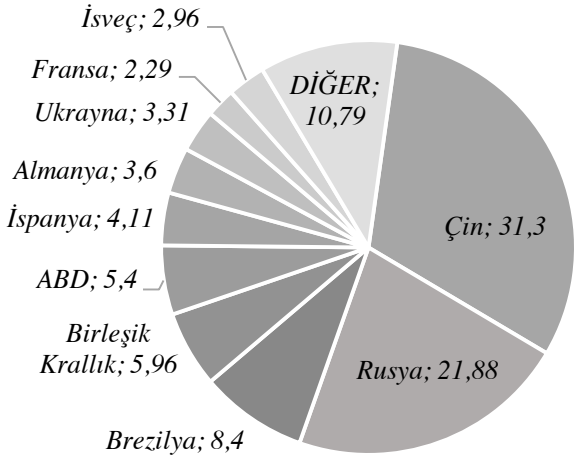
ENISA koordinatörlüğünde ilk siber tatbikat olan *Cyber Europe*, 4 Kasım 2010 tarihinde gerçekleştirilmiş ve güvenlik ile iş birliği alanındaki sütuna dair önemli bir katkı ve gelişme sağlamıştır. Çeşitli zamanlarda siber tatbikatlar yapılarak, AB'ye üye ülkelerin, diğer gruplar tarafından yapılacak saldırılara karşı önlem alması hususunda savunma boyutu oluşturulmaktadır. Üye ülkelerin bir araya gelmesiyle merkezi Hollanda'nın Lahey kentinde

[95] NATO Genel Sekreteri Stoltenberg'in, *"Siber alanı, operasyonel alanlarımız olan kara, hava ve deniz alanlarımıza dahil ettik, yeni operasyonel alan olarak kabul ettik."* sözleriyle ilan ettiği karar siber saldırıların sadece devletler boyutunda ele alınmayıp bireyler, organize suç ve terör örgütlerine karşı iş birliği noktasında bir duruşu ortaya koymuştur.

bulunan EUROPOL bünyesinde hizmet veren, *Siber Suçlarla Mücadele Merkezi* de siber alanda faaliyetlerini artırmıştır. İnternet suçlarına karşı AB ülkelerinin şimdiye dek ulusal çapta faaliyet gösterdiği gözlenmiştir.

Uluslararası alanda yapılan düzenlemelerin ve gelişmelerin teknik boyutunda her ne kadar ABD önde gibi olsa da AB üyesi ülkeleri içerisinde zararlı yazılımların çoğaldığı ve siber güvenlik açısından bir teklike oluşturduğu bir gerçektir. Son yıllarda uluslararası alanda yapılan AB merkezli çalışmaların arkasında bu sebep yatmaktadır. Grafik 13'te görüldüğü üzere; İsveç, Fransa, Ukrayna, Almanya, İspanya ve İngiltere merkezli AB ülkelerindeki bu hareketlilik dikkat çekicidir. Siber alana artan bağımlılık ile birlikte zararlı yazılımların kaynaklandığı ülkeler olarak toplamları Rusya ve Çin düzeyine yaklaşmaktadır.

Grafik 13: Zararlı Yazılımların Kaynaklandığı Ülkeler



Kaynak: Botezatu, 2011: 7

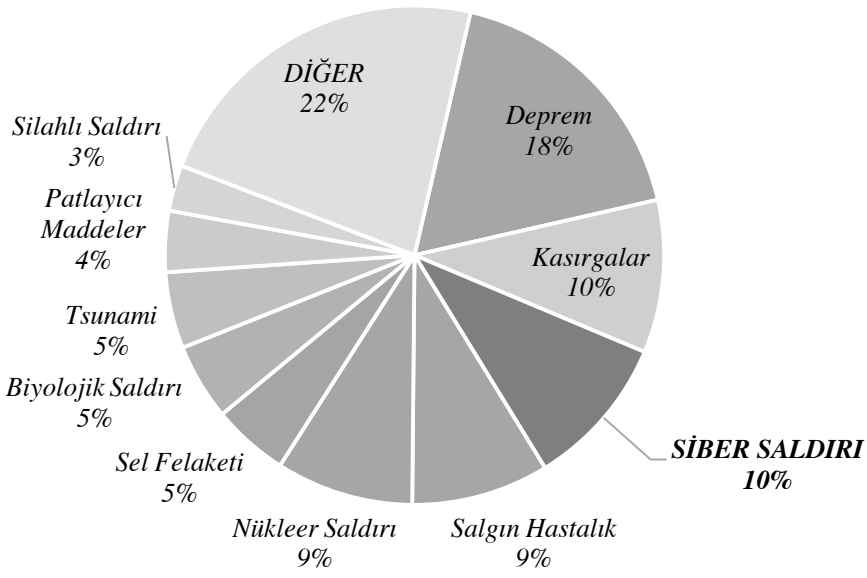
2016 yılı başında AB Konseyi, AB Komisyonu ve AB Parlamentosu'nun ilk siber güvenlik yönetmeliği üzerinde uzlaşmış olması önemli bir adım olmuştur. Yeni düzenlemeyle birlikte AB üyesi 28 ülkenin farklı siber güvenlik sistemleri uygulamalarının sonlandırılması yönünde somut bir karar alınmıştır. Ayrıca siber saldırılara karşı, enerji, ulaşım, banka, finansal piyasalar, sağlık ve su sistemi gibi kritik sektörlerdeki firmaların iş birliği ve önlemleri değerlendirilmiştir. Daha sonra NATO ve AB arasında hibrit tehditler, savunma sanayi, koordineli tatbikatlar, siber güvenlik ve deniz güvenliği alanlarında daha fazla iş birliği yapılmasını öngören ortak deklarasyon gecikmemiştir.

2.3.3. Amerika Birleşik Devletleri

Siber güvenlik ve uluslararası ilişkiler boyutunda ABD hem gelişim hem de bu gelişmişlik içinde uğradığı saldırılar açısından ön plandaki ülkelerden birisidir. 2014 ve 2015 yılları boyunca siber saldırılar sonucunda, ABD bünyesindeki kamu ve özel kurumlardaki hassas verilerin birçoğu düşman birimlerin eline geçmiştir.

ABD siber güvenlik yapılanmasının gelişimi ve uzmanlaşılmasında, hassas verilerin düşman eline geçmesiyle birlikte tehdit algısının değişimi ve toplumsal bir reaksiyona dönüşmesi etkili olmuştur. Yapılan farklı araştırmalarda siber tehdidin nükleer saldırıların, tsunami ve sel felaketi gibi tehditlerin önüne geçmesi ve algısal bir boyut oluşturması dikkatleri ve gündemi bu yöne çekmiştir. Grafik 14'te görüldüğü üzere farklı yıllarda yapılan çalımalarda siber saldırı tehlikesinin tehditsel boyutu algı olarak deprem, kasırgalar, nükleer saldırılar ve salgın hastalıklarla eşdeğer bir noktaya ulaşmıştır.

Grafik 14: ABD İçin Tehlike Unsurlarının Dağılımı



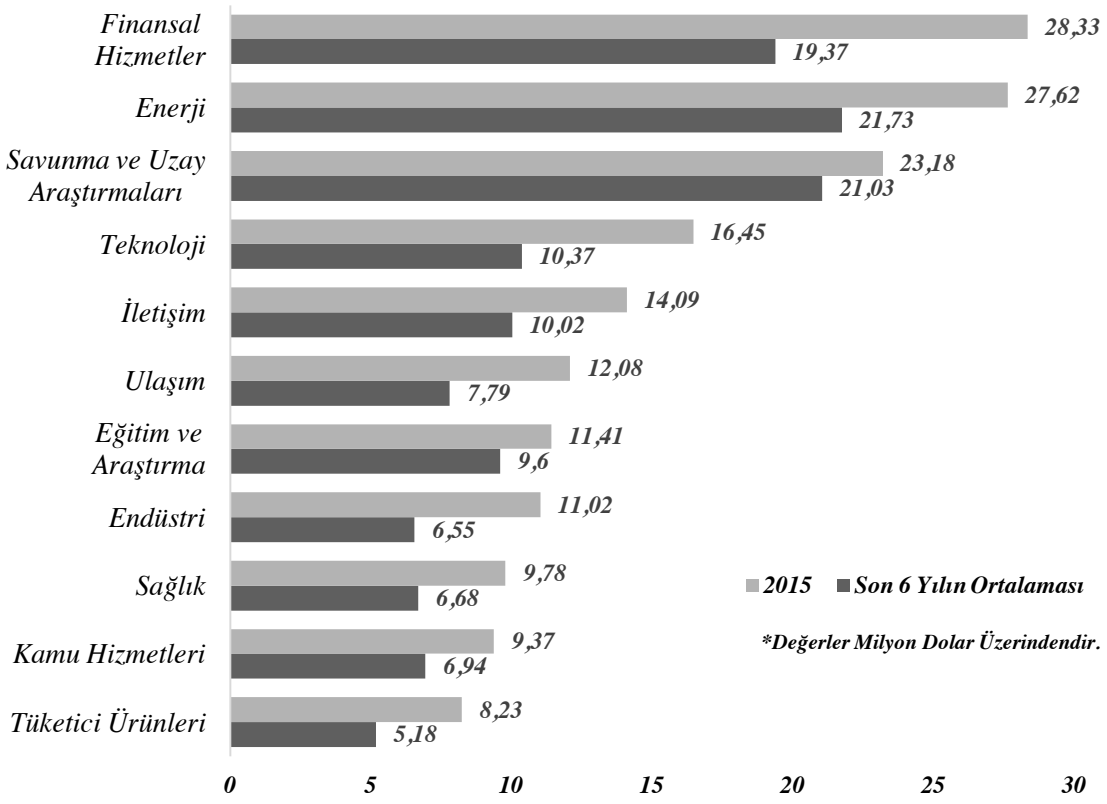
Kaynak: Paganini, 2012a

Artan olaylar, algı boyutunun siber savaşa kayması ve son yıllarda maruz kalınan siber saldırılarla birlikte ABD Başkanı Obama, ülkedeki siber güvenlik önlemlerini artırmak için senatodan 19 milyar dolarlık bütçe istemeyi uygun görmüştür. 2017 yılının bütçesi

olarak oylanacak bu dilim 2016 için ayrılan 14 milyardan sonra %33 artışla ciddi bir yatırıma işaret etmektedir. Gerek sahip olduğu profesyonel kabiliyet gerekse kapasite açısından bu yatırımlar da karşılığını almaktadır.

Ciddi bir bütçenin ayrılışı ve siber güvenlik alanına ilişkin yapılanmanın oluşturulmasına yönelik uzmanlaşmanın artışında, halihazırda siber saldırıların ABD'ye vermiş olduğu mali zarar da etkili olmuştur. Grafik 15, bu durumu açıklayan iyi bir bütünlük sunmaktadır. Gerek kritik altyapılar, gerek finans ve gerekse hükümet kurumlarının mali zararı siber saldırılar sonucunda çok ciddi boyutlara ulaşmıştır. Başta finansal hizmetler, enerji, savunma, uzay araştırmaları ve teknoloji sektörleri olmak üzere siber suçların ABD'ye toplam faturası 2015 yılı itibariyle yaklaşık 200 milyon dolara ulaşmıştır.

Grafik 15: Siber Suçların ABD'de Sektörlere Verdiği Mali Zarar

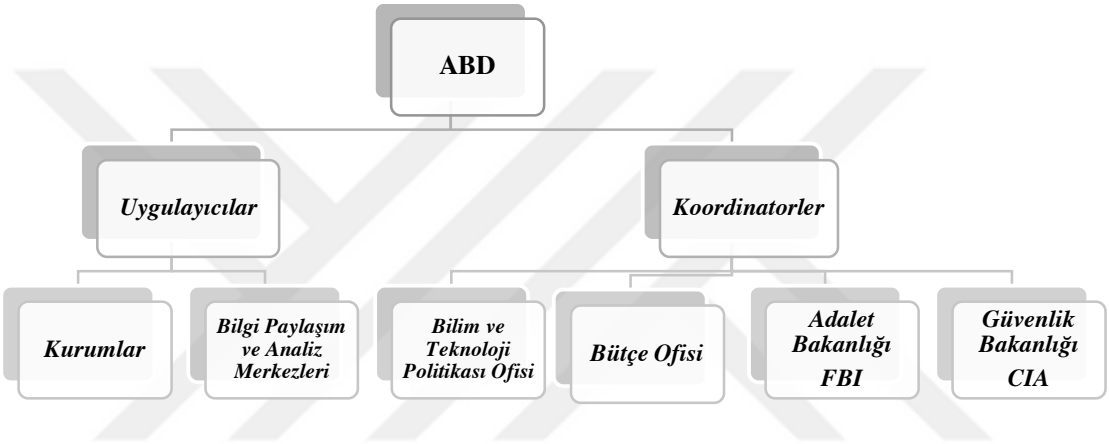


Kaynak: The Statistics Portal, 2016b

Gerek mali zararlar gerekse veri kayıplarıyla mücadele eden ABD, siber güvenlik stratejisi uygulama adına kurumsallaşma yönünden ciddi adımlar atmış ve özel sektörle de

iş birliği yoluna gitmiştir. Güvenlik stratejisinin uygulanmasında uygulayıcılar ve koordinatörler olmak üzere keskin bir ayrıma gidilen süreçte hiyerarşik bir yapılanma benimsenmiştir. Bu yapılanma içerisinde sadece savunma ve saldırı stratejilerinin oluşturulması adına karar mekanizmaları oluşturulmamış; araştırma ve geliştirme, bilim politikalarının belirlenmesi ve uzay faaliyetleri ile mali konuların görüşülmesi konusunda uzmanlık birimleri oluşturulmuştur.

Şekil 22: ABD Siber Güvenlik Stratejisi Uygulama Organizasyonu



Kaynak: Ladani ve Berejkoub, 2006: 3

ABD bünyesinde siber güvenlikten sorumlu en üst düzeyde dört kurum bulunmaktadır ve bu kurumlar aynı zamanda siber güvenliğin tesis edilmesinde beraber çalışmaktadır. Bu kurumlar şu şekildedir:

- Milli Güvenlik Teşkilatı (NSA)
- Federal Araştırma Bürosu (FBI)
- Siber Komutanlık (USCYBERCOM)
- İç Güvenlik Bakanlığı (DHS)

2.3.3.1. Ulusal Güvenlik Teşkilatı (NSA)

Hem ABD Savunma Bakanlığı hem de ABD İstihbarat Toğluluğu'nun (U.S. Inteligence Community) üyesi olan NSA, dış siber tehdit istihbaratını yürütmekten, milli

güvenlik sistemlerinin emniyetli hale getirilmesi için rehberlik etmekten ve istihbarat uzmanlık desteği sağlamakla sorumludur. NSA özellikle ülke sınırları dışındaki iletişim ve sinyal istihbaratından da sorumludur.[96]

Küresel kriptolojide en üstün kurum olma stratejisi içerisinde olan NSA için, bu anlamda dışardaki tüm kriptolojileri çözebilecek kabiliyete sahip olduğu iddia edilmektedir. Her ne kadar varlığı artık tüm dünya tarafından biliniyor olsa da NSA'in yerleşkesine girmek mümkün olmamaktadır. NSA'in TOR gibi sistemleri dahi izleyebildiği, dünya üzerindeki tüm iletişim ağının şifrelenme ve deşifrelenme işlemleri arasındaki verileri de gözetlediği belirtilmektedir (Keleştemur, 2015: 184).[97]

NSA başkanı aynı zamanda USCYBERCOM'un da komutanıdır. NSA'in görevi bu kapsamda sadece iletişim istihbaratı ile sınırlandırılmıştır, insan veya saha istihbaratı yapmamaktadır. Kanunen NSA bünyesinde sadece ülke toprakları dışında istihbarat toplama yetkisi vardır. Özellikle Başkan Bush yönetimi sonrası NSA'in bir ucunun ülke içinde olan iletişimleri izlediğine dair tartışmalar yaşanmaktadır.[98]

Temel olarak popüler iletişim anlamında, internete bağlı bir çok iletişim aracı ABD merkezlidir ve çoğu zaman NSA için gizli bilgiler sızdırdığı da bilinen bir gerçektir. NSA, güvenlik anlamındaki sorumluluk ve avantajını bu bilgilerin elde edilmesinde ve depolanmasında çok kolaylıkla kullanabilmektedir.

Özellikle ulusal güvenliğin kurumsallaşması ve geleceği açısından ABD yönetimi tarafından el üstünde tutulan NSA, kimi zamanda istihbarat faaliyetlerinin vermiş olduğu zorluktan dolayı tartışma konusu olabilmektedir. Bu durumun temel sebepleri arasında

---

[96] Dünyada en fazla matematikçi istihdam eden kurum olarak dikkat çeken NSA, uzun yıllar kamuoyundan saklı tutulmuş, çok gizli bir servis olarak görev yapmıştır. Bu yüzden NSA için ayrıca *"No Such Agency"* de denilmektedir.

[97] NSA yüz tanımlama programının geliştirilmesi için, her gün milyonlarca fotoğraf taramaktadır. Bu anlamda Whatsupp, Facebook ve Instagram gibi popüler sosyal medya araçları üzerinden paylaşılan fotoğrafların, bu program kapsamında sürekli olarak taranmakta olduğu, her fotoğrafın kime ait olduğu belirlenip dosyalandığı da ifade edilmektedir.

[98] Washington Post gazetisinin 19 Temmuz 2010 yılındaki haberine göre NSA günde 1.7 milyar e-posta, telefon konuşması ve diğer iletişimi yakalamakta ve kaydetmektedir. Bu bilgileri de 70 farklı veri tabanında sınıflandırmaktadır.

ulusal güvenlik yanında ekonomik hedeflere ve verilere yönelinmiş olunmasıdır. Bu durumun tartışılmasındaki diğer bir sebep ise bağımsız operasyonlar yapabilmesidir.[99]

2.3.3.2. Federal Araştıma Bürosu (FBI)

FBI, ABD Adalet Bakanlığı bünyesinde, federal suçların araştırılması ve ülke içinde istihbarata karşı koyulmasından sorumlu teşkilattır. Aynı zamanda FBI, ülke sınırları içinde suçla veya istihbarata karşı koymayla ilgili siber olayların araştırılması ve engellenmesinden sorumlu hale getirilmiştir. Yasa uygulama ve istihbarata karşı koymaya ek olarak, ülke içi siber tehdit istihbaratının en üst düzeyde yetkili kurumudur. FBI ayrıca, siber güvenlik konularında İç Güvenlik Bakanlığı'na bilgi ve destek sağlamaktadır (Çifçi, 2012: 41).

Hukuki anlamda, organizasyonel olarak yeniden yapılandırma çalışmalarının en önemli örneklerinden bir tanesi 2001 yılında gerçekleşmiştir ve FBI, *Ulusal Beyaz Yaka Suç Merkezi (NWC3)* ile işbirliğinde bulunarak *İnternet Suçu Şikayet Merkezi'ni (IC3)* kurulmuştur. Daha önce INTERPOL tarafından oluşturulan 7/24 ağıyla benzerlikler içermesiyle birlikte IC3, internet suçlarının raporlanması açısından merkezi bir iletişim noktası oluşturulması amacıyla kurulmuştur.[100]

Her ne kadar FBI ve DOJ'un çalışmaları ulusal anlamda siber suçlarla mücadeleye odaklanmış olsa da, siber suçlarla ortaya çıkan problemleri önlemek amacıyla yerel kuruluşlara siber suç uzmanları yerleştirilmiştir. Örneğin; 2003 yılında FBI, *Bilgisayar Suçları Görev Kuvvetleri (Computer Crime Task Forces)* adı altında bir organizasyon kurarak polis kuruluşlarına, lokal bilgisayar suçlarının soruşturulması sırasında yardım etmektedir (Berber, 2012: 17). Şu anda ABD'de, bu anlamda çalışan 92 civarında kuvvet birimi yer almaktadır. Aynı sebepten yola çıkarak, Adalet Departmanı (Department of

[99] NSA operasyonları ile yüzlerce insana habersiz olarak, uzun süreli kontrol ve sabotaj yapılmış olması muhtemeldir. NSA ağı, ABD vatandaşlarına gizli olarak hastalıklar, akıl ve ruh bozuklukları yayabilecek gizli psikolojik kontrol operasyonları araçlarına sahiptir.

[100] Bu program halen kullanılmakta olup ülke çapında önemli bir başarıya sahip olmuştur. Yalnızca 2008 yılında sisteme düşen şikayet sayısı 275.000'i geçmiş, bu şikayetlerin %26'sı doğrulanmış ve ilgili hukuki yaptırım kuruluşlarına aktarılmıştır. Her ne kadar bu çalışma ülke açısından, büyük bir başarı simgesi olarak kabul edilse de siber suçların önüne geçilmesinde etkin olamamıştır. FBI anketlerine göre halen internet suçlarının büyük bir bölümü daha önceden tespit edilememiş olmakla beraber, gerçekleşen vakaların çok küçük bir bölümü IC3 tarafından tespit edilmiştir.

Justice); *Bilgisayar Hackleme ve Fikri Mülkiyet (Computer Hacking & Intellectual Property)* adı altında yerel federal mahkemelerde yer alan ve siber suçların verimli bir şekilde anlaşılması ve gerekli adli takibin yapılması konusunda avukatlara eğitim veren birimler kurmuştur.

Artan siber tehdit ve olaylar karşısında eyalet ve yerel düzeyde çalışma perspektifini değiştiren FBI, *"Siber Kalkan İttifakı"* adlı bir program da başlatmıştır. Diğer federal dairelerle birlikte, siber suçlarla ilgili paylaşım içerisinde olduğunu belirten FBI özel sektörle olan ortaklığını artırmıştır. Kurum uzunca bir süredir siber saldırılarla ilgili bilgi almaktadır.

2.3.3.3. Siber Komutanlık (USCYBERCOM)

ABD Siber Komutanlığı, resmi olarak 21 Mayıs 2010 tarihinde; Maryland eyaletinin Fort Meade kentinde faaliyete başlamış olup, 31 Ekim 2010 tarihinde tam harekat kabiliyetine kavuşmuştur. ABD Savunma Bakanlığı Siber Komutanlığı'nın tam operasyonel kabiliyeti bulunmaktadır. Böylelikle siber savaş ortamında, gerektiğinde harekat gerçekleştirebilecek bir yapıya sahiptir. Düşman iletişim ağlarının, komuta kontrol sistemlerinin ve bilgisayarların kullanılamaz hale getirilmesi, veri çalınması gibi faaliyetler gerçekleştirilmektedir (Keleştemur, 2015: 178).

Ayn zamanda Siber Komutanlık, ABD Silahlı Kuvvetlerinin yüksek tempoda ve etkili bir şekilde harekat yapma yeteneğini desteklemekte ve komuta kontrol sistemleri ile silah sistemlerini destekleyen siber alan altyapısını saldırı ve bozulmalara karşı korumaktadır. Siber Komutanlığın, temel olarak Savunma Bakanlığı iletişim ağlarını koruyacağı belirtilmektedir. Federal sivil ağlar (.gov alanı) *İç Güvenlik Bakanlığı (DHS)* tarafından korunmaktadır.

Bazı askeri liderler; Kara, Deniz ve Hava Kuvvetlerinin mevcut kültürünün, dördüncü bir kuvvet olarak teşkil edilen Siber Komutanlık ile temel olarak uyumsuz olduğunu iddia etmektedir. Eskiden beri var olan üç ana kuvvet komutanlığının geleneksel savaşlar için uygun olduğu ancak bu kabiliyetlerin siber savaş için yeterli ve uygun olmadığı belirtilmektedir. Bu nedenlerle geleneksel kuvvetlere ilave olarak, tamamen teknik ve

teknolojinin hakim olduğu, savunma ve saldırı kabiliyetlerini bünyesinde barındıracak dördüncü bir kuvvet olan Siber Komutanlığın caydırıcı olamayacağı tartışılmaktadır (Çifçi, 2012: 29).

Yapılan eleştirilere rağmen Siber Komutanlığın diğer kurumlarla olan organik bağı siber güvenlik adına ABD'nin elini güçlendirmektedir. Siber Komutanlık, *ABD Stratejik Komutanlığı*'na[101] bağlı olmasına rağmen kendi içinde ayrıca dört bölüme ayrılmıştır ve etkinlik alanı geniştir. Bu etkinlik alanının alt birimleri ise şu şekidedir:

- *Kara Kuvveleri Siber Komutanlığı/ 2. Ordu*
- *Donanma Siber Komutanlığı/ Deniz Kuvvetleri 10. Filosu*
- *Hava Kuvvetleri Siber Komutanlığı/ 24. Hava Kuvvet Komutanlığı*
- *Deniz Piyadeleri Siber Komutanlığı*

2.3.3.4. İç Güvenlik Bakanlığı (DHS)

11 Eylül saldırıları sonrasında 25 Kasım 2002 tarihinde kurulmuş olan bakanlık, ABD topraklarını terör saldırılarından, insan merkezli kazalardan ve doğal afetlerden korumakla yükümlüdür. Sivil devlet ağlarının korunması, kritik altyapı ağlarının siber güvenlik açısından savunulması ve güvenlik önlemlerinin alınmasından sorumludur. Bakanlık ayrıca özel sektöre de bu konuda destek vermektedir. İç güvenliği tehdit eden, yüksek seviyedeki siber saldırılara karşı da koordinasyon yetkisi bulunmaktadır.[102]

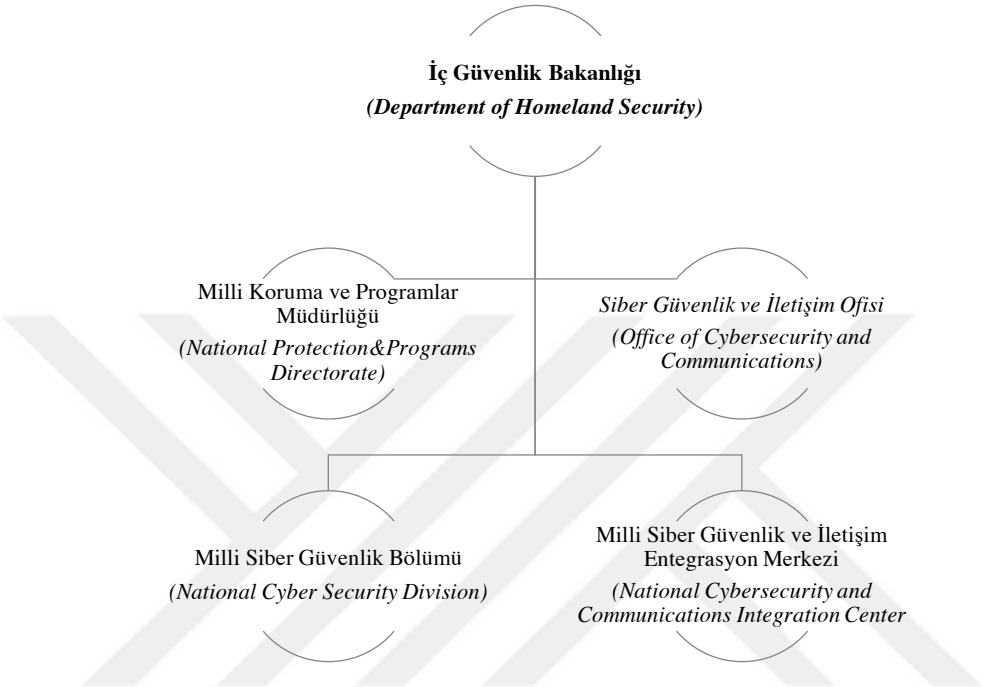
DHS birimi siber internet güvenliğinin sağlanmsı için tüm sorumluluğu üzerine almıştır. Bu doğrultuda hukuksal bütünlük açısından da yetkileri çeşitlenmiştir. *"Ulusal Siber Uzay Güvenliğini Sağlama Stratejisi"* dokümanında siber savunmanın sağlanması açısından iki taraflı bir yaklaşım ortaya konmuştur. CERT/CC iş birliği ile DHS organizasyonu içerisinde bulunan *Ulusal Siber Güvenlik Birimi* altında, ulusal bir CERT

[101] ABD Strateji Komutanlığı uzay harekatı, bilgi harekatı, füze savunması, komuta kontrol, istihbarat, keşif ve gözetleme ile nükleer silahlardan sorumlu olan bir komutanlıktır.

[102] 2016 yılı içinde ABD Adalet Bakanlığı'nın e-posta hesabını ele geçiren hackerlar özel ağlara sızmayı başarmıştır. 20000 FBI çalışanı ve 9000 civarı İç Güvenlik Bakanlığı çalışanının kişisel bilgileri ele geçirilerek internet üzerinden paylaşılmıştır.

organizasyonu (US-CERT) kurulmuştur. Bu kuruluşun amacı federal sivil ağları (.gov uzantılı) korumak olarak belirlenmiştir.[103]

Şekil 23: DHS Siber Güvenlik Birimleri



Kaynak: Çifçi, 2012: 39

ABD Hükümeti sorumluluk yetkisini geniş tuttuğu DHS açısından farklı bir güvenlik yapılanmasını tercih etmiştir. İç güvenlik, Amerika'yı teröristlere karşı savunmak için gösterilen bir çaba olarak tanımlanmıştır. DHS çalışmaları açısından bakacak olursak iç güvenlik kavramı farklı bir şekilde ele alınmıştır ve ulusal güvenlik kavramına göre farklılaşmıştır (Yılmaz, 2011: 364).

Bilgisayar ağlarına ve sistemlerine karşı yapılan saldırıların tespit edilmesi maksadıyla *EINSTEIN 2 Projesi*'ni yürüten DHS, önemli siber saldırılara karşı koordinasyon yetkisine sahiptir. Yakın zamanda bir hackerın 9000'den fazla DHS çalışanının kişisel bilgilerini yayınlamasıyla gündemi oldukça meşgul etmiştir. Bu tür kurumların hedef haline gelmesi zamanlama açısından manidardır.

[103] İzleme ve İstihbarat sürecinde ise *CIA ve NSA* iş birliği altında *İstihbarat Toplumu-Vaka Tepki Merkezi (IC-IRC)* ve *Ulusal Güvenlik Kuruluşu Tehdit Operasyonları Merkezi (NTOC)* gibi kuruluşlar görev almaktadır.

2.3.4. Rusya Federasyonu

Rusya'da 1999 yılında Putin'in göreve gelmesi ile birlikte, 2000 yılında ulusal güvenlik politikası yeniden ele alınmış ve bilgi harekatı üzerine odaklanılmıştır. Bu tarihte ilk defa *Rusya Federasyonu Bilgi Güvenliği Doktrini*, yetkili Güvenlik Konseyi'ne sunulmuştur.

Bir çok farklı uzmana göre Rusya, siber savaş kapasitesi açısından Çin'den daha tehlikeli görülmektedir. Rusya'nın Moskova'da, ABD'nin NSA yapılanmasına benzeyen *FAGCI (Devlet İletişim ve Bilişim Federal Teşkilatı)* isimli bir kuruluşu vardır. Rusya siber yapılanması içinde *Federal Güvenlik Servisi* ve *Beşinci Boyut Siber Ordusu* öne çıkan birimlerdir.

2.3.4.1. Federal Güvenlik Servisi (FSB)

Bir dönem Vladimir Putin'in de başında olduğu FSB, Rusya Federasyonu'nun iç güvenliğinden sorumlu teşkilattır. Rusya Devlet Başkanı'na doğrudan bağlı olan kurum, istihbarata karşı koyma, iç güvenlik, sınır güvenliği ve terörle mücadeleden sorumludur. Sovyetler zamanındaki KGB'nin günümüzdeki halidir.

FSB, siber uzayda iletişim ağları dahil kritik altyapıların korunmasından sorumludur. FSB Kanunu'na göre. Rusya'da hizmet vermekte olan tüm telekomünikasyon hizmeti veren birey ve kurumlar, FSB'nin ek yazılım ve donanımlarına müsaade etmek zorundadır. Bir başka deyişle, ülkenin telekomünikasyonel anlamdaki istihbarat altyapısı FSB tarafından denetlenmektedir (Keleştemur, 2015: 188).[104]

Rusya'da siber savaş; hizmet dışı bırakma, hacker saldırıları, internet üzerinden dezenfermasyon yayma, devlet destekli grupların siyasi bloglarındaki faaliyetleri, siber takip ve muhaliflere baskı şeklinde gerçekleşmektedir. Yönetimsel anlamda, muhaliflerle olan siber mücadele yoğun bir şekilde Rusya gündemini meşgul etmektedir. FSB'nin

[104] SORM adı verilen bir internet izleme sistemi vasıtasıyla takipler yapılmakta, internet eşirim noktaları ve internet servis sağlayıcılarına sensörler yerleştirilmektedir. *İnternet Elektronik Gözetleme Merkezi*, elektronik iletişimin dinlenmesi ve deşifre edilmesinden sorumludur.

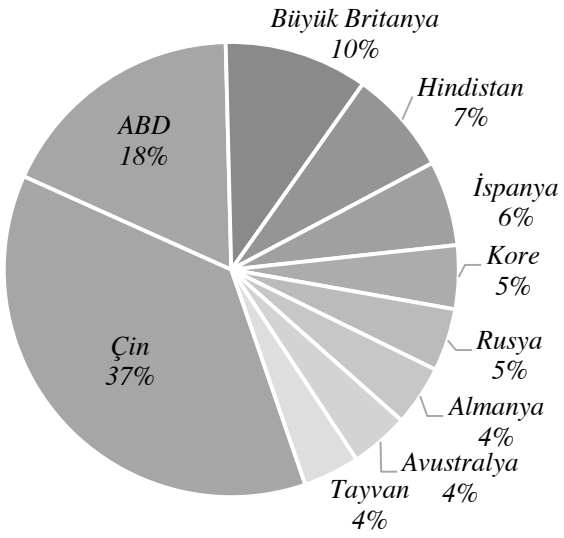
kontrolündeki çeşitli gruplar, Rus ve uluslararası politik bloglarında Putin ve Rusya yanlısı propagandayı teşvik etmek amacıyla hareket etmektedirler.

2.3.4.2. Beşinci Boyut Siber Ordusu

Beşinci Boyut Siber Ordusu, Savunma Bakanlığı'na bağlı Elektronik Harp Birlikleri ile profesyonel siber korsanlık eğitimi veren kurumların yetiştirdiği kişilerden oluşmaktadır. Kriptografi, kablosuz veri iletişim jammerlarının geliştirilmesi, elektromanyetik dalga silahlarının üretilmesi, virus ve solucanların yazılması, DDoS ve istihbarat amaçlı gelişmiş büyük Botnet oluşturulması gibi hususlarda çalışmaktadır (Keleştemur, 2015: 188).

DDos saldırıları ve istihbarat amaçlı Botnetlerin kullanımında Rusya'nın saldırı kapasitesinin özellikle çevre ülkelerde, etkin şekillerde kullanıldığı; bu saldırı türlerine maruz kalınması açısından Rusya'nın bazı temel noktalarda hazırlıklı olduğu görülmektedir. Grafik 16'da DDoS saldırılarının kaynaklandığı ilk 10 ülke verilmiştir. Özellikle 2015 yılı içinde ABD, Çin ve İngiltere gibi ülkelere oranla geride kalan Rusya, tehdidin ortaya çıkışı açısından ve saldırı amaçlı kaynaklara göre, farklı araçlara sahip oluşu itibariyle DDoS saldırılarında olduğu gibi düşük oranlara kaynaklık etse de farklı siber silahlarla etkinliğini sürdürmektedir.

Grafik 16: 2015 Yılı DDoS Saldırılarının Kaynaklandığı İlk 10 Ülke



Kaynak: Platform, 2015

Rusya sahip olduğu saldırı ve savunma kapasitesi itibariyle, siber ordusu olduğunu kabul etmemektedir ve yapılanmasını gizli tutmaktadır. Çevre ülkelerle kıyaslandığında etkin bir yapıda çalışan Rusya siber birimleri, ABD'ye kıyasla daha kapalı ve sessiz durmaktadır. ABD'nin farklı birimlerle siber olaylarla mücadele ettiğini belirtmesi ve kurumlarını adres göstermesinin altında daha çok caydırıcı olma isteği bulunmaktadır.

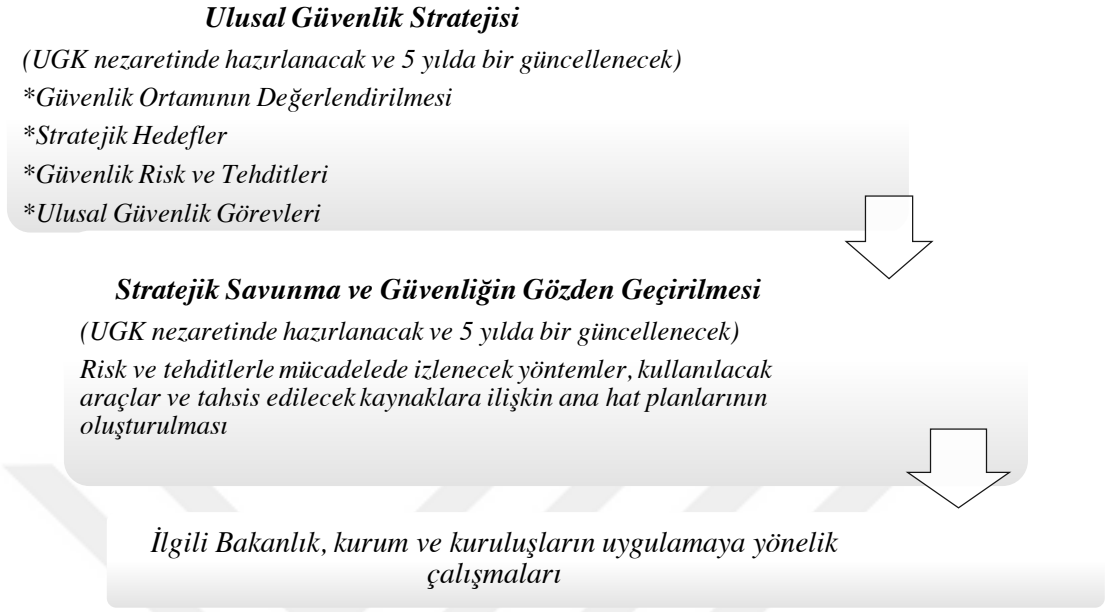
2.3.5. İngiltere

İngiltere son yıllarda siber savaş ve siber istihbarat konularında büyük atılımlar yapan ülkeler arasında yer almaktadır. Özellikle ABD'deki NSA benzeri bir yapıya sahip olan GCHQ, Snowden tarafından sızdırılan belgelerde adı en çok geçen kurumlar arasındadır. İngiltere'de, Haziran 2009'da Milli Güvenlik Stratejisi kapsamında ilk kez siber güvenlik konularının ele alınmasıyla birlikte, ülke çapında siber güvenlik ve siber saldırı alanlarında önemli adımlar atılmıştır.

Hükümet, özel sektör ve bireyler olarak ciddi bir iş birliğinin gözlendiği ülkede, uluslararası gelişmeler anlık takip edilmektedir. Ekonomik altyapının ve politik gelişmelerin birbirine doğru entegre edildiği ve olumlu bir ivmenin yer aldığı ülkede siber casusluk ve hibrit savaş unsurlarına karşı hazırlıklı olma temel prensipler arasında yer almaktadır. Birleşik Krallık'ın, *2010 Ulusal Güvenlik Stratejisi'*ne dayanılan verilere göre küresel olarak siber suçlardan ve saldırılardan 1 trilyon dolarlık bir kayıp söz konusudur (Cornish ve diğerleri, 2010: 9).

İngiltere bünyesinde oluşturulan yeni ulusal güvenlik kurulu ve temel dokümanlar ciddi bir çalışmanın ürünü olarak uluslararası alanda takdir toplamıştır. Şekil 24'te görüldüğü üzere özellikle uygulumaya yönelik çalışmaların temel dokümanlar içinde inceleme alanı bulması ve kontrollü olarak yapılan değerlendirmeler olumlu bir hiyerarşik yapılanmayı oluşturmuştur. *Ulusal Güvenlik Stratejisi* içerisinde; güvenlik ortamının değerlendirilmesi, stratejik hedefler, güvenlik risk ve tehditleri ile ulusal güvenlik görevleri, kısa ve uzun vadeli programlarla uygulamaya konulmuştur. Aynı zamanda, temel dokümanlar içerisinde verilen maddi kayıplara ve oluşturulabilecek savunma unsurlarına dair düzenli olarak raporlar oluşturulmaktadır.

Şekil 24: İngiltere'nin Yeni Ulusal Güvenlik Kurulu Temel Dokümanları

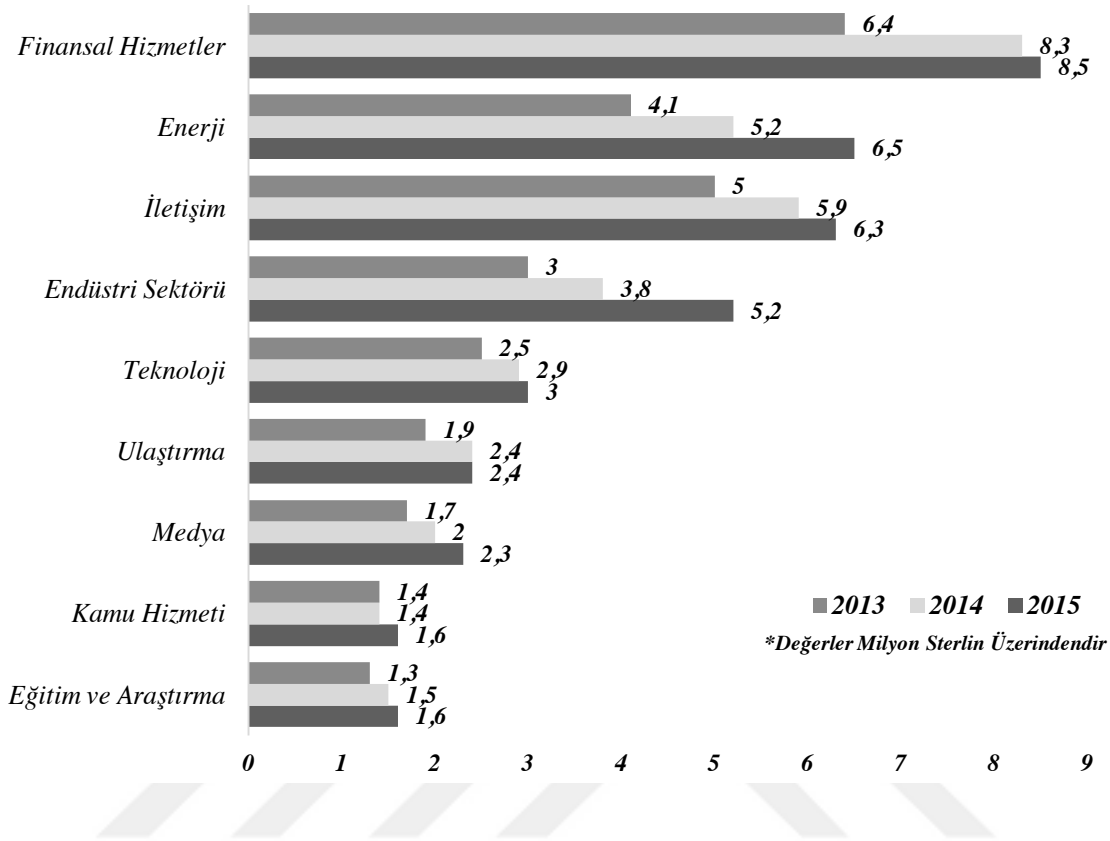


Kaynak: İngiltere'nin Yeni Ulusal Güvenlik Yaklaşımı (t.y.: 8), http://www.mgk.gov.tr/calismalar/calismalar/006_ingilterenin_yeni_guvenlik_yaklasimi.pdf

İngiltere yapılanması içerisinde teorik olarak ortaya konan dokümanlar, atılacak adımlarla pratiğe dönüştürülmesi adına hızlı bir ivme kazanmıştır. Alınan yolda İngiltere'nin uğramış olduğu mali zararların etkisi dikkat çekmektedir. Son yıllarda artış gösteren veriler sonucunda İngiltere Savunma Bakanlığı, tehditlerin tespiti ve savunulması hususunda farklı kurumlar arasında iş birliği oluşturacak bir altyapı kurmuştur (Dewar, 2014: 9).

Grafik 17'de, siber suçların İngiltere'de sektörlere verdiği mali zarar detaylandırılmıştır. Son yıllarda tüm sektörlerde uğranılan zarar artış göstermiştir. Özellikle finansal hizmetler, enerji ve iletişim hemen hemen diğer tüm ülkelerde olduğu gibi siber saldırılardan en çok etkilenen sektörler arasında yer almıştır. Kritik altyapılara da yönelen siber saldırılar endüstri, teknoloji ve ulaşım gibi alanlarda rahatsız edici boyutlara ulaşmıştır. 2013, 2014 ve 2015 yıllarında belirtilen sektörlerde toplam zarar 100 milyon sterlini bulmuştur. Devletlerin saldırı amaçlarından daha çok kendi bünyesindeki sektörlerin uğradığı zararlarla birlikte savunma niteliğindeki gelecek kaygıları da artmıştır.

Grafik 17: Siber Suçların İngiltere'de Sektörlere Verdiği Mali Zarar



Kaynak: Ponemon Institute, 2015b: 10

İngiltere siber güvenlik adına, ajanda oluşturulması açısından gerçekçi bir bütünlüğü sağlayabilmiş bir ülkedir. Siber alanda kurumsallaşmaya da giden İngiltere bünyesinde faaliyet gösteren temel birimler; *Siber Güvenlik ve Gilgi Güvencesi Ofisi (OCSIA)* ve *Siber Güvenlik Harekat Merkezi (CSOC)*'dir.[105]

2.3.5.1. Siber Güvenlik ve Bilgi Güvencesi Ofisi (OCSIA)

İngiltere'nin ulusal bilgi güvenliği kapsamındaki faaliyetlerinin koordinasyonu 2009 yılında *Siber Güvenlik Ofisi (The Office of Cyber Security)*'ne verilmiş, daha sonra bu kurum 2010 yılında *Siber Güvenlik ve Bilgi Güvencesi Ofisi (OCSIA)*'ne dönüştürülmüştür. Dönüşümlerdeki temel sebep altyapıların kurumsal olarak yenilenmesidir. OCSIA, *Birleşik*

[105] İki teşkilata ek olarak; *Devlet İletişim Karargahı (GCHQ)*, *Milli Altyapıları Koruma Merkezi (CPNI)*, *İş, Yenilikçilik ve Yetenekler Birimi (BIS)*, *İngiltere Bilgisayar Olaylarına Müdahele Ekibi (GovCertUK)* ve *Polis Merkezi e-Suç Ünitesi (PCEU)* kurumları da İngiltere'de farklı görevler üstlenmiştir.

Krallık Kabine Ofisi bünyesinde bir merkezi kamu kurumu olarak faaliyetlerini sürdürmekte olup merkezi Cheltenham şehrinde bulunmaktadır.

OCSIA, *Birleşik Krallık Güvenlik Bakanlığı* ile *Ulusal Güvenlik Konseyi'*ne siber ortama ilişkin politika önceliklerini tespit etmekte yardımcı olmaktadır. Diğer bir ifadeyle bu kurum, ulusal bilgi güvencesi ve siber güvenlik ekseninde Birleşik Krallık'ın stratejik yönelimini tayin ve bu kapsamdaki eylemleri koordine etmektedir (Güngör, 2015: 89). OCSIA'nın başlıca görevleri şunlardır:

- *Birleşik Krallık Siber Güvenlik Stratejisi'nin yürütülmesi,*
- *Siber güvenlik stratejik liderliğini hükümet çapında üstlenmek,*
- *Kurumlar arası programlar vasıtasıyla strateji hedeflerine ulaşılması.*

2.3.5.2. Siber Güvenlik Harekat Merkezi (CSOC)

Siber alandaki gelişmelerin takip edilmesi, bütüncül bir durum bilgisi sağlanması, eğilimlerin analiz edilmesi ve siber olaylara karşı teknik müdahele işlemlerinin koordine edilmesinden sorumlu bir birimdir. CSOC, Devlet İletişim Karargahının (GCHQ) Cheltenham'daki binası ile aynı yerleşkede bulunmaktadır ve 12 Mart 2010 tarihinde faaliyetlerine başlamıştır (Çifçi, 2012: 47).

İngiliz Hükümeti, devleti siber saldırılara ve tehditlere karşı korumak amacıyla görevlendirilen bu kuruma, işletmelere siber güvenlik danışmanlığı vereceğini de duyurmuştur. Bu birimin işletmeler için her ihtiyaç duyduklarında tek başvuru merkezi olma özelliğiyle önemi artacaktır.

2.3.6. İsrail

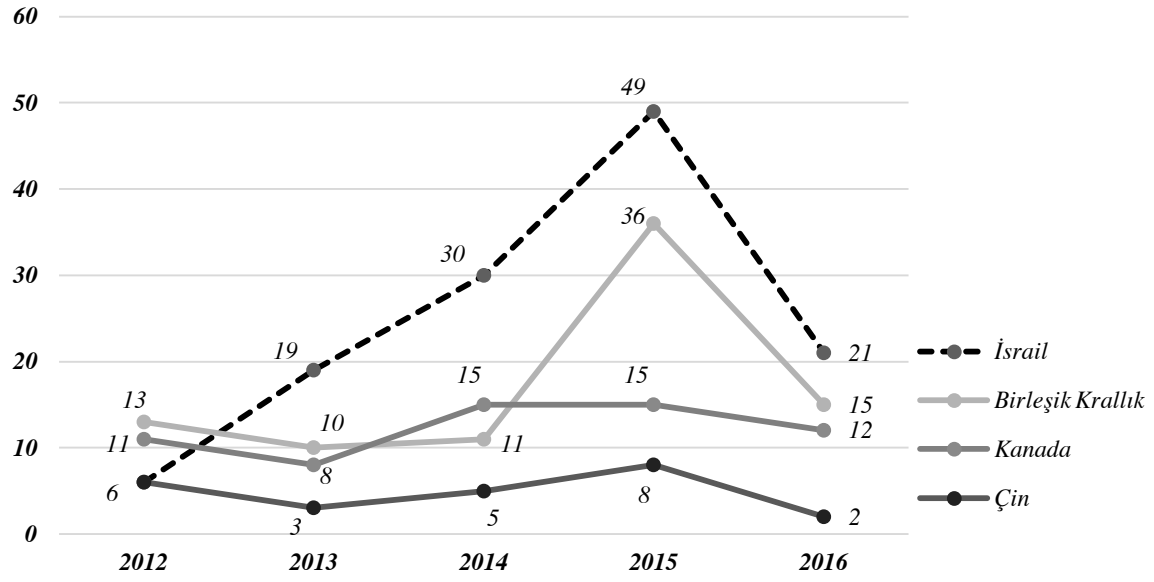
İsrail, başta Avrupa ülkeleri olmak üzere birçok ülkenin aksine, siber savaş alanında faaliyet gösterme kabiliyetine çok daha önceden başlamıştır. İsrail savunma kuvveti bünyesindeki siber savaş birimine personel alırken, sadece siber alandaki teknik kabiliyetlere değil, aynı zamanda komando seçimlerindeki gibi bireylerin fiziksel savaş yeteneklerini de test etmektedir. İsrailli siber savaşçılar, hem siber hem de fiziksel tahribat yapabilme

yeteneğine sahiptirler. Bu anlamda güçlü ve tehlikeli bir siber orduya sahiptir (Keleştemur, 2015: 191).

İsrail'deki tüm yüksek teknoloji firmalarının %20'si, ülkenin en büyük sektörü haline gelen siber güvenlikle uğraşmaktadır. İsrail siber güvenlik çözümleri kapasitesi açısından dünya lideri konumundadır ve siber savaş kapasitesi açısından, siber saldırılara en hazırlıklı ülkeler arasındadır. Ayrıca İsrail siber güvenlik çözümlerinin ihracından da ciddi bir kazanç elde etmektedir.

Grafik 18'de; İsrail, Birleşik Krallık, Kanada ve Çin'in son 5 yılda yaptıkları siber güvenlik anlaşmaları yer almaktadır. Özellikle siber güvenlik çözümlerinin ihracı ve yapılan anlaşmalar açısından İsrail'in ciddi anlamda bir üstünlüğü ve nüfuzu bulunmaktadır. 2012 yılı başlarına kadar siber güvenlik anlaşmaları düzeyinde oldukça gerilerde yer alan İsrail, siber saldırılar ve siber savaşın tartışıldığı uluslararası alanda etkinliğini ciddi bir ivmeyle artırmıştır ve üstünlüğünü kurmuştur. Son iki yılda yapılan siber güvenlik anlaşma sayısı 70'i bulmuştur.

Grafik 18: Siber Güvenlik Anlaşmaları: İsrail, Birleşik Krallık, Kanada, Çin



Kaynak: CB Insights, 2016

2.3.6.1. Unit 8200

İsrail'in sinyal istihbarat ve şifre çözme teşkilatıdır. Yeni dünya düzenine uyum sağlamak amacıyla, siber faaliyetler için de çeşitli çalşmalar yapmaktadır. Yüksek teknoloji standartlarına sahip bir yapılanmadır. Standart çözümler yerine talebe göre özel yazılımlar da geliştirebilmektedir.

Televizyon, radyo, gazete ve internet gibi tüm iletişim araçlarından düzenli olarak veriler toplamaktadır. Kimi ülkeler açısından uluslararası alanda tepkilerle karşılaşsa da, İsrailli yetkililer tarafından sadece savaş ortamının getirdiği caydırıcı unsur adına var olmadıklarını, barış için var oldukları yönünde açıklamalar yapılmaktadır.

2.3.6.2. C4I Tugayı

Komuta, kontrol, muharebe ve bilgisayarla ilgili faaliyetlerden sorumludur. Askeri ağları siber saldırılara karşı savunmaktadır. 2009 yılında Jerusalem Post gazetesinde, Askeri İstihbarat Teşkilatı ve C4I Tugayı'nın koordinesi altında bir savaş biriminin kurulduğu ve bilgisayar uzmanlarının istihdam edildiği haberi yankı uyandırmıştır (Çifçi, 2012: 51). Komuta, kontrol ve muharabe faaliyetlerinin tamamından askeri olarak sorumludur.

C4I birçok yeni uygulamanın hayata geçirilmesinde kilit konumdadır. Heron insansız hava araçlarını da üreten en önemli savunma sistemleri şirketi *Elbit* tarafından tasarlanan siber simülatör, C4I Direktörlüğü tarafından satın alınmıştır.

2.3.6.3. İsrail Güvenlik Teşkilatı (Shin Bet veya Shabak)

İsrail'in iç güvenlik istihbarat servisidir. Diğer istihbarat teşkilatları ise askeri istihbarat birimi AMAN ve yurt dışı istihbarat birimi MOSSAD'dır. Shin Bet altında, güvelik açısından önemli altyapıların savunmasından sorumlu bir birim *(Protective Security Department)* de mevcuttur.

Terörizm döngüsü karşısında şüpheliler ile ilgili bilgi toplama, karşı faaliyette bulunma yetkileri vardır. Önemli kritik altyapıların siber saldırılar ile igili kısmında

görevleri vardır ve hükümet binalarının, havayollarının istihbarat açısından verilerinde söz sahibidir.

2.3.6.4. Ulusal Sibernetik Görev Gücü (NCT)

18 Mayıs 2011 tarihinde kurulan NCT, ABD Siber Komutanlığı'nın benzeri gibi İsrail'in kritik ağlarını korumak, özel kuruluşları sanayi casusluğuna karşı korumak ve İsrail'i bir bilgi merkezi haline getirmekle görevlidir (Keleştemur, 2015: 191). Özellikle Brezilya ve Estonya'da yakın dönemde yaşanan saldırılardan sonra kurulmasına karar verilmiştir.

2008 yılında İsrail Merkez Bankası'nın devre dışı kalması, Mavi Marmara gemisine yapılan saldırının ardından Tel Aviv Belediyesi'nin de aralarında bulunduğu bir çok İsrail internet sitesinin saldırıya uğraması kuruluşunda temel parametreler olmuştur. İsrail Başbakanı Netanyahu tüm hayati sistemleri felce uğratabilecek siber saldırılar karşısında NCT'nin kurululuş sürecini hızlandırmıştır.

2.3.7. Çin

Çin, 1990'lı yılların başından beri sistematik bir şekilde siber savaşla ilgili projeler geliştirmekte, bu anlamda ülkenin internet alt yapısını da koruma altına almaktadır. Çin kendi bünyesinde yetiştirdiği birçok siber savaşçıyı, ayrı hacker grupları altında birleştirmiştir. Yapılan saldırılar Çin hükümetinden bağımsız bir şekilde dışarıya servis edilmektedir. ABD kökenli yazılımlardan uzak durulmakta ve kendi yazılım, donanımlarını oluşturma konusunda gayret göstermektedirler. Siber alanda yapılan faaliyetlerinin birçoğunun da gizli tutulduğu bilinmektedir. Özellikle siber saldırı yönünde atılan adımlar hususunda, Çin'in bazı illegal gruplarla yakın ilişki içinde olduğu gözlenmektedir ve bu konuda tepki çekmektedir.

Çin geçmiş yıllarda, ABD kökenli altyapılara siber saldırılar düzenleyerek, önemli ölçüde istihbarat bilgileri elde etmiştir. Geliştirdiği siber strateji sayesinde özellikle hacker grupları ile büyük bir hareket içindedir. Son yıllarda siber savaş kabiliyetlerinin yanında, nükleer ve uzay alanındaki kabiliyetlerin gelişmesi de Çin'in kapasitesini genişletmiştir

(Keleştemur, 2015: 185).[106] Çin ordusu konvansiyonel savaşları desteklemek maksadıyla siber alanda faaliyetlerini genişletmekte, araç ve personelinin eğitim kapasitesini sürekli artırmaktadır.

2.3.7.1. Genelkurmay 3. ve 4. Daireleri

2011 yılında Çin, *Mavi Ordu* adını verdiği siber savaş birimine sahip olduğunu kabul etmiştir. Çin'in siber harekata yönelik dört temel unsuru mevcuttur. Bunlardan ikisi *Çin Genelkurmay Başkanlığı* altında görev yapmaktadır. Çin ordusu, bilgisayar ağı harekatı yürütmek maksadıyla gereken kabiliyetleri geliştirme çabası içindedir ve geleneksel savaşları destekleyecek şekilde bilgisayar ağı harekatını uygulayabilmek için gereken stratejik rehberlik, araç ve eğitimli personeli oluşturmaya yönelik adımlar atmaktadır.

Genelkurmay 3. Dairesi, bu kapsamda sinyal istihbaratı ve siber savunma ile ilgili faaliyetlerin yerine getirildiği birimdir. Çin'in çeşitli yerlerine konuşlanmış bölgesel komutanlıklar ile sinyal istihbaratını toplamakta ve değerlendirmektedir. ABD'deki NSA gibi, ülke dışındaki sinyalin toplanması, ele geçirilmesi ve analizi ile Çin ordusunun ses ve iletişim ağlarının güvenliğinden sorumludur (Çifçi, 2012: 43).

Genelkurmay 4. Dairesi ise elektronik karşı tedbirler ve radar unsuru olarak görev yapmaktadır. Bu daire aynı zamanda geleneksel elektronik taarruz birimidir. Bilgi harekatı ve siber saldırı birimlerinin bu daireye bağlı çalıştığı rapor edilmektedir. Elektronik istihbarat (ELINT) elde etmekle yükümlü oluşu ve sinyal istihbaratı (SIGINT) elde etme özelliğine sahip olduğundan, Genelkurmay 3. Dairesi'ne de yardımcı olmaktadır.

2.3.7.2. Teknik Keşif Büroları

Stratejik ve taktik hedeflerden sinyal istihbarat toplamakla görevli, bilgisayar ağı harekatı uygulama kapasitesine sahip bürolardan oluşmaktadır. Sayısı net olmamakla birlikte, yapılan planlar oldukça geniş kapsamlıdır. Boeing'in C-17 yolcu uçağı ile Lockheed

[106] Çin, savunmadan daha çok saldırıya dönük bir gelişme planı uygulamaktadır. Bu anlamda Tayvan ile Çin arasındaki dönemsel sorunlara ABD'nin müdahil olmaya çalışması sebebiyle, ABD'nin elektrik şebekesini çökertebileceğini ispatlayan çeşitli eylemlerde bulunmuştur.

Martin'in F-22 ve F-35 savaş uçaklarına ait oldukça önemli bilgilerin ele geçirilmesinde büyük rol oynadığı bilinmektedir (Keleştemur, 2015: 186).

Diğer taraftan bu bürolarla ortak çalışmalar içinde olan bilgisayar korsanları, bireysel ve web üzerinden irtibat kuran birçok farklı grup, zengin bir saldırı birikimi ve yeteneğini bir araya getirmektedir. Çinli bilgisayar korsanları dünyanın çeşitli ülkelerine düzenledikleri başarılı siber saldırılar ile, en yetenekli saldırganlar arasında kabul edilmektedir.

2.3.8. Fransa

Fransa yaşanan terör saldırılarıyla birlikte, ülkedeki siber güvenliğin artırılmasıyla ilgili olarak çalışmalar başlatmış, bu konuda mevcut birimlerle çalışmak üzere yeni bir yapılanmaya gitmiştir. 2008'de *yayımlanan Savunma ve Milli Güvenlik Belgesi (Defense and National Security White Paper)'*nde siber güvenlikle ilgili hususlara değinilmiş; siber güvenlik koordinasyonu ve siber saldırılara karşı koyma adına saldırı kabiliyetine sahip bir teşkilatın oluşturulması hedeflenmiştir. Fransa adına kısa zamanda katedilen yol dikkat çekicidir.

Söz konusu belgede, Savunma ve Milli Güvenlik Genel Sekreterliği altında *Bilgi Sistemleri Güvenliği Teşkilatı (Security of Information Systems Agency)* kurulması ve Genelkurmay Başkanlığı bünyesinde, siber saldırı kabiliyetine sahip bir birimin kurulması planlanmıştır. Şubat 2011'de, *"Bilgi Sistemleri Savunma ve Güvenlik Stratejisi"* yayımlanmıştır. Belgede stratejik hedefler belirlenmiştir (Çifçi, 2012: 49).

2.3.8.1. Fransız Ağ ve Bilgi Güvenliği Teşkilatı (ANSSI)

ANSSI, 8 Temmuz 2009 tarihinde kurulmuştur. Devlet iletişim ağlarına yapılan siber saldırıları tespit etmek ve bertaraf etmekle yükümlü olan kurum, bu maksatla devlet ve ekonomik birimlerin kullanmakta oldukları altyapıların geliştirilmesi hususunda görev yapmaktadır. Siber istihbaratla ilgili olarak *Fransız Dış İstihbarat Teşkilatı (DGSE)* ve *İç Güvenlik Teşkilatı (DGSI)* ile ortak hareket etmektedir (Keleştemur, 2015: 191). Temel olarak görevleri şu şekildedir:

- *Devlet iletişim ağlarına yapılan siber saldırıları tespit etmek ve bu saldırılara hızlı cevap vermek için bir harekat merkezi olarak görev yapmak.*
- *Tehditleri engellemek amacıyla, devlet birimleri ve ekonomik aktörler için güvenli ürün ve hizmetlerin geliştirilmesini desteklemek.*
- *Devlet birimleri ve kritik altyapı aktörlerine güvenilir tavsiye ve destek sağlamak.*
- *Şirket ve kamuoyunu, bilgi güvenliği tehditleri konusunda bilgilendirmek (Çifçi, 2012: 49).*

2.3.9. Türkiye

Türkiye'de, siber güvenliği tehdit eden kişi ve kuruluşlara karşı yapılan mücadelede önemli rol oynayan çeşitli kurumlar bulunmaktadır. Bu kurumlardan bir kısmı istihbarat toplamak, karşı istihbarata karşı tedbirler gibi çalışmalar yaparken, bir kısmı siber güvenlik konusunda faaliyetler yürütmektedir.

Siber güvenlik konusunda faaliyet gösteren kurumlar bünyesinde koordineli olarak siber tatbikatlar da gerçekleştirilmektedir. İstihbarat birimleri ve siber güvenlik konusunda faaliyet gösteren birimler arasında; 2011 yılında *1. Ulusal Siber Güvenlik Tatbikatı*, 2012 yılında *Siber Kalkan Tatbikatı* ve 2013 yılında *2. Ulusal Siber Güvenlik Tatbikatı* gerçekleştirilmiştir. Farklı aşamalarla koordine edilen tatbikatlarda Türkiye'nin siber saldırı-savunma altyapılarna ilişkin tespitler ortaya konulmaya çalışılmıştır (Col ve Sagbansua, 2015: 53).

Türkiye'de siber güvenlik yapılanma faaliyetleri Tablo 9'da görüldüğü üzere 2012 sonrasında ciddi bir ivme kazanmıştır. Gerek TSK, gerekse TÜBİTAK ve bakanlıklar bünyesinde atılan adımlar koordinasyon birimlerinin oluşturulmasında, eylem planlarının yürürülüğe girişinde önayak olmuştur. Her ne kadar atılan adımların faaliyet boyutu hız kazansa da, pratikte yaşanan engeller gözden kaçırılmaması gereken hususların başında gelmektedir. Özellikle 2012 yılında, *Siber Güvenlik Kurulu*'nun faaliyete geçmesi ve 2013 yılında *Siber Güvenlik Dairesi*'nin kurulması yapıcı gelişmeler olmuş fakat teorinin pratiğe geçirilmesi konusunda yine sıkıntılar yaşanmıştır. *2013-2014 Eylem Planı*'nın bu eksikliği gidermesi beklenmiştir.

Tablo 9: Türkiye'de Siber Güvenlik Yapılanma Faaliyetleri

Haziran 2012	*TSK Siber Savunma Merkezi Başkanlığı kuruldu.*
Temmuz 2012	*TÜBİTAK Siber Güvenlik Enstitüsü kuruldu.*
Ağustos 2012	*UDHB ve TÜBİTAK ile Siber Güvenlik Projeleri oluşturuldu.*
20 Ekim 2012	*Siber Güvenik Kurulu faaliyete geçti.*
Ocak 2013	*UDHB Siber Güvenlik Dairesi kuruldu.*
20 Haziran 2013	*Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı yürürlüğe girdi.*
Şubat 2014	*5809 sayılı Elektronik Haberleşme Kanunu'na siber güvenlik temeli eklendi.*

Kaynak: Haberleşme Genel Müdürlüğü, 2014

Siber güvenlik farkındalığının artırılması, kurumların siber saldırı anında ve sonrasında koordinasyonlarının sağlanması için TÜBİTAK BİLGEM ve BTK tarafından düzenlenen *Ulusal Siber Güvenlik Tatbikatı*'nın ilki, Ocak 2011'de 41 katılımcı kurum ile gerçekleştirilmiştir. Daha büyük katılımlı ikinci tatbikat 2013 yılında düzenlenmiştir. 2012 yılında yapılan *Siber Kalkan Tatbikatı,* kamu ve özel sektör ortaklığı ile yapılmış ve 3G teknolojisini kullanan firmaların katılımına önem verilmiştir. *"Siber Kalkan Tatbikatı 2012",* port taraması ve DDoS türündeki siber saldırıları kapsamakta, erişim sağlayıcıların bu tip saldırılardaki kritik rolünü ön plana çıkarmaktadır (Kırdı, 2015).

2.3.9.1. Türkiye Bilimsel ve Teknolojik Araştırma Kurumu (TÜBİTAK)

TÜBİTAK 1963 yılında, Türkiye'de planlı ekonomi döneminin başlangıcında kurulmuştur. Kuruluş aşamasında en temel görevleri, özellikle doğa bilimlerinde temel ve uygulamalı akademik araştırmaları desteklemek ve genç araştırmacıları teşvik etmek, özendirmek olarak ortaya çıkmıştır. Bu görevleri yerine getirebilmek amacıyla, temel bilimler, mühendislik, tıp, tarım ve hayvancılık alanlarında dört araştırma grubu (şimdi on araştırma grubunu içeren Araştırma Destek Programları Başkanlığı) ile Bilim Adamı Yetiştirme Grubu (şimdi Bilim İnsanı Destekleme Daire Başkanlığı) oluşturulmuştur (https://www.tubitak.gov.tr).

Bünyesinde barındırdığı SGE ve UEKAE ile teorik altyapıyı pratiğe dökmeye çalışan TÜBİTAK, siber alanda eğitimler ve siber güvenlik geliştirmeleri ile Türkiye'de önemli bir boşluğu doldurmaktadır. 2008 yılında TÜBİTAK tarafından 8 kamu kurum ve kuruluşunun katılımıyla ulusal seviyedeki ilk siber güvenlik tatbikatı olan *"BOME 2008 Bilgi Sistem Güvenliği Tatbikatı"*; 2011 yılında TÜBİTAK ve BTK iş birliğiyle 41 kamu, özel sektör ve sivil toplum kuruluşunun katılımıyla *"Ulusal Siber Güvenlik Tatbikatı 2011"*; 2013 yılında Ulaştırma, Denizcilik ve Haberleşme Bakanlığı'nın koordinasyonunda TÜBİTAK ve BTK iş birliğiyle 61 kamu, özel sektör ve sivil toplum kuruluşunun katılımıyla *"Ulusal Siber Güvenlik Tatbikatı 2013"* gerçekleştirilmiştir.

Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı Türkiye'de siber güvenlik alanında temel olarak önemli bir belgeyi oluşturmuştur. Tablo 10 ve 11'de görüldüğü üzere özelllikle TÜBİTAK'ın sorumlu ve ilgili olduğu alanlardaki yelpazenin genişliği dikkat çekicidir ve ciddi bir yükü omuzlarında taşımaktadır. Tablo 10'da eylem planına göre TÜBİTAK sorumluluğundaki eylemler sıralanmaştır. Kritik altyapılar, kamu bilgi güvenliği, yazılım güvenliği ve AR-GE gibi konularda sorumlu hale gelen TÜBİTAK siber alana ilişkin faaliyet alanını daha da genişletmiştir.

Tablo 10: 2013-2014 Siber Eylem Planı ve TÜBİTAK Sorumluluğundaki Eylemler

Eylem No. 5	*Kritik Altyapılarda Bilgi Güvenliği Yönetimi Programı*
Eylem No. 6	*Kamu Bilgi Güvenliği Programı*
Eylem No. 10	*Yazılım Güvenliği Progarmının Yürütülmesi*
Eylem No. 18	*Açık Kaynak Kodlu Ürünlerin Kullanımının Teşvik Edilmesi*
Eylem No. 21	*Siber Güvenlik Uzmanlığına Yönlendirme Programının Yürütülmesi*
Eylem No. 26	*Siber Güvenlik Konusunda AR-GE Laboratuvarlarının Kurulması*

Kaynak: Türkiye Cumhuriyeti Ulaştırma Denizcilik ve Haberleşme Bakanlığı (t.y.), 2013-2014 Siber Güvenlik Eylem Planı

Tablo 11'de 2013-2014 eylem planına göre TÜBİTAK'ın ilgili olduğu eylemler yer almaktadır. Siber olaylarla mücadele, kritik altyapılara ilişkin konular, siber güvenlik alanındaki eğitimler, verilerin yedeklenmesi ve sızdırılmasına ilişkin konularda, AR-GE faaliyetleri, uluslararası alanda siber güvenlik etkinliklerinin düzenlenmesi gibi konularda

dolaylı olarak da ilişkilendirilen TÜBİTAK ciddi bir alanda söz sahibidir ve düzenlemeler yapabilme yetkisine sahiptir.

Tablo 11: 2013-2014 Siber Eylem Planı ve TÜBİTAK'ın İlgili Olduğu Eylemler[107]

Eylem No. 3	*Siber Olayların Delillendirilmesi*
Eylem No. 4	*USOM ve SOME'lerin Oluşturulması*
Eylem No. 5	*Kritik Altyapılarda Bilgi Güvenliği Yönetimi Programı*
Eylem No. 7	*Siber Güvenlik Eğitim Altyapısının Güçlendirilmesi*
Eylem No. 8	*Siber Güvenlik Tatbikatlarının Düzenlenmesi*
Eylem No. 9	*Kamu Güvenli İletişim Kurallarının Belirlenmesi*
Eylem No. 11	*Siber Tehditleri Önleme Projesinin Yürütülmesi*
Eylem No. 12	*Siber Güvenlik Konusunda Ürünlerin ve Hizmet Sağlayıcıların Belgelendirilmesi*
Eylem No. 14	*İç Sürekliliği ve Veri Yedekleme Sistemleri Kurulması*
Eylem No. 15	*Kamu Kurum ve Kuruluşlarının İnternet Sayfalarının Yerli Veri Merkezlerine Taşınması*
Eylem No. 16	*Veri Sızmasını Tespite Yönelik Test Altyapısı Geliştirilmesi ve Uygulamaya Alınması*
Eylem No. 17	*Kamu Kurumlarında Verilere Erişim Düzeylerinin Belirlenmesi*
Eylem No. 19	*Siber Güvenlik Konusunda Akademisyen Yetiştirilmesi*
Eylem No. 20	*Üniversitelerde Siber Güvenlik Eğitimlerinin Yaygınlaştırılması*
Eylem No. 21	*Siber Güvenlik Uzmanlığına yönlendirme Programının Yürütülmesi*
Eylem No. 22	*İlk, Orta, Lise Öğretimi ve Yaygın Eğitimde Siber Güvenlik Eğitimlerinin Yaygınlaştırılması*
Eylem No. 24	*Ulusal ve Uluslararası Siber Güvenlik Etkinlikleri Düzenlenmesi*
Eylem No. 25	*AR-GE Faaliyetlerinin Teşvik Edilmesi*
Eylem No. 26	*Siber Güvenlik Konusunda AR-GE Laboratuvarlarının Kurulması*
Eylem No. 27	*Siber Güvenlikte Yerli Ürün ve Çözüm Çalışmaları*

Kaynak: Türkiye Cumhuriyeti Ulaştırma Denizcilik ve Haberleşme Bakanlığı (t.y.), 2013-2014 Siber Güvenlik Eylem Planı

[107] TÜBİTAK; Eylem No. 5, Eylem No. 21, Eylem No. 26 üzerinde *Alt Eylemlere* ilişkin sorumluluklarının yanı sıra ilgili olduğu eylemlerle de ön plana çıkarılmıştır.

2.3.9.1.1. Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü (UEKAE)

TÜBİTAK enstitülerinden biri olan UEKAE, bilgi güvenliği haberleşme ve ileri elektronik alanlarında teknolojik çözümler üretmekte ve uygulamaktadır. 1972 yılında kurulan UEKAE kamu ve özel sektör kuruluşlarıyla ortak AR-GE projeleri üzerinde çalışmaktadır. Bünyesinde bulunan *Kripto Analiz Merkezi, Ürün Geliştirme Bölümü, Yarı İletken Teknolojileri Araştırma Laboratuvarı, EMI/EMC/TEMPEST Test Laboratuvarı, Akustik Test ve Analiz Laboratuvarı, Ortak Kriter Test Merkezi* ve *Optoelektronik Laboratuvarları* ile araştırma ve geliştirme çalışmalarını sürdürmektedir.[108]

UEKAE, bilgi güvenliği ve ileri elektronik teknolojileri alanlarında NATO'da aktif bir rol oynamaktadır. UEKAE'de geliştirilen kriptografik cihaz ve algoritmalarından NATO kullanımına uygun hale getirilenler, NATO Askeri Komitesi tarafından, NATO ve NATO'ya üye ülkelerin tüm gizlilik seviyelerindeki haberleşme ve bilgi güvenliğinin sağlanması yönünde onaylanmıştır (Çifçi, 2012: 374).

2.3.9.1.2. Siber Güvenlik Enstitüsü (SGE)

Ulusal siber güvenlik kapasitesinin artırılmasına yönelik çalışmalar gerçekleştirmek amacıyla kurulan *SGE,* faaliyetlerine 1997 yılında *Bilişim Sistemleri Güvenliği (BSG) Birimi* adı ile *TÜBİTAK UEKAE* altında başlamıştır. 2012 yılından bu yana ise TÜBİTAK BİLGEM bünyesinde ayrı bir enstitü olarak faaliyetlerini sürdürmekedir (Keleştemur, 2015: 176).[109] SGE, siber güvenlik alanında araştırma ve geliştirme faaliyetleri yürütmekte, askeri kurumlara, kamu kurum ve kuruluşlarına, özel sektöre yönelik projeler gerçekleştirmektedir (Keleştemur, 2015: 176). SGE bünyesinde verilen hizmetler şu şekildedir:

- *Bilgi Güvenliği Yönetim Sistemi (ISO/IEC 27001) danışmanlığı,*
- *Bilişim sistemi güvenlik testleri,*

[108] UEKAE, 2007 yılı itibariyle 8000 adedi aşkın kitap ve 80 farklı süreli yayın aboneliği ile kriptoloji ve bilgi güvenliği konusunda ülkemizin en büyük kütüphanesine sahiptir.

[109] BİLGEM temel olarak siber güvenlikle ilgili alanlarda görev yapmaktadır. Ayrıntılarına değinilen UEKAE ve SGE'nin yanında teknik konular başta olmak üzere görev yapan *Bilişim Teknolojileri Enstitüsü (BTE), Temel Bilimler Araştırma Enstitüsü (TBAE), İleri Teknoloji Araştırma Enstitüsü (İLTAREN), Yazılım Teknolojileri Araştırma Enstitüsü (YTE)* de alt birimler olarak faaliyetlerini sürdürmektedir.

- *Güvenli bilişim sistemi kurulum ve danışmanlığı,*
- *Açık kaynak kodlu çözümler,*
- *Bilişim sistemleri güvenliği eğitimleri,*
- *Araştırma geliştirme faaliyetleri,*
- *İş Sürekliliği Yönetim Sistemi (BS 25999) danışmanlığı,*
- *Yan kanal analizi,*
- *Bilgisayar olaylarına müdahele,*
- *Ortak kriter değerlendirmeleri.*

2.3.9.2. Türk Silahlı Kuvvetleri (TSK) Siber Savunma Merkezi Başkanlığı

TÜBİTAK UEKAE bünyesinde 2001 yılında kurulan *Bilişim Sistemleri Güvenliği Bölümü,* bu alandaki faaliyetlerine ilk önce TSK ile başlamıştır. Bunun yanında TSK; kara, deniz, hava harekat alanlarıyla birlikte, siber ortamda harekat kapasitesini artırmak için 2012 yılında *TSK Siber Savunma Merkezi Başkanlığı*'nı oluşturmuştur (Öğün ve Kaya, 2013: 168). Başkanlığın görev ve sorumluluğu, TSK'nın kullanmakta olduğu sistemlerin siber savunmasından oluşmaktadır.

Siber tehditleri önlemek, gelişmiş bir siber savunma ikaz ve püskürtme sistemlerinin oluşturulması amacıyla Ulaşım, Denizcilik ve Haberleşme Bakanlığı, TÜBİTAK ve diğer kamu kurumları ile koordinasyon içerisindedir. NATO ile de sürekli olarak ulusal ve uluslararası alanda ortaklaşa faaliyetler yürütülmektedir (Keleştemur, 2015: 177). NATO ile eşgüdümlü programlarının yanı sıra temel olarak faaliyetleri ve uygulamaları şu şekilde karşımıza çıkmaktadır:

- *TSK'nın kullandığı siber ortamda bulunan tüm sistemlerin siber savunmasını yapmak,*
- *Siber olaylara 7/24 esasına göre müdahele etmek,*
- *Ulusal olarak ve NATO tarafından icra edilen tatbikatlara katılım sağlamak,*
- *TSK çapında bilinçlendirme ve eğitim faaliyetlerini yürütmek,*
- *TSK tarafından kullanılan ağlarda düzenli olarak siber güvenlik denetleme ve testleri yapmak (Çifçi, 2012: 356).*

2.3.9.3. Emniyet Müdürlüğü İstihbarat Dairesi Başkanlığı

İçişleri Bakanlığı dahilinde, Emniyet Genel Müdürlüğü (EGM)'ne bağlı olarak çalışan bir kurumdur. Emniyet Genel Müdürü'ne doğrudan bağlı olarak faaliyet gösteren *İstihbarat Dairesi Başkanlığı*, *"32013 sayılı Emniyet Teşkilatı Kanunu"*na göre düzenlenen ve 13 Şubat 1989 tarihinde çıkartılan yönetmelik hükümlerine uygun olarak teşkilatlandırılmıştır.

Devletin, ülkesi ve milletiyle bölünmez bütünlüğüne, anayasa düzenine ve genel güvenliğine dair önleyici ve korucuyu tedbirler alma misyonunu edinmiştir. Ülke seviyesinde istihbarat faaliyetlerinde bulunmak, bilgi toplamak, değerlendirmek, yetkili mercilere veya kullanma alanına ulaştırma amaçları vardır. Devletin diğer istihbarat kuruluşlarıyla iş birliği yapmaktadır.

2.3.9.4. Ulaştırma, Denizcilik ve Haberleşme Bakanlığı

1 Kasım 2011 tarihli *"Ulaştırma Bakanlığının Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararname"* kapsamında görevleri belirlenmiştir. Siber Güvenlik Kurulu'nun faaliyetlerine başlamasında, siber güvenlik konusunda mevzuat çalışmaları yapılmasında, siber olayların delillendirilmesinde, USOM ve SOME'lerin oluşturulmasında, siber güvenlik eğitim altyapılarının güçlendirilmesinde, siber güvenlik tatbikatlarının düzenlenmesinde 2013-2014 eylem planında sorumlu olan kuruluşlar arasındadır.

Bakanlığın başkanlığında *Siber Güvenlik Kurulu* oluşturulmuştur. Siber Güvenlik Kurulu'nun sekreterya hizmetleri yürütülmekte ve ulusal siber güvenliğin sağlanması için politika, strateji ve eylem planları hazırlanmaktadır.

2.3.9.4.1. Siber Güvenlik Kurulu

2012'de yapılan düzenlemeyle hayata geçirilen kurul, siber güvenlikle ilgili olarak alınacak önlemleri belirlemek, hazırlanan plan, program, rapor, usül, esas ve standartları onaylamak ve bunların uygulanmasını, koordinasyonunu sağlamak amacıyla kurulmuştur. Kritik altyapılara ilişkin yapılacak müdahelelere karşı da görevleri tanımlanmıştır.

Ulusal siber güvenlik alanında yapılacak çalışmalar sürecinde, mümkün olan tüm alanlarda milli çözümler geliştirilmesi, yazılım ve donanım altyapılarında azami ölçüde milli kaynakların kullanılması esas alınmıştır. Kamu kurumlarında verilere erişim düzeyinin belirlenmesi, ulusal siber güvenliğin milli güvenliğe entegrasyonunda sorumlu kurum olarak 2013-2014 eylem planında yer almıştır.

2.3.9.5. Milli İstihbarat Teşkilatı (MİT)

MİT, 2937 sayılı *Devlet İstihbarat Hizmetleri ve İstihbarat Teşkilatı Kanunu*'na göre kurulmuştur. 2937 sayılı kanun devlet istihbarat faaliyetlerine ilişkin yegane kanundur. Bu kanun, devlet istihbaratının üretimi ve kullanılması ile Milli İstihbarat Teşkilatı'nın kuruluş, görev ve faaliyetlerine ait esas ve usulleri düzenlemektedir (Yılmaz, 2006: 373).

Yeni çıkarılan yasalarla teknik ve yasal altyapısı siber casusluğa karşı güçlendirilmiştir. Dış istihbarat, savunma, terör ve casusluğa odaklanılmıştır. Özellikle yabancı istihbarat birimlerinin imkan ve kabiliyetlerinin siber uzayda artması ve teknolojik olarak başdöndürücü şekilde gelişmesi MİT ile ilgili yasal düzenlemelerde daha da belirginlik kazanmıştır.

Dünyada ve Türkiye'de güvenlik şirketleri tarafından siber operasyonlara maruz kalma; işyeri, ev veya kamu kurumlarındaki bilgisayarlara erişerek yasadışı dinlemeler yapma, izleme ve kayıt vakalarının artması yabancı istihbarat ve yasadışı kurumların faaliyetlerini artırdığı alanlar olarak belirginleşmiştir. Bilişim teknolojisinin verdiği imkanlarla bu tür yasadışı faaliyetler yapılmasına karşı MİT teknik ve yasal olarak altyapıya kavuşturulmaya çalışılmaktadır.

2.3.9.6. Bilgi Teknolojileri ve İletişim Kurumu (BTK)

BTK, Türkiye'nin telekomünikasyon sektörünü düzenleyip denetleyen kurumdur. Türkiye'nin ilk sektörel düzenleyici kurumu olma özelliğine sahiptir. Bünyesinde bulunan *Siber Güvenlik Kurumu* ile siber saldırılara karşı mücadele yürütmektedir ve bu noktada kısmi olarak görev yetkisi geniştir.

USOM ve SOME'ler, BTK'ya bağlı olarak faaliyet göstermektedir. Telekomünikasyon aracılığıyla yapılan iletişimin tespiti, dinlenmesi, sinyal bilgilerinin değerlendirilmesi ve kayda alınmasındaki işlemler, bünyesindeki diğer birim olan *Telekomünikasyon İletişim Başkanlığı (TİB)* vasıtasıyla gerçekleştirilmiştir.

TİB, uzun yıllar Türkiye'de telekomünikasyon yoluyla yapılan iletişimin içeriğini kontrol etmekle yükümlü devlet kurumu olmuştur. 2005 yılının Ağustos ayında kurulmuş olan TİB, bugüne kadar MİT, emniyet ve jandarma istihbaratının ayrı ayrı birimler ve savcılıklardan aldıkları izinlerle gerçekleştirdikleri telefon dinlemelerindeki tek merkez halinde görev almıştır (Keleştemur, 2015: 175).

Türkiye'nin, uluslararası telekomünikasyon alanındaki standart organizasyonları ile ilişkileri TİB vasıtasıyla yürütülürken; söz konusu kuruluşlar nezdinde yürütülen çalışmalar kapsamında ilgili kuruluşlarla koordinasyonun sağlanması, Türkiye görüşünün hazırlanması ve alınan kararların uygulanması uzun yıllar bu kurum vasıtasıyla devam ettirilmiştir. 17 Ağustos 2016 tarihinde, olağanüstü hal (OHAL) kapsamında Resmi Gazete'de yayımlanan *"671 sayılı Kanun Hükmünde Kararname"* ile kapatılmıştır. Yapılan yeni düzenleme ile, TİB'e ilişkin görev tanımları daha önce bağlı olduğu BTK bünyesindeki merkeze kaydırılmıştır.

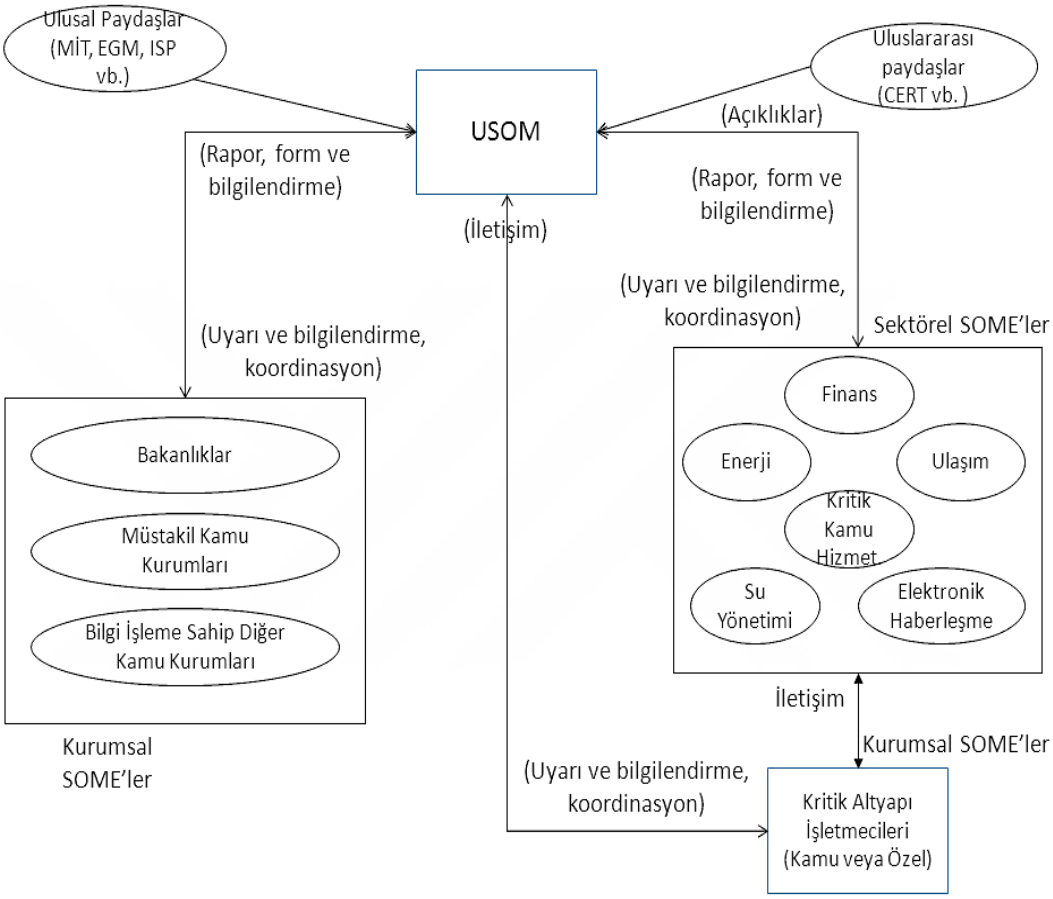
2.3.9.6.1. USOM ve SOME

Ulusal Siber Olaylara Müdahele Merkezi (USOM); internet aktörleri, kolluk güçleri, uluslararası kuluşlar, araştırma merkezleri ve özel sektör arasındaki iletişim ve koordinasyondan sorumludur. *Siber Olaylara Müdahele Ekipleri (SOME)* ise *Sektörel SOME* ve *Kurumsal SOME* olmak üzere ikiye ayrılmıştır:

- *Sektörel SOME'ler düzenleyici ve denetleyici kurumların bünyesinde kendi sektörlerinde faaliyet gösteren kurum, kuruluş ve işletmeleri kapsayacak şekilde kurulmaktadır. Kritik sektörlerde, sektörel SOME kurulması zorunludur.*
- *Kurumsal SOME'ler kurumlara doğrudan ya da dolaylı olarak yapılan veya yapılması muhtemel siber saldırılara karşı gerekli önlemleri alma veya kaldırma, bu*

tür olaylara karşı müdahele edebilecek mekanizmayı ve olay kayıt sistemlerini kurmakla yükümlüdürler.

Şekil 25: USOM Organizasyonu



Kaynak: Yalçın, 2014

ÜÇÜNCÜ BÖLÜM

3. ULUSLARARASI GÜVENLİK AÇISINDAN BİR YAKLAŞIM DENEMESİ: MİKRO SİBER İTTİFAK TEORİSİ (*MICRO CYBER ALLIANCE THEORY: Micro-CAT)*

"Siber savaşta oyun devam ettikçe, bir sonraki tırmanma turunda, ABD liderlerinin hızlı bir şekilde Çin'den daha fazla kaybedecek şeyleri olup olmadığına karar vermeleri gerekmektedir."

Richard A. Clarke

İki kutuplu yapıya dayanan Soğuk Savaş ve bitişi, yapay sınırları kaldırarak uluslararası ilişkilere yeni bir boyut katmıştır. Çok yönlü ve daha dinamik olan bu boyut içinde güvenlik kavramının algısal yapısının yeni tartışmaları ve farklı politika arayışlarını getirmesi ise olağan gözükmektedir.

Güvenliğin bile tanımı üzerinde kesin bir ifade kullanılamazken yeni bir yaklaşım geliştirebilme ve güvenliğin daha fazla anlam ifade edebilmesi adına devletlere ilişkin yeni politikalar sunabilme, bu çalışmada olduğu gibi fikirsel bir altyapı üzerinden sağlanmaktadır. Bu bölümde, çalışmanın bütününe ilişkin özellikle Türkiye gibi *"siber güvenlik"* alanında gelişmekte olan ya da gelişme arzusu duyan devletlerin atabilecekleri adıma ilişkin perspektif sunulmaya çalışılmıştır ve geliştirilip özgün bir niteliğe de sahip olabileceği düşünülerek *Mikro Siber İttifak Teorisi (Micro Cyber Alliance Theory, Micro-CAT)* adı verilmiştir.

3.1. Uluslararası Güvenlikte Politika Üretme Sorunu

Uluslararası siyaset açısından güvenliğin içeriği, korunması gereken değerle birlikte üretilecek politikanın nasıl olması gerektiği sorusuna verilecek cevapla şekillenmektedir. Güvenlik açısından "*Kimin güvenliği?"* ya da "*Neyin güvenliği?"* sorularının cevabı güvenlik politikalarının temelini oluşturmaktadır. Güvenlik çalışmalarında bu soruların

cevapları *"devlet odaklı güvenlik"* ya da *"birey odaklı güvenlik"* olması açısından iki temel yaklaşımı ortaya çıkarmıştır (Birdişli, 2016: 21).[110]

Devletin yaşamsal sınırları vardır ve bu sınırlar dahilinde uluslararası politikada aktör olma konumu güçlendirilerek güvenlik çerçevesi oluşturulmaktadır. Devlet odaklı güvenlikte var oluş ve bu varlığı devam ettirme adına kimi zaman başka devletlerdeki bireyler göz ardı edilebilmekte, müdaheleler gerçekleştirilebilmekte ya da yaşanan olaylara sessiz kalınabilmektedir. Realist paradigmanın da sık sık atıf yaptığı bu durumla ilgili insan doğasının güvenilmezliği devlet odaklı güvenlik anlayışını güçlendirmektedir.

Yaşam hakkı, inanç özgürlüğü ya da mülkiyet hakkı gibi temel hak ve özgürlüklere ilişkin devletin güvenlik politikaları oluşturması ve bu politikaların merkezinde bireyin olmasına ilişkin görüşler ve çalışmalar da bir hayli fazlalaşmıştır. Siber güvenliğin içerdiği kavramsal çeşitlilikle birlikte birey-devlet ilişkisi, teknolojik gelişmelerle birlikte uluslararası yapılanmaların etkileşimi bu tartışmalar içerisinde politika üretiminde inşacı perspektifi ön plana çıkarmaktadır.

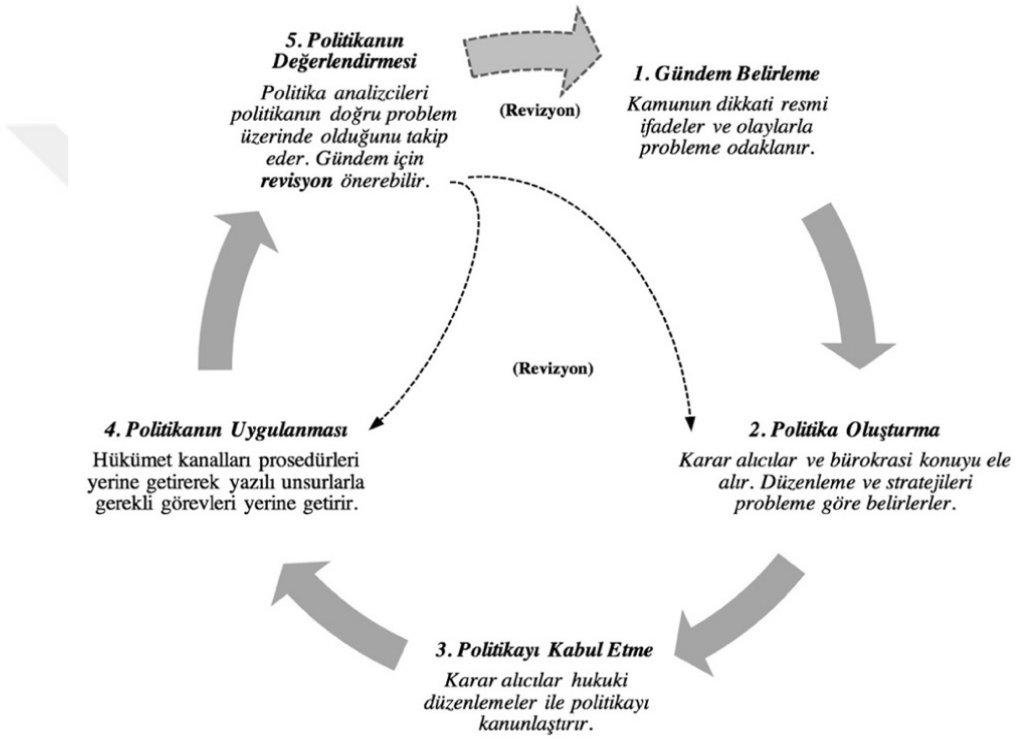
Uluslararası güvenlik açısından, devlet-birey-güvenlik üçgeninde karar alıcıların politika üretmesi ve bunun siber uzayda karşılık olarak çıkarsal bir döngü haline gelmesi, en az teorik yaklaşım kadar önemlidir ve ciddi bir birikim istemektedir. Bu durumu önemli kılan ise kimi zaman tehdit algısının ortaya çıkması ve doğru algılanması, kimi zaman ise çıkarsal bir durumun arzulanmasıdır. Sonuç olarak devletlerin varlık sebebi bu mücadelede üstün gelinmesidir.

Üretilecek politikaların teorik çerçevesi sosyal bilimler gibi alanlarda kurgusal olarak daha zordur ve oluşturulan politik çerçeve de bir o kadar temel düzeyde kalmaktadır. Uluslararası güvenliğe ilişkin sergilenecek bir yaklaşımın temeli, uluslararası politikada teori oluşturulmasıyla benzerlikler göztermektedir. Sönmezoğlu (2014: 94) teori oluşturmaya ilişkin başlıca üç noktayı şu şekilde tanımlamıştır:

[110] Farklı yaklaşımlar arasında *"siber güvenlik"* ve *"ulusal güvenlik"* gibi kavramların resmi dokümanlarda kullanılışında doğrudan bir kıyaslama yapılmaktan kaçınılmaktadır. Bunun sebebi "siber güvenlik" kavramının kabul edilen ortak bir tanımının olmayışıdır (Hathaway ve Klimburg, 2012:20).

- *Teoriyi oluşturan önerme ve genellemelerin birbirleri ile mantıklı ve tutarlı bir bağlantı içerisinde bulunmaları,*
- *Bu önerme ve genellemelerin olgularla bağlarının kurulabilmesi,*
- *Sözkonusu önermelerin belirli ölçülerde betimleme, açıklama ve tahmin kapasitesine sahip olmaları gereği.*

Şekil 26: Politika Oluşturma Diyagramı



Kaynak: The Texas Politics Project, 2016

Uluslararası politika açısından yaklaşacak olursak siber savaşlar için de benzer bir teori oluşturma mantığından söz edebiliriz. Örgütler, bireyler, uluslararası kuruluşlar ve devletler düzeyindeki farklılık, analiz düzeyini inşacı teoriye yaklaştırmaktadır. Olayların siber uzayda kendi içerisindeki döngüsel ağı, politik bir düzlem oluştururken, teori oluşturma mantığıyla benzer işlemektedir (Sard, 2014:4). Bu noktada güvenlik ikileminin siber boyutta ne ifade ettiği, küresel risk toplumunda siber politikalar ve doğal olarak karşımıza çıkacak yeni güvenlik algısı çerçeveyi ana hatlarıyla anlamamıza yardımcı olacaktır.

3.1.1. Güvenlik İkileminin Siber Uzayda Aşılması

"Güvenlik İkilemi (security dilemma)"[111] kavramı hem Uluslararası İlişkiler disiplini, hem de karar alıcılar için üzerinde düşünülmesi gereken önemli bir husustur. *Güvenlik ikilemi* en temel anlamıyla bir devletin başka devletten tehdit algılayıp silahlanması durumunda, bunu tehdit olarak algılayan devletin de aynı şekilde cevap vermesi anlamına gelmektedir. Karar alıcılar, güvenlik sorunlarını nasıl çözebilecekleri konusunda farklı seçeneklerle karşı karşıya kaldıkları sürece güvenlik ikilemi hep var olacaktır.[112]

Güvenlik kaygısını ortadan kaldırma adına yasa ya da yasal bir otorite olmadığı için devletler kendi güvenliklerini kendileri sağlamakta ve kimi zaman sorunun temeline ilişkin benzer ülkelerle ortak hareket etmektedir. Her devletin kendi bünyesinde alternatifler üretmesi ve silahlanma gibi benzeri adımlarla hareket etmesi güvenlik ikilemi açısından diğer devletin güvenliğinin de azalması anlamına gelmektedir. Güvenlik ikilemi bu noktada alana ilişkin paradoksların başında gelmektedir (Karabulut, 2015: 40).

Özellikle Soğuk Savaş sonrası dönemde *güvenlik ikilemi* kavramının gelişmesinde önemli parametreler vardır. Bunlardan ilki yeni güvenlik sorunlarının artan şekilde dünya siyasetini etkilemesidir. İkinci durum ise, sorunlar uluslararası ilişkiler disiplininin dünya politikasına bakışı, sorunları algılayışı ve tanımlayışında değişikliklere yol açmıştır (Bilgiç, 2012: 339). Özellikle silahlanma yarışı hız kesmeden yoluna devam ederken, siber güvenliğe ilişkin algı da devletleri birbirlerine karşı önlemler almalarına ve harcamaların artışına neden olmuştur (Tang, 2009: 590).

Dünya siyasetini meşgul eden siber güvenlik yeni olmasının yanında, güvenlik ikilemi açısından uluslararası ilişkiler disiplinine siber savaş olgusunu da eklemiştir. Savaş olgusu ise pratikte çoğu zaman birlikteliklere ve ortak güvenlik kaygısına sebep olmuştur. Devletler arasındaki siber mücadelenin boyutu da konvansiyonel mücadelenin temelindeki

[111] *Güvenlik ikilemi*, uluslararası ilişkiler terminolojisine John H. Herz'in yazdığı *Politik Realizm ve Politik İdealizm* kitabıyla girmiştir. Ayrıca yine aynı döneme ait Hurbert Butterfield'ın *Tarih ve İnsan İlişkileri* adlı kitabında da benzer bir durum farklı bir üslupla dile getirilmektedir.

[112] *Güvenlik ikilemi* kavramının ilk ortaya konuş biçimi, Soğuk Savaş döneminde disipline egemen olan realist düşüncenin öğelerini yansıtır. Öncelikle, güvenlik ikilemi kavramı devlet-merkezci bir yaklaşım dahilinde üretilmiştir.

çatışma olgusuyla örtüşmeye başlamıştır ve devletler bu konuda saldırı unsurlarını geliştirme seçeneklerini masaya koymuştur.

Uluslararası alanda egemenlik tartışması sadece çatışmaların oluşması yönünde adımları getirmemektedir. Aynı zamanda statükoya ilişkin ortak çıkar halini de beraberinde getirmektedir. Devletlerin farkında olduğu şey anarşinin, statükonun dağılması durumunda kötüye gidişi cesaretlendirici etki yaptığıdır (Jervis, 1978: 167). Siber uzaydaki faaliyetler tam bu noktada söz konusu durumu teşvik edici niteliktedir. Siber uzayda güvenlik ikileminin geldiği nokta, gelişen her unsurun savaşa ve çatışmaya neden olabileceği yönündeki yaklaşımla daha çok örtüşmektedir.

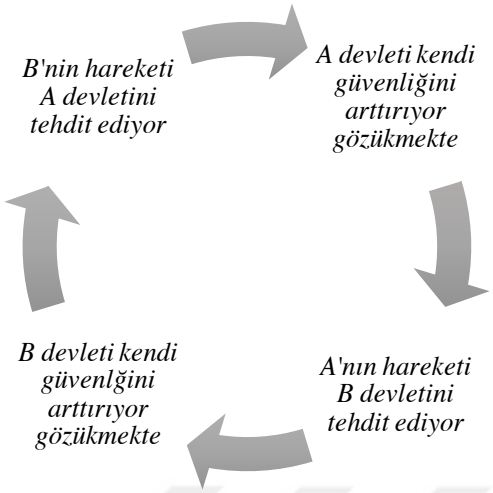
Neden olunan çatışma, sadece çıkarsal veya egemenlik alanına ilişkin mücadelenin sonuçlarını birer çıktı olarak devletlere vermemektedir. Örneğin; 1998 yılında ortaya çıkan ve Çernobil Virüsü olarak da bilinen CIH virüsü, 1999 yılında etkin hale gelmiş ve birçok kullanıcının verilerini kaybetmesine yol açmıştır. 2000 yılında Mellisa, Love Bug ve Killer Resume gibi büyük mali kayıplara neden ola virüsler yine bu durumun çeşitliliğine ilişkin bir örnektir (Bayraktar, 2015: 155).[113]

Gelişen her unsur sahip olduğu altyapıyla birlikte devletlerin çıkar arzusunu körüklemektedir. Güvenlik ikileminin de temelinde bu durum vardır. Uluslararası ortamda güvenlik oluşturma adına caydırıcı olma, kendi sınırlarını aşıp çatışmaya dönüşmektedir (Booth, 2012: 481). Uluslararası düzenleme ve yasa koyucu olmadıkça şartlar daha da ağırlaşmaktadır. Konu kendi içerisinde döngüsel bir soruna dönüşmektedir. Şekil 27'de görüldüğü üzere A devletinden tehdit algılayan B devleti silahlanabilmekte, ittifaklara katılabilmekte ve siber mücadele içinde siber saldırı seçeneklerini kullanabilmektedir. Fakat B devletinin silahlanması bu kez A devletinin güvenlik kaygılarını ön plana çıkarmakta ve bu durumda A devleti de silahlanma kapasitesini artırmaktadır.[114]

[113] Diğer bir husus ise siber uzayın toplum ve kitle hareketleri üzerindeki etkisini gösteren Facebook, Twitter, Youtube gibi sosyal paylaşım siteleri üzerinden yaşanan Arap Baharı örneğidir. Arap Baharı'nı *"Facebook Devrimi"* olarak nitelendiren ve Arap Baharı'nda sosyal medyanın gücü görüldükten sonra, siber uzayın politik gücünün önemli bir savaş yeteneği olduğunu niteleyenlerin sayısı oldukça fazladır.

[114] Türkiye ve Yunanistan'ın 1990'lı yıllar boyunca birbirlerine karşı silahlanmaları bir güvenlik ikilemi oluşturmuştur. Özellikle yakın coğrafyalarda sorunlar yaşayan devletlerin attıkları her adım belirli düzeylerde tehdit boyutu dahilinde algılanmaktadır.

Şekil 27: Ülkeler Arasındaki Güvenlik İkilemi Diyagramı



Kaynak: Krickovic, 2016: 116

3.1.2. Küresel Risk Toplumunda Siber Politikalar

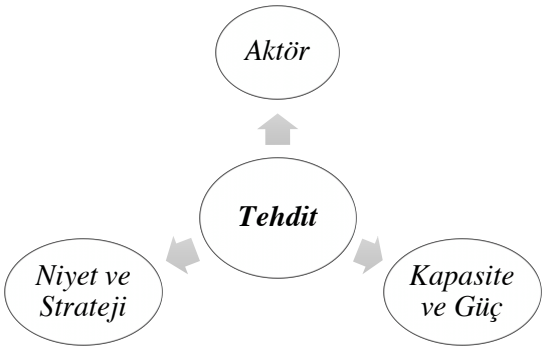
Modernliğin beraberinde getirdiği çevresel, ekonomik ve güvenliğe ilişkin kimi riskleri konu alan *risk toplumu* yaklaşımı, riskin sosyolojik boyutunu inceleyen çalışmalar arasında önemli bir yere sahiptir. Modern toplumların birer risk toplumu haline dönüştükleri iddiasına ilişkin tartışmalar büyük oranda Çernobil'deki nükleer facia sonrasında alevlenmiştir (Elmas, 2013: 101).[115]

Şekil 28'de görüldüğü üzere Soğuk Savaş döneminde tehdidin boyutları aktör, strateji ve güç arasında sıkışmışken günümüzde bu duruma öngörülemez tehditler de eklenmiş ve risk toplumu yaklaşımı açısından gelişmeleri olumsuz yönde etkilemiştir. Coğrafi olarak kırılganlıkların artışında risk toplumu yaklaşımıyla açıklanabilecek ciddi veriler vardır.[116] Risk toplumu açısından oluşturulacak politikalarda tehdidin çok yönlülüğü içerisine siber tehditler de yerleşmiştir.

[115] Çernobil gibi kaza anında sebep olduğu yıkımlardan ziyade bu gibi teknoloji ürünü facialarn meydana getirdiği asıl problem, bilimsel otoritelerin geleceğe dair topluma inanılır cevaplar verememesi ve buna bağlı olarak da bireylerin gelecek yaşamlarının kendilerine ne getireceğini kestirememesinde yatmaktadır.

[116] Risk toplumu tartışmalarına ilişkin yaklaşımı sadece felaket toplumuna dönüşüm olarak algılamamak gerekir. Anthony Giddens (1998), bu duruma ilişkin şu tespiti yapmaktadır: *"Risk toplumu düşüncesi, dünyanın daha tehlikeli bir hal aldığını iddia ediyormuş gibi görünebilir, ancak bu gerçekte böyle değildir. Aksine bu,*

Şekil 28: Soğuk Savaş Döneminde Tehdidin Üç Boyutu



Kaynak: Williams, 2005: 7.

Özellikle 11 Eylül 2001 tarihindeki İkiz Kuleler'e saldırı uluslararası güvenlik politikaları, toplumsal analizler açısından en az Soğuk Savaş'ın sona erdiği Berlin Duvarı'nın yıkılışı kadar önemli bir yere sahiptir. Alman sosyolog Ulrich Beck (2009: 157), ortaya attığı risk toplumu kavramı ile beraber küresel terörizm probleminin bu noktaya gelişinde Batı medeniyetinin teknoloji, ordu ve disiplin aracılığıyla Asya'dan Amerika'ya siyasi anlamda baskın bir rol izlemesinin önemli rol oynadığını düşünmektedir.

Teknoloji, ordu ve disiplin modern toplumların gündemine dahil etttiği siber güvenlik politikalarının yönünü değiştirmiştir. Sadece teknolojik gelişmelere ilişkin riskler değil, aynı zamanda uluslararası alanda yeni bir mücadele alanı olarak toplumların değişen riski haline gelen siber savaşlar kaygıları artırmıştır. Geçmişte yaşanan facialar bilinen haliyle kaza gibi görünse de, devletlerin ve farklı grupların kritik altyapılara müdahele edebilir yöndeki gelişmişlikleri ve olanaklar *küresel risk toplumu yaklaşımıyla* örtüşmekte, teknik ve bilimsel ilerlemenin, bireyin hayatını daha da kolaylaştıracağı yönündeki savunma geri planda kalmaktadır.

Elmas (2013: 113) risk toplumunda belli risklerin gerçek olması durumunda ortaya çıkabilecek kimi felaketlerin varlığından bahsetmekte ve bu felaketlerin kontrol edilemeyen etkilerinin söz konusu olduğunu vurgulamaktadır. Bu durum risk toplumu yaklaşımının kaos ve anarşi dolu yeni bir toplum modeli ortaya koymaya çalıştığı şeklinde

devamlı artan bir biçimde geleceği üzerine kendisini meşgul ederek risk düşüncesini ortaya çıkaran bir toplumdur."

değerlendirilmemelidir. Bu yaklaşım modern sanayileşmenin ve modern teknolojilerin dolaylı olarak ve istemeden sebep olduğu etkilerinin, modern kurumlar tarafından kontrol edilememesi ve nasıl yönetileceğinin bilinememesi durumunu tartışmaya açmaktadır. Siber politikalar oluşturma ya da oluşturamama arasındaki itici güç de bir yönüyle buradan kaynak almaktadır.

Siber politikalar oluşturulması ve uluslararası alanda etki doğurmasına ilişkin risk toplumunun algısal değişimi ve gelişimi önemli bir çerçeveyi oluşturmaktadır. Kritik altyapılara ilişkin oluşabilecek tehlikeli girişimler moderniteyi karşı bir silaha dönüştürebilir. Karar alıcıların algısal düzeyi ve gelecek vizyonu moderniteyle doğru orantılı şekilde yükselmelidir.[117]

3.1.3. Yeni Güvenlik Algısı ve Siber Uzay

Küreselleşme süreci ile birlikte güvenliğe yönelik tehditlerin farklılaşması yeni bir güvenlik tanımlamasını gerekli kılmıştır. Geleneksel tehdit algılamaları ve bu unsurlarla mücadele yöntemleri yeni güvenlik tehditleriyle mücadele konusunda yetersiz kalmaktadır. Bu yetersizlik yeni bir güvenlik tanımlamasının yanı sıra bu tanımlamadan hareketle yeni mücadele araçlarını da devreye sokmayı gerekli kılmaktadır (Karabulut, 2015: 119). Yeni mücadale araçları ise sadece fiziksel ya da sanal boyuttaki unsurları kapsamamaktadır. Toplumlar arasındaki hareketlenmeler ve çoğu zaman bu toplumlar arasındaki dini ve etnik farklılıklar dahi kapsam dahilinde olabilmektedir.

Mücadele araçları içerisinde, gelişimini ve farklılaşmasını hızla sürdüren siber saldırı araçları geleneksel tehdit anlayışını yeni güvenlik yaklaşımı içerisinde belirginleştirmiştir. NATO'nun tehdit tanımlamaları, ABD'nin özellikle siber güvenlik alanında vermiş olduğu öncelik ve yeni bir harekat alanı oluşturan siber savaş bu temel değişim içerisinde en somut tespitlerdir.

[117] Danışmanlık şirketi Marsh&McLennan'ın Davos Zirvesi için hazırladığı *"2016 Yılı Küresel Riskler Raporu"* çevresel sorunlardan zoraki göçe, enerji fiyatlarından siber saldırılara kadar birçok alanda dünyanın en riskli dönemini yaşadığını ortaya koymuştur. Raporda ilk kez; beş kategoriden dördü, yani çevresel, jeopolitik, toplumsal ve ekonomik riskler ilk beş en yüksek etkiye sahip riskler arasında yer almıştır. Teknolojik risklere de dikkat çekilirken, siber saldırıları kapsayan teknoloji riski hem gerçekleşme olasılığı hem de etkisi bakımından 11. sırada yer almıştır. Siber saldırılar, 27 ekonominin ilk beş riski arasında yer almaktadır.

1990'lardan itibaren küreselleşme olgusunun hız kazanmasıyla *"artık hiçbir şey eskisi gibi olmayacak"* sözünü doğrularcasına, her alanda çok hızlı ve önüne geçilemez bir değişim süreci başlamıştır. Böylece önceki devirlerde benimsenen ekonomik, politik ve güvenlik stratejilerinin dayandırıldığı parametrelerin çoğunun sarsıldığı ya da ortadan kalkmaya yüz tuttuğu bir sürece girilmiştir. Bireyler arasında etkileşimin arttığı günümüzde politik alan farklı unsurlarıyla genişlemeye başlamıştır.

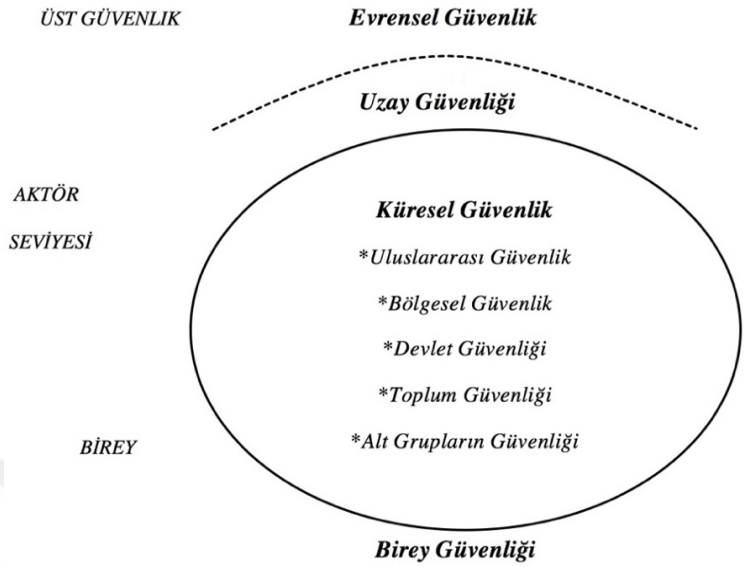
Soğuk Savaş sonrası dönemde küreselleşme sürecinin itici gücüyle tehdit olgusunda niceliksel bir artış, niteliksel boyutta bir çeşitlenme meydana gelmiştir. Bu yeni dönemde, öncelikle askeri olduğu kadar ekonomik, sosyal, dini ya da kültürel, ideolojik, çevresel, toplumsal ve sağlıkla ilgili yeni tehdit unsurları ortaya çıkmıştır (Erdoğan, 2013: 269). Siber terör de bu boyutta etken bir araç olarak yerini almıştır.[118] Siber terörün kendi içerisindeki boyutsal nitelik ile uzayda yapılan çalışmalar, insanların sosyal hayatta yaşadıkları her yeri içerisine dahil etmiştir (Der Derian, 2009: 121).

Güvenliğin derinleşmesi ve genişlemesi, temel olarak güvenlik tehditlerinin çoğalmasıyla doğru orantılı bir süreçtir. Bunun yanı sıra tehditlerin küresel bir şekilde ele alınmasının gerekliliği, tehditlerin teknolojik gelişim ve küreselleşme gibi etmenlerle daha yaygın bir hale gelmesidir. Bu bağlamda güvenlik, küreselleşme ve teknoloji ilişkisini irdelemek gerekmektedir. Küreselleşme ve teknolojinin ortaya çıkardığı akışkanlık ve sınırların geçirgenliği, bireye ve devlete yönelik tehditlerin dozunu da artırmıştır (Aksu ve Turhan, 2012: 71).

Yeni güvenlik anlayışının siber güvenlik boyutu, Şekil 29'da görüldüğü üzere tüm güvenlik unsurlarının temelde, belirli verilere sahip olmasıyla da kapsayıcılık açıdan en üst düzeyde yer almaktadır. Küresel güvenlik açısından ele alınan tüm unsurlar uzay boşluğunda teknolojik unsurlarla birbirlerine yakınlaştığı ölçüde siber teröre maruz kalabilecektir ve sorunsal alan daha da genişleyecektir. Verilerin artan bir hızla entegre edildiği siber alan kaygıları daha da artırmaktadır.

[118] Küreselleşmenin, dolayısıyla *kültürel emperyalizmin* aktörleri olarak algılanan gelişmiş ülkelere karşı gösterilen reaksiyonların belki de en basit örneği tek kişilik ordu konumuna gelebilmiş hackerların siber ortamda gerçekleştirdikleri saldırılar olmuştur.

Şekil 29: Güvenliğin Katmanları



Kaynak: Yılmaz, 2014: 12

3.1.4. Güvenliğin Bölgeselleşmesi ve Siber Politikalar Oluşturma

Bölgesellik ve güvenlik birbiriyle pek çok farklı şekilde ilişkilendirilebilmektedir. Özellikle Barry Buzan'ın (1991: 190), *"bir grup ülkenin temel güvenlik kaygılarının, gerçekçi bir şekilde birbirinden ayrı düşünülemeyecek kadar birbirine bağlanması"* şeklindeki tarifi özellikle siber güvenlik açısından ve çalışma kapsamında oluşturulmasının düşünüldüğü siber ittifak teorisi açısından açıklayıcıdır. Bölgesel olarak çatışmalarda, devletler arasındaki belirleyici faktörler siber politikaları etkilemektedir ve ittifak arayışında yakın coğrafyadan uzaklaşılmasını sağlamaktadır ki bu durum, siber politikalar açısından çoğu zaman tehlikeli bu durumdur.

Özellikle kritik altyapılar açısından, yakın coğrafyalardaki ülkelerin birbirine bağlılığı düşünülecek olursa ittfak arayışının ve siber politikalar oluşturmada güvenliğin bölgeselleşmesi bu çalışmadaki yaklaşım açısından önem kazanacaktır. Bu yaklaşım ile ilgili olarak özellikle Türkiye gibi ülkelerin çevresindeki devletlerde, siber saldırılara ilişkin olay döngüsü, yakın coğrafyalardaki birliktelikleri gerekli kılmaktadır. Bunun temelindeki etken tarihi bütünlük ve hafızadır.

Şu ana kadar dünyanın farklı bölgelerinde oluşturulan bölgesel güvenlik çerçeveleri, Avrupa dışında gelişme aşamasındadır ya da başarıya ulaşamamıştır. Bundaki temel etken, devletlerin *Avrupa Birliği* yapılanmasına her yönden benzemeye çalışmasıdır. Avrupa'nın bu konudaki çıkarımı tarihsel olarak gergin ve savaşa eğilimli Almanya-Fransa çatışmasının tanımladığı güvenlik yapısını, bölgesel iş birliği ile savaşın artık çatışmaları çözebilmek için seçenek dahi olmadığı bir güvenlik topluluğuna dönüştürmüştür ve ciddi bir supranasyonal nitelik ortaya çıkmıştır (Hettne, 2012: 357).

Siber politikada çıktılar oluşturma adına genelde G-8, özelde ise bu çatı altındaki İngiltere, Fransa, Almanya, İtalya ile Japonya, Kanada, Rusya ve ABD arasındaki siber suçlarla olan mücadelede güvenliğin bölgeselleşmesi açısından eldeki veriler kayda değerdir. Yapılan toplantılarda, 1995 yılından beri bölgesel gelişmelerle birlikte siber suçlarla mücadele konusu ele alınmaktadır. Bu toplantılar neticesinde çalışma grupları oluşturulmuş, siber suçlarla mücadelede eylem planları hazırlanmış ve faaliyete geçirilmiştir.

Diğer taraftan *Siber Savunma Politikası* hedefi altında NATO, siber saldırılara karşı önem teşkil eden tüm iletişim ve bilgi sistemlerinin korunmasını, ittifak üyelerine sağlamak için NATO yeteneğinin kuvvetlendirilmesi hususunda müdahelelerde bulunmuştur. NATO'nun en üst karar organı olan Kuzey Atlantik Konseyi, *Siber Savunma Programı*'nı desteklemektedir (Keleştemur, 2015: 440).[119]

Etkileşimin yoğunluğu siber politikalar oluşturma açısından güvenliğin bölgeselleşmesi adına karşımıza daha önce örneklerini verdiğimiz; G-8, NATO gibi yapılanmalara benzer şekilde örgütlenme mantığını ve politikalar üretme gereğini karşımıza çıkarmaktadır. Çalışmanın konusunu da oluşturan ittifak anlayışının oluşmasında yakın çevredeki gelişmeleri takip etme ve siber güvenlik adına bu gelişmeleri doğru okuyabilme, iş birliği oluşturulabilmesi adına daha kazançlı gözükmektedir. Siber alanda girişimler, günümüz gerçekliğinde rasyonel boyutlarda tartışılmalıdır.

[119] NATO da tıpkı ülkeler gibi siber saldırılara maruz kalmaktadır. Özellikle yığın e-posta saldırıları, web sitelerinin çökertilmesine yönelik saldırılar ve NATO sunucularına karşı sürekli saldırılar düzenlenmektedir. Diğer taraftan NATO, siber casusluk faaliyetlerinin de artmakta olduğunu, bu konuyla ilgili olarak da İKK faaliyetlerinin artması ve güçlendirilmesi gerektiğini belirtmektedir.

Güvenliğin bölgeselleşmesi perspektifinden bölgesel iş birliği, bölgesel bütünleşme ve bölgesel birlik açısından ülke içi yapılanma da önemli bir yere sahiptir. Bölgeselleşme düzeyinin gevşek olduğu bölgesel iş birliğinde bu yapılanma sorunlara sebep olabilmektedir ve bu yüzden daha küçük, mikro yapılarda bölgesel birlikler daha da yapıcı kararlar alabilmektedir ve manevra yetenekleri daha kuvvetli olabilmektedir.

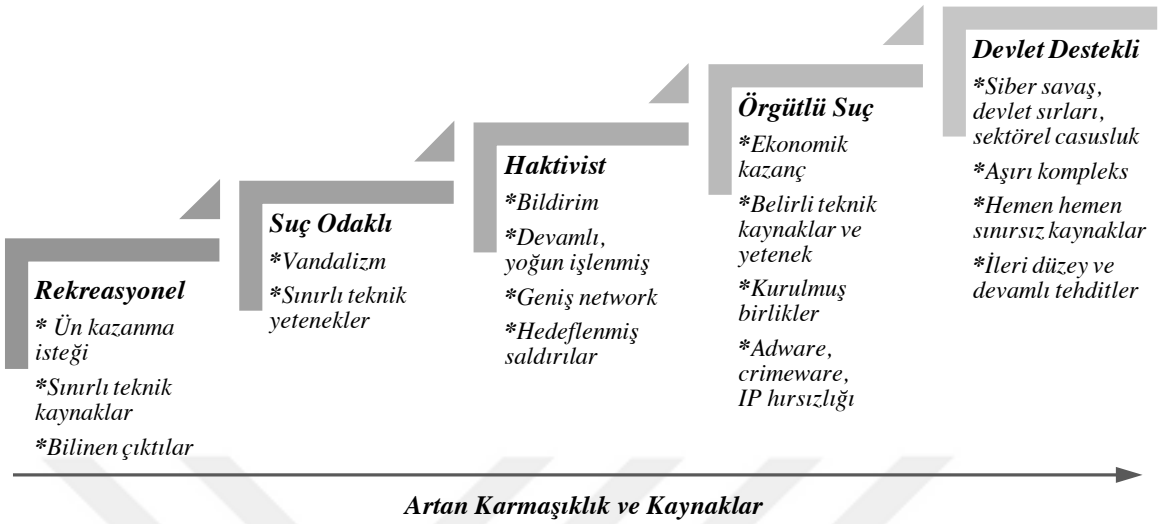
3.2. Değişen Uluslararası Sistemde Siber Güvenlik Yaklaşımı Oluşturma

Güvenlik çalışmalarının tarihi, sosyal bilimlerin ilerlediği mekanizmaları uluslararası güvenlik temelinde ortaya koymaktadır. Uluslararası ilişkilerin geri kalanı gibi güvenlik çalışmaları da bilginin diğer dallarından faydalanmıştır. İlerlemenin diğer kaynağı da rakip teoriler arasındaki mücadeledir. Rekabet, mücadele eden yaklaşımların argümanlarını incelemeye ve daha iyi ampirik destek aramaya teşvik etmektedir (Walt, 2003: 101).

Siber güvenlik yaklaşımı oluşturma da farklı yaklaşımlar arasında kimi zaman komplo teorileri, kimi zaman gelecek beklentileri arasında zorlaşmaktadır. Özellikle sosyal bilimler içerisinde uluslararası ilişkilere dair konuların eklektik düzlemde ele alınması ve tartışılması, siber güvenlik gibi konularda bölgeler arası ayrım yapmada ve strateji geliştirmede bazı zorluklar içermektedir.

Siber güvenlik içerisinde zaman ve mekan algısının klasik çatışmalara göre farklı şekillerde ortaya çıkışı, saldırgan profillerinin farklı düzeylerde ve amaçlarda faaliyetlerini sürdürüşü güvenlik yaklaşımı oluşturmada zorlaştırıcı unsurlardır. Şekil 30'da görüleceği üzere, saldırı ve savunma perspektifinde siber güvenlik; bireylerin sınırlı teknik kaynaklarıyla oluşturdukları saldırılardan, devlet destekli siber orduların saldırı ve savunma kapasiteleriyle çok daha geniş bir alana yayılmıştır. Her düzeyde farklı kaynaklara ihtiyaç duyulmaktadır ve bu konuda daha ileri altyapılara ihtiyaç artmaktadır. Artan kaynaklar ve kapasitesi genişleyen aktörlerle birlikte karmaşıklık daha da fazlalaşmaktadır. Farklı düzeylerdeki aktörlerin, çatışma kültürü içinde siber güvenlik alanındaki çıkar mücadeleleri profillerin daha da çeşitleneceği imajını ortaya koymaktadır. Uluslararası ilişkilerdeki boyutu da bu yaklaşımla birlikte genişleyecektir.

Şekil 30: Değişen Saldırgan Profilleri



Kaynak: McAfee Labs Threat Report, 2015: 9

Uluslararası sistem kendi içinde değişimini, kendine has özellikler ile sağlarken stratejik bir değişim algısı oluştuğu yadsınamaz bir gerçekliktir. Stratejik sorunlar ve siber güvenlik temelinde geleneksel tehditlerle birlikte siber tehditlerin de dönüşümü bu temeli farklılaştırmaktadır. Güvenlik stratejilerini siber uzayda uygulayabilme ve ittifak oluşturabilme mantığı bu ana başlık içerisinde irdelenerek bir yaklaşım ortaya konulacaktır.

3.2.2. Stratejik Değişim Algısı ve Siber Uzay

Genel olarak aktörler güvenlikleri adına öncelikle barışçıl stratejiler denemektedirler, bunlardan amaçları doğrultusunda sonuç alamadıklarında ya da alamayacakları algısı oluştuğunda çatışma stratejisine yönelmektedirler. Hangi türü seçilirse seçilsin, güvenlik stratejilerinin tümü belirli yöntemler ve operasyonlar içermektedir. Bu yöntemlerin yine hemen hepsi, şiddet ya da şiddet kullanma tehdidi içermektedir (Dedeoğlu, 2003: 108).

Şiddet ve şiddet kullanma tehdidi ile birlikte, küreselleşme sürecinin güvenlik alanına etkisi genellikle yeni tehditler üzerine odaklanılarak ele alınmıştır. Bu yaklaşım doğru olmakla birlikte eksik kalmaktadır. Küreselleşmenin ortaya çıkardığı tehditler konunun yalnızca bir yönünü temsil etmektedir (Karabulut, 2015: 190). İnşacı perspektifin değişen tehditlere ilişkin analiz düzeyi de bu yöndedir. Devletlerin küresel aktör olarak

uluslararası örgütlenmelerin de merkezinde yer aldığı uluslararası sistem birçok farklı unsurdan etkilenebilmektedir.

Stratejik olarak değişimden anlaşılması gereken tercihlerin farklılaşması ve bu alanda uzmanlaşılmasına yönelik adımlar atılmasıdır. Sadece teorik bir zeminin ortaya çıkması yetmemektedir. Stratejik olarak atılacak adımın bir sonucunun oluşması, özellikle değişim algısının doğru yönlendirilmesi açısından bir zorunluluktur.

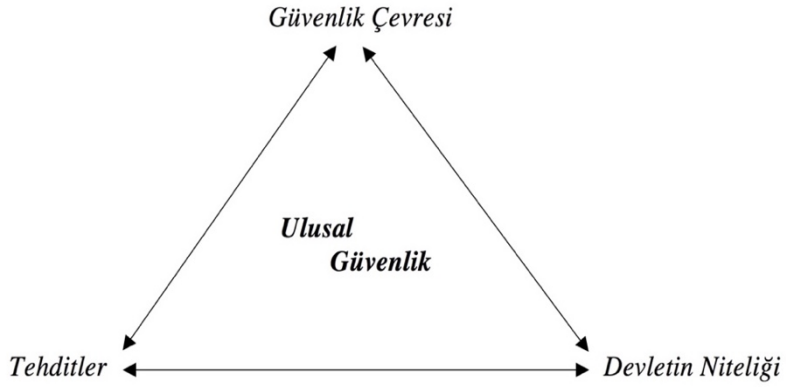
Siber saldırılar içindeki teorik yaklaşım, pratikteki boyutuyla kendi içerisinde zorlaşmaktadır. Siber alana ilişkin, stratejik değişim algısına yönelik olarak, ülkelerin siber savaş stratejilerinin etkileyeceği hususlar Çifçi'ye (2012: 66) göre şu şekildedir:

- *"Siber alana doğrudan veya dolaylı olarak uygulanabilecek olan ulusal, uluslararası yasal düzenlemeler ve ülkeler arası sözleşmeler,*
- *Ülkenin rejimi, insan hakları ve demokrasiye olan yaklaşımı,*
- *Ülkenin uluslararası camiada kendini konumlandırmak istediği yer ve bu kapsamda mücadelesini hangi alanlara taşıyacağı,*
- *Ülkenin siber alanı kullanma yaygınlığı ve siber alana olan bağımlılığı,*
- *Ülkenin siber savunma ve saldırı kabiliyetleri."*

Siber alana ilişkin değişimde güvenlik stratejilerinin küreselleşmesi ile ters orantılı olarak savaş stratejileri de şekillenmiştir. Tehdit olarak algılanan olgu ve aktörlerin artışı, güvenlik halkaları arasındaki ayrımın giderek azalması, diğer bir ifadeyle uluslararası çevrede tehdit olan her unsurun doğrudan bireyi etkiler hale gelmesi, güvenlik stratejilerinin içten çok dışa göre düzenlenmesine yol açmaktadır (Dedeoğlu, 2003: 111).

Siber güvenlikle ilgili dışa göre düzenlenecek stratejik değişim döngüsünde rakibin yok edilmesi gibi bir husus söz konusu olmadığı için tercih edilecek unsur olarak saldırının dönüştürülmesi ya da düşmanın durdurulması amaçlanmaktadır. Bu durum uzun vadede çatışmaların boyutunu siber alanda güçlendirecek ve genişletecektir. Stratejideki değişim algısındaki bu süreç özellikle ulusal güvenlik açısından ciddi bir tehdit oluşturmaktadır. Ulusal güvenlik açısından önemli bileşenler haline gelen güvenlik çevresi siber saldırılar ile ciddi bir travmayı yaşarken, siber tehditler bu alanda değişimle birlikte daha çok çeşitlenecektir.

Şekil 31: Ulusal Güvenlik Problematiğinin Bileşenleri



Kaynak: Dreyfus, 2002

Güçlenen ve genişleyen siber alandaki tehditlere karşın stratejilerin *"ulusal"* olması devletlerin elini güçlendirecektir. Ulusal stratejiler, stratejik değişim algısıyla siber şoklara karşı direnç de gösterebilmektedir. Çok yönlü ve çok üyeli uluslararası yapılanmalar ve örgütlenmeler siber güvenlik anlayışında ulusal stratejilerin gelişimini zorlaştırmaktadır (Bejtlich, 2015: 164). Özellikle siber stratejinin devletleri ilgilendiren uluslararası yönünde devletlerin sahip olduğu güç, benzer kapasiteli güçlerle kıyaslanabilir. Stratejik değişim algısıyla birlikte *"ulusal siber stratejiler"* geliştirilirken izlenecek yolu Ian Wallace[120] (2014) şu şekilde tarif etmektedir:

> - *"Strateji yalnızca nasıl davranılması gerektiğini değil, aynı zamanda nasıl bir politika izleneceğini de ortaya koymalıdır.*
> - *Değişimin yanında devamlılığa da odaklanılmalıdır. Yeni ulusal koordinasyon yapılanmaları siber zorluklara cevap verebilecek nitelikte olmalıdır.*
> - *Stratejiler özü itibariyle "ulusal" olmalıdır. Ulusal stratejiler genel olarak, hükümetlerin siber güvenlikteki rolüne işaret etmektedir.*
> - *Stratejilerin güvenilir olması sağlanmalıdır. Strateji oluştururken kullanılan kaynakların belirtilmemesi hatasına düşülmemelidir.*
> - *Siber güvenlik gerçeğiyle birlikte planlar yapılmalı ve sürdürülebilir amaçlar gözetilmelidir. Siber stratejiler, gelecekte yaşanması kaçınılmaz saldırılara ve bu saldırılardan doğabilecek olası sonuçlara göre tasarlanmalıdır."*

[120] *Ian Wallace*, Brookings Institute'de, 21. Yüzyıl Güvenlik ve İstihbarat Merkezi uzmanıdır. İngiltere Savunma Bakanlığı'nda ulusal siber stratejilerinin geliştirilmesinde görev almıştır.

3.2.2.1. Geleneksel Tehditlerin Dönüşümü

Uluslararası sistemin anarşik yapısı çerçevesinde kavramsallaştırılan devlet merkezli ve askeri odaklı güvenlik anlayışı, Soğuk Savaş'ın sona ermesi ve küreselleşme sürecinin etkisiyle birlikte yeniden ele alınmaya başlamıştır. Bu çerçevede, yeni/eleştirel güvenlik yaklaşımları, güvenliğin nesnesi olarak devletin yerine ya toplumsal grupları ya da bireyi koyarak güvenliği daha geniş sosyal, ekonomik, çevresel ve politik amaçlarla birleştirmektedir (Ağır, 2011: 99).

Daha geniş amaçlarla birleşen güvenlik konuları özellikle küreselleşme ile birlikte hiçbir dönemde olmadığı kadar çeşitlenmiş ve yoğunlaşmıştır. Geleneksel tehditler açısından başta terörizm olmak üzere birçok farklı başlık kendi içerisinde dönüşmeye başlamıştır. Özellikle *terörizm, yoksulluk, çevre kirliliği, etnik sorunlar, nükleer, kimyasal* ve *biyolojik silahların varlığı* ve de *siber terörizmin* şekil değiştirmesi 21. yüzyılda uluslararası güvenlik açısından tehdit boyutunu farklılaştırmıştır.[121]

Savaş teknolojilerinde meydana gelen gelişmeler, bu teknolojilerin insan kayıplarını artıracak kapasiteye erişmesi ve yıkıcı etkiler, devletlerin doğrudan doğruya savaşa girmelerinin risklerini daha da fazlalaştırmıştır. Savaş teknolojilerindeki gelişmeler her iki dünya savaşından beri bu yönde bir endişeye neden olmuştur ancak özellikle kimyasal silahların yaygınlaşması ve nükleer silahlara sahip olan ülkelerin sayılarının artmasıyla savaşın yol açabileceği tehlikeler farklı boyutlara taşınmıştır (Karabulut, 2015: 193). Silah ve teknolojinin birbiri ile ilişkili olduğu düzlem artınca terörist grupların hem konvansiyonel silahlara ulaşmadaki teknoloji kabiliyetleri hem de siber alandaki faaliyetleri etkinlik kazanmıştır (Lutz ve Lutz, 2008: 28).

Geleneksel tehditler arasından günümüze boyut değiştirerek gelen askeri tehditler yanında ekonomik, çevresel, toplumsal konuların da güvenlik alanı içine dahil edilmesi süreci başlamıştır. Özellikle geleneksel olarak tehdit algısının yoğunlaştığı birey kavramı

[121] *Küreselleşme,* Soğuk Savaş dönemi sonrasında oldukça tartışılan kavramlardan birisidir. Akademik anlamda kavramı ilk kullanan Thedore Levit'tir. Bu bağlamda küreselleşmenin ilk halkasının coğrafi keşiflerle, ikinci halkasının 1870-1914 yılları arasında, son halkasının ise iki kutuplu düzenin yıkılmasıyla oluştuğu kabul edilmektedir.

daha makro bir hal alarak büyümüş ve tehdit boyutunda daha karmaşıklaşarak siber uzaya yayılmıştır. Küreselleşme sürecinde yaşanan tehdit çeşitlenmesi geleneksel tehditleri daha karmaşık hale getirmiştir.

Güvenlik algılamalarında özellikle geleneksel tehditlerin dönüşümündeki en önemli sebeplerden birisi tehdidin tek boyutlu, devletten devlete olma boyutundaki klasik halinden çıkarak, asimetrik ve çok boyutlu bir konuma ulaşmasıdır. Bu durum, günümüz tehditleri ile mücadelede klasik yapılanma ve anlayışların geçerliliğini tamamen yitirdiğini göstermektedir.

Küreselleşme ile ortaya çıkan asimetrik tehdit ile birlikte saldırganın muhatabından göreceli olarak daha zayıf olmasına karşın, değişen tehdit unsurlarıyla birlikte, ani ve hazırlıksız saldırılarla dengeleri değiştirebildiği gözlenmiştir. Bu sebepten dolayı birçok uzman, devletlerden öte sivillere yönelik olan ve askeri olmayan güvenlik anlayışı içinde mücadele edilmesi gereken hususları ön plana çıkarmaya başlamıştır. Küreselleşme süreci ve etkileriyle beraber geleneksel tehdit algısındaki değişimin etkilendiği durumları Önen (2015) şu şekilde gruplandırmıştır:

> - *"Güvenlik alanında yeni tehditlerin ortaya çıkmasının yanında siber terör, bilimsel çalışmaların siber uzaydaki saldırganlığı ve uyumu da bozacak şekilde hızla ilerlemesi, ekolojik dengeyi genetik bilimiyle bozma girişimleri ve yeni tür hastalıklar.*
> - *Geçmişte var olan fakat güvenlik alanı içinde düşünülmeyen konuların güvenlik alanına eklemlenmesi; birey güvenliği ve çevre güvenliği gibi.*
> - *Geleneksel güvenlik tehditlerinde terör, savaş, organize suçlar gibi hususların kabuk değiştirmesi."*

11 Eylül 2001 terör olayları güvenlik kavramının kapsamının küresel terör, örgütlü suç şebekeleri, uyuşturucu, silah ve insan ticareti, yasadışı göç, etnik ve dinsel nitelikli çatışmalar ve kitle imha silahlarındaki artış gibi tehditlerle daha da genişlediğini göstermiştir. Geleneksel tehdidin dönüşümünde Soğuk Savaş dönemi sonrasında ABD'nin hegemon güç olması uluslararası ortamı yumuşatmamış; küreselleşmenin ekonomik ve sosyal bakımdan getirmiş olduğu olumsuz sonuçlar, ABD ve Batı karşıtı terörü körükleyen farklı etkenler olmuştur. Devletler ve bireyler adına tehdidin her an ve her yerde faaliyette olabileceği düşüncesi korkutucu boyutlarla dönüşüme uğramıştır (Yorulmaz, 2014: 121).

3.2.2.2. Siber Tehdidin Dönüşümü

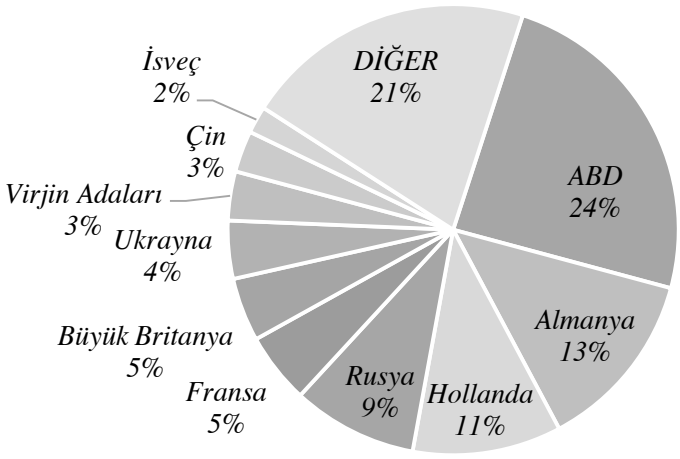
Siber alanda gerçekleştirilen saldırıların geleneksel saldırılardan önemli farklılıkları bulunmaktadır. Her şeyden önce siber saldırılar ışık hızında gerçekleştirilebilme olanağına sahiptir. Bununla birlikte modern toplumlardaki altyapının yüksek teknolojiye ihtiyaç duyması nedeniyle, sanal dünya üzerinden gerçekleştirilen saldırıların etkileri konvansiyonel silahlar kadar büyük olabilmektedir. Ayrıca siber saldırıların maliyeti geleneksel saldırılarla mukayese edilemeyecek kadar düşüktür ve siber saldırının hedefinde yer alan objenin kasten mi yoksa kazayla mı saldırıya maruz kaldığının anlaşılması kolay değildir (Gürkaynak ve İren, 2011: 265).

Siber tehdidin fiziksel etkisinin olması cazip olan farklı bir yönü ortaya çıkararak küresel bir değişim algısını da bizlere sunmaktadır. Bilginin küresel düzeyde birbirine bağlı olduğu teknolojik alt yapı kendi içerisinde ayrı bir karmaşıklığı meydana getirmektedir (Eriksson ve Giacomello, 2007: 174).

Siber saldırıların hedeflerindeki anlaşılması zor olan durum özellikle, birçok olayın miladı olan 11 Eylül 2001 sonrasında ivme kazanarak daha da farklı bir hal almıştır. Bunun en önemli sebebi İkiz Kuleler ile birlikte tehdit konusundaki geleneksel anlayışın da değişmesidir. Devletlerin toprak sınırlarının yanı sıra askeri mekan ve zaman kurallarının da anlamsız hale gelmesi siber uzaydaki faaliyetlerin yönünü değiştirmiştir.

Siber tehditlerin dönüşümü farklı verilerle de tartışılmaktadır. Özellikle zararlı yazılımların, faaliyet alanlarının bağımlı olunan siber ortamda evrim geçirmesi son yıllarda dikkat çekici bir durumdur ve devletlerin tehdit algısında da hissedilmiştir. Grafik 19'da görüldüğü üzere çevrimiçi kaynakların zararlı yazılımlar üzerinden dağılımı, ülkelerin siber ortamda faaliyetlerinin artışıyla doğru orantılı bir yön bulmuştur. Başta ABD olmak üzere Almanya, Hollanda, Fransa, İngiltere gibi ülkeler bu konuda en çok etkilenen ülkelerin başında gelmektedir. Siber alana artan bağımlılık bu noktada riski daha da artırmaktadır. Siber alanda gelişmekte olan ülkelerin, bu alanda gelişmiş ülkeleri takibi ve siber saldırılarda savunmaya ilişkin kapasitelerini artırmaya çalışması kısmi olarak avantaj sağlayabilecektir. Önemli olan husus kısa ve uzun vadeli politikaların belirlenmesidir.

Grafik 19: Çevrimiçi Kaynakların Zararlı Yazılımlar Üzerinden Dağılımı



Kaynak: Kaspersky Security Bulletin, 2015: 62

Siber saldırıların uzunca bir süre risk olduğu farkında olunan bir hususta fakat zarar kapsamı önemsenmemiş ve sınırlı olduğu düşünülmüştür. Bu algı 11 Eylül ile birlikte hem siber istihbaratın önemini artırmış, hem de 2007 yılında Estonya'da yaşanan olaylardan sonra siyasi çevrelerin de dikkatini çekmiştir. NATO'nun elektronik iletişime bağımlı toplumlarının aynı zamanda siber cephede son derece zayıf olmalarının ortaya çıkması ciddi bir tehdit dönüşümünü siber alanda ortaya çıkarmıştır.[122]

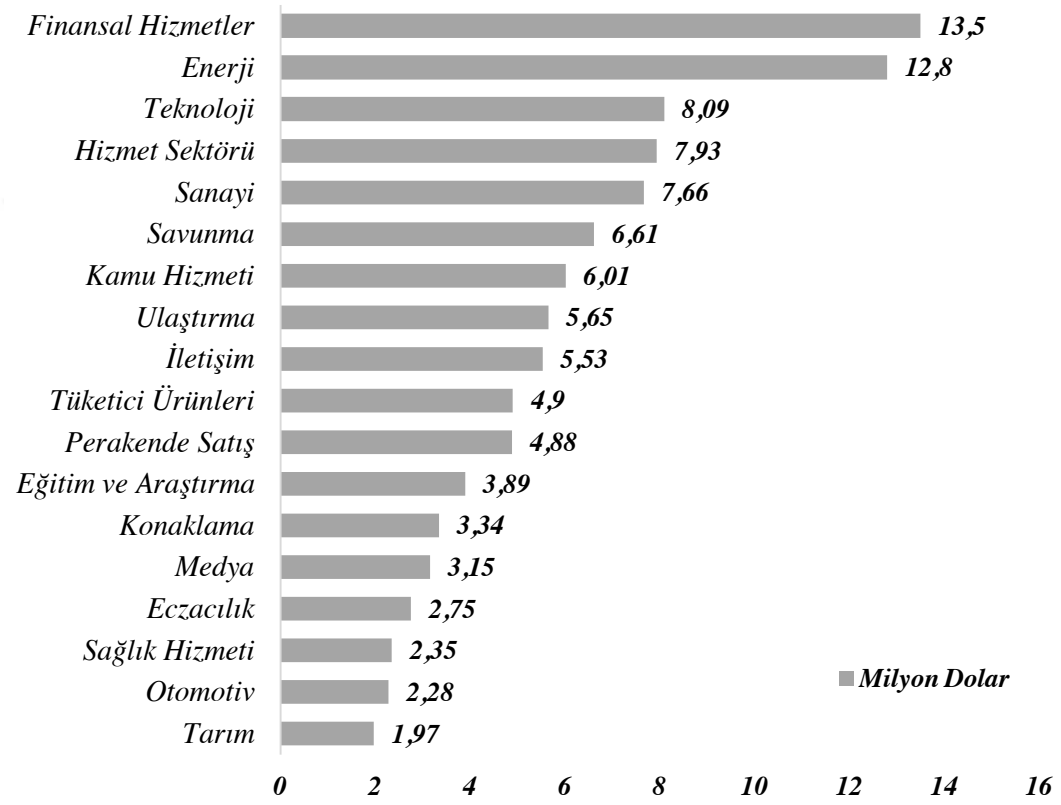
2008 yılında, ABD askeri bilgisayar sistemlerine yapılan kapsamlı saldırılarla birlikte siber casusluk daimi tehdit haline gelmiştir. Buna benzer olayların tekrarlanması ve artması ile birlikte dünyada ciddi bir farkındalık oluşmuştur. Ortaya çıkan çok sayıdaki siber olaylarla birlikte sıkı korunan devlet verilerinin kötü niyetli kişilerin eline geçmesi, tehdit algısının boyutunu uluslararası aktörlere taşımıştır.

Siber tehdidin dönüşümü sadece casusluk ve devletlerin verilerine ilişkin bir problemi devletlerin gündemine sokmamıştır. Aynı zamanda siber tehdidin mali olarak,

[122] NATO'da, ciddi boyutlu bir olay olarak ilk defa Kosova Krizi'nde karşılaşılan siber saldırı dalgası ile birlikte ittifakın e-posta hesabı günlerce ziyaretçilere kapatılmış ve NATO web sitesi kullanılamaz hale gelmiştir. Çatışmanın siber boyutu sadece NATO'nun istihbarat kampanyasını engellemek için girişilmiş bir çaba olarak algılanmıştır.

küresel anlamda devletlere ve kurumlara verdiği zarar çok ciddi boyutlara ulaşmıştır. Başta finansal hizmetler olmak üzere, kritik altyapıların da bağlı olduğu enerji, teknoloji, sanayi ve savunma birimlerine verilen zarar, tehdidin dönüşümü açısından ve oluşturulacak politikaların yetkinliği merkezinde önemli bir yere sahiptir.

Grafik 20: 2015 Yılı Siber Saldırıların Küresel Düzeyde Sektörlere Verdiği Zarar



Kaynak: Ponemon Institute, 2015a: 10

Yakın coğrafyalardaki ülkelerin kritik altyapılarının, özellikle kimi enerji nakil hatlarında birbirlerine olan bağlılığı ve rakip ülkelerle olan ilişkilerde önemli bir kart oluşu siber tehdidin dönüşümünde dış politika yaklaşımı oluşturmayı da gerekli kılmaktadır. Gelişmekte olan ülkeler açısından bu hatların korunmasına ilişkin oluşturulacak ittifaklarda tehdidin dönüşümü bulunulan coğrafyaya göre avantaj dahi sağlayabilecektir. Enerji diplomasisi ve bağlı olduğu kritik altyapıların korunması siber ittifaklarda caydırıcılık oluşturacaktır.

3.2.3. Güvenlik Stratejilerini Siber Savaşa Uygulayabilme

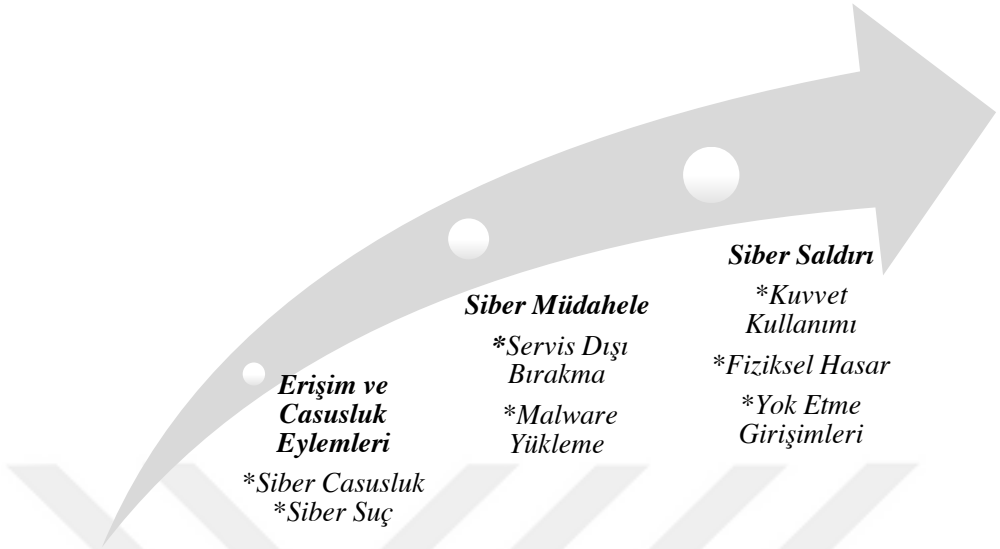
Kimi zaman otoriteleri kimi zaman da fiziksel anlamda bireyleri etkileyen olaylar karşısında, güvenlik stratejilerinin siber saldırılarla birlikte nasıl uygulanacağı konusunda çeşitli tartışmalar vardır. Siber saldırılar ve siber savaş anına ilişkin güvenlik stratejilerinde, uluslararası güvenliğe ilişkin çatışmacı stratejileri uygulayabilmenin hangi durumlarda hayata geçirileceği hususu hem uluslararası hukuk alanında, hem de devletlerin birbiriyle olan ilişkilerinin politik teori zemininde oturmamıştır.

Güvenlik stratejileri açısından, çatışmacı bir boyutta ekonomik yaptırımların siber saldırılara ilişkin, hangi zamanlarda ve nasıl uygulanacağına dair bir düzenleme yapılmamıştır. Bu noktada örneklendirilebilecek olay da yok denecek kadar azdır. Ekonomik anlamda sarmalın daha da yoğunlaştığı uluslararası sistemde ekonomik yaptırımlar yönünde karar almak zaten zorken siber olaylara ilişkin adımlar gelecek açısından oldukça düşündürücüdür. Bu durumun en önemli sebebi siber saldırılara ilişkin verilerin artık tüm uluslararası aktörleri etkilediği yönündedir ve ekonomik olarak zorlamaların bu tür saldırılardan sonra ciddi paradoksları doğuracağıdır.

Siber saldırıların fiziki olarak bir sonuç doğurması akıllara daha çok askeri yöntemleri getirmektedir. Askeri yöntemler, aşamalı şiddet uygulamasına dayanmaktadır. Farklı yöntemler sonrasında sonuç alınmadığı zaman ortaya çıkan uygulamalarda siber saldırıların boyutu ve verdiği zarar sonrası karşı tarafın kullanacağı askeri bir unsurun da olabileceği kesinlikle düşünülmesi gereken bir husustur. Bu konudaki en önemli sorun saldırıların siber uzayda manipüle edilip, bilinmeyen aktörler tarafından savaşı diğer aktörler ya da unsurlar adına körüklemesidir. Siber orduların da askeri birimler olarak yerini aldığı günümüzde, askeri bir karşılık olarak yine siber bir müdahele mi olacağı ya da konvansiyonel unsurlara mı başvurulacağı devletlerin kararlarına ve etkilemek istediği alana bağlıdır. Siber harekatlarda siber saldırıların da fiziksel bir hasar oluşturucağı unutulmamalıdır.[123] Bu durumu Şekil 32, gelişim itibariyle ortaya koymaktadır.

[123] Özellikle Gürcistan-Rusya çatışması sırasında Gürcistan hükümetinin servis sunucularına karşı yapılan saldırılar, siber savaş terimine daha da somut bir nitelik kazandırarak çatışmacı güvenlik stratejilerine yerleşecek bir müdaheleyi gözler önüne sermiştir. Yapılan müdaheleler fiziksel bir zararı gözle görülecek şekilde ortaya koymamıştır fakat çatışmanın önemli bir bölümünde Gürcistan hükümetini zayıf düşürmüştür.

Şekil 32: Siber Harekat Spektrumu



Kaynak: Doğru (t.y.), "Siber Harekatın Uluslararası Hukuk Çerçevesinde Analizi"

Siber saldırıların öngörülemez oluşu ve gerçekleşme hızının saniyelerden daha az zaman dilimleriyle ölçülmesi özellikle tarafların konuyu müzakere etmesi açısından olanaksız görünmektedir. Bunun en önemli sebebi siber savaşa karşı etkili bir caydırıcı niteliğin olmaması ve uluslararası hukuka bağlı kalmanın olanaksızlığıdır. Bu şartlar altında askeri bir missileme, hem yasal hem de siyasi açıdan zorunlu gözükmektedir.[124]

2010 yılında Stuxnet'in yıkıcı siber savaş yeteneklerindeki öz, güvenlik stratejilerinin siber saldırılarla buluştuğu noktada, önemli bir atılım yaşandığına dikkat çekmiştir. 45000 Siemens kontrol sisteminin etkilendiği saldırılar İran'daki nükleer enerji santralleri açısından, çok önemli olan teknik süreçlerin manipüle edilebileceğini göstermiştir (Denning, 2012: 675). Yapılan saldırı, enerji arzını ve trafik ağlarını yöneten kritik bilgisayar sistemlerini etkileme riskini açığa çıkarmıştır. Siber saldırıların ciddi felaketlere yol açabileceği yönündeki algı, güvenlik stratejileri açısından siber müdahele yöntemlerini askeri unsurlar içerisine oturtmuştur.

[124] Devletlerin askeri amaçla kullanılabilecek siber yeteneklere büyük yatırım yaptığından ve siber ordulardan daha önceki başlıklarda bahsedilmişti. İlk bakışta dijital silah yarışı açık ve kaçınılmaz bir mantığa dayanıyor gibi gözükse de siber savaşların çeşitli avantajları mevcuttur. Bu savaş asimetrik, oldukça maliyetsiz ve sadıranın avantajlı olduğu bir durumu ortaya çıkarmaktadır.

Siber müdahele yöntemlerinin etkinliğinin artışıyla savunma boyutu yanında devletler saldırı ve çıkar arzusuyla ittifaklar da kurabilecektir. Özellikle tarihsel boyutta güven ilişkilerinin geliştirilebildiği yakın coğrafyadaki devletler bu konuda çıkarsal olarak geçici ittfaklar oluşturabilir ve amaçlar masaya konulabilir.

3.2.4. Siber Uzayda Ortak Güvenlik ve İttifak Oluşturma

Devletlerin dış politika stratejileri açısından en çok sözü edilen konulardan birisi de ittifaklardır. Günümüz dünyasında ise izolasyon türünden bir dış politika stratejisi izleyen ülke sayısı oldukça azdır. Daimi tarafsızlık gibi istisnai nitelikteki durumları da hariç tutarsak, uluslararası sistemde yer alan devletlerin çok büyük bir bölümü dış politikalarını sürdürmekte ittifak oluşturma stratejisinden geniş bir şekilde yararlanmaktadır (Sönmezoğlu, 2014: 425).

Çalışma kapsamında tercih edilen ve uygulamaya çalışılan ittifak oluşturma ve özelde, siber uzayda ortak hareket edebilme uygulanabilirlik açısından olumlu ve olumsuz yönleriyle, siber politikaların uluslararası düzeyinde irdelenmesi gereken bir hususdur. Özellikle iki kutuplu sistemin çöküşü ile birlikte, siber uzaydaki çatışma alanı ittifak oluşturma adına, kimi gelişmekte olan ülkeler açısından daha da önemli bir yere sahiptir ve pratikte veriler mevcuttur.

Zaten çatışmalı olan bir sistemde siber saldırılar gibi bilinmez bir boyutta, siber alanda gelişme zemini arayan devletler niçin ve nasıl ittifak kurmalıdır? Oluşturulabilecek ittifakların devamlılığı ya da süresine ilişkin ne tür kararlar alınacaktır? Bu ve benzeri soruların altında yatan temel neden, siber saldırılar sonrasında rakip tarafın vereceği tepkinin ölçülemeyecek oluşudur.

Temelde benzer birçok sorunun cevabında devletlerin belirli bir amaca ulaşmak açısından yeterli imkanlara sahip olmakla beraber, bu amaca meşru yollardan ulaşmak veya bu nedenle girişeceği dış politika eylemlerinin sorumluluğunu başka ülkelerle paylaşmak istediğinden diğer ülkelerle ittifaklar yapabilir (Sönmezoğlu, 2014: 428). Bu noktada siber ittifaklara yönelik olarak değinilmesi gereken husus tepkinin öngörülemezliği neticesinde

sorumluluğun paylaşılması ve hafifletilmesi olabilir.[125] Gücün ittifaklar içinde dengelenmesi veya zayıf toplumların güçlendirilirek, ittifak adına uzun dönemli amaçlar güdülmesi dış politika çıktısı olarak geliştirilebilir (Morgenthau, 2004: 126).

İttifak örnekleri bazında, özellikle siber savaş açısından bazı devletlerin NATO bayrağı altında ortak hareket etmesinde, temel olarak farklı nitelikler göze çarpmaktadır. NATO ittifakı altındaki siber müdahelelerde temel olarak sorun, gündemin belirlenmesinde belli devletlerin baskınlığıdır. Bunun farkında olan ABD, denetim imkanlarını arttırmak adına NATO bünyesinde siber güvenliğe ilişkin farklı projelere imza atmakta ve askeri boyutla ilgili baskın bir şekilde olaylara müdahil olmaktadır.

NATO zaten var olan bir örgütlenme olarak siber güvenliğe ilişkin düzenlemeler yaparken, oluşturulacak farklı siber ittifakların işlerliği açısından *casus foederisin,* yani ittifaka ilişkin antlaşmada yer alan taraflara ilgili hak ve yükümlülüklerin hangi koşullar altında geçerli olacağının belirlenmesi de önemli hususlardan birisidir. Uluslararası aktörler açısından, özellikle devletler adına siber saldırıların tespiti ve atılacak ortak adımlar üzerinde anlaşılması zor hususların varlığı sorunsalın başında gelmektedir. Siber güvenliğin gelişimine ilişkin ivmeyi de düşünecek olursak sadece çıkarların gözetilmesi, ittifak bünyesindeki her birimin temel önceliği olacaktır.

NATO gibi bölgesel yapılanmalarda, askeri harekat alanlarına siber savaşın dahil edilmesi, olaylara müdahil olmada manevra yeteneği de sağlamaktadır. Bu noktada özellikle savunma konseptinde oluşturulan birliklerde seviye eğer bölgeselse bu niteğini korumakta ve kapsam güvenlik boyutuyla beraber çıkar elde etme güdüsüne dönüşmektedir. Özellikle NATO gibi örgütlenmelerin, siber güvenliğe ilişkin attığı adımlarda etkinlik kurma arzusu buna iyi bir örnektir. Tablo 12'de görüleceği üzere NATO gibi bölgesel seviyede faaliyet gösteren ve aynı şekilde güvenlik kapsamında oluşturulmuş birliktelikler azımsanmayacak kadar çoktur. Fakat başarı konusunda NATO, siber güvenlik alanında ciddi bir yol katetmiştir.

[125] 1950 yılında, ABD'nin Kuzey Kore'ye müdahelesinde Birleşmiş Milletler bayrağı altında hareket etmek, eyleme meşruiyet kazandırılması açısından önemli bir düşünceydi. ABD'nin bu konudaki sorumluluğunun diğer ülkelerle paylaşılması sağlanmıştır. Türkiye'nin 1974 Kıbrıs Harekatı öncesinde İngiltere'ye başvurarak duruma beraberce müdahele edilmesini istemesi de esas olarak bu türden bir girişimdir (Sönmezoğlu, 2014: 429).

Tablo 12: Uluslararası Güvenlik/Savunma Örgütleri ve Kapsam

Birlik/Örgüt	***Seviye***	***Kapsam***
BM	*Evrensel*	*Genel Güvenlik*
NATO	*Bölgesel*	*Güvenlik ve Savunma*
AB (AGSP)	*Bölgesel*	*Güvenlik ve Savunma vd.*
OSCE	*Bölgesel*	*Güvenlik*
Şangay İşbirliği Örgütü	*Bölgesel*	*Güvenlik ve Savunma vd.*
Amerika Devletleri Teşkilatı (OAS)	*Bölgesel*	*Güvenlik ve Savunma*
Afrika Birlikği Örgütü (OAU)	*Bölgesel*	*Güvenlik ve Savunma vd.*
Arap Birliği	*Bölgesel*	*Güvenlik vd.*
İslam Konferansı Örgütü	*Bölgesel*	*Güvenlik vd.*
Avrupa Polis Bürosu (EUROPOL)	*Bölgesel*	*Güvenlik ve İstihbarat*
INTERPOL	*Evrensel*	*Suçla Mücadele*
OPANAL	*Bölgesel*	*Nükleer Güvenlik*
SAARC	*Bölgesel*	*Ekonomi ve Güvenlik*
GCC	*Bölgesel*	*Güvenlik ve Savunma vd.*

Kaynak: Yılmaz, 2015

3.3. Mikro Siber İttifak Teorisi (Micro Cyber Alliance Theory: Micro-CAT)

İttifak aslında ortak çıkarları birleştirmek, olası anlaşmazlıklarda ortak çıkar geliştirebilmek ve bu ortak çıkarda yetenekleri dengeleyebilmektir. Bu çalışma kapsamında ortaya atılan fikirsel bütünlük siber güvenlik bağlamında, ortak çıkar geliştirebilme adına devletler temelinde bir yaklaşım sergilemeyi amaçlamıştır.

Özellikle siber güvenik alanında gelişmekte ya da gelişme arzusu içinde olan devletlerin siber politikalara ilişkin adım atmalarında, çalışmanın da konseptini oluşturan siber ittifak oluşturulmasıyla ilgili veriler, geçici türde bir ittfak oluşturulması yönünde belirlenmiştir. Bunun açıklığa kavuşturulmasında siber güç kapasitesi ve güç dengesine ilişkin tanımlamalar ele alınmış, siber güvenlikte savunma disiplini kavramı tartışılmış ve bir yol haritası çizilmiştir.

Mikro Siber İttifak Teorisi (Micro-CAT) olarak tanımlanan bu yaklaşımın teori olarak nitelendirilmesinin sebebi, oluşturabilecek siber diplomasi kanatlarının ve ittifakın aynı zamanda bir gelecek vizyonu sunmasıdır. Özellikle ele alınan çalışmalarda devletlerin siber güç kapasitelerinin kıyaslanması ile ilgili olarak, gelişmekte olan devletlerin çıkar elde etmesinde atılacak adımlarda uygulunabilirlik, teorik olarak farklı gelişmelerle desteklenerek sunulmaya çalışılmıştır.

3.3.1. Siber Güç Kapasitesi

Güç olgusu, genellikle ilişkisel bir durumun çıktısı olarak anlaşılmaktadır. Robert Keohane ve Joseph Nye; *"Güç, bir aktörün diğerlerine, normal olarak yapmayacakları bir şeyi yaptırabilme yeteneğidir."* derken bu eğilimi göstermektedirler. Yazarlar bu kategorinin de kendi içerisinde (askeri imkanlar, ekonomik kapasite gibi) *sert güç (hard power)* ve (kültürel zenginlik, özgürlükçü siyasal rejim, refaha dayalı ekonomik bir sistem gibi) *yumuşak güç (soft power)* olarak ikiye ayrıldığına işaret etmekte, işin bu yönü açısından da yumuşak güç kategorilerinin bilgi-iletişim alanındaki gelişmelerle büyük önem kazandığına dikkat çekmektedirler (Sönmezoğlu, 2014: 264).

Özdemir (2008: 125), güce ilişkin çalışmaların ortak yönünün, gücü doğrudan veya dolaylı, gözlemlenebilir veya gözlemlenemeyen mekanizmalar yoluyla mutlaka birileri üzerinde kullanılan bir araç olarak ele almaları olduğunu belirtmektedir. Aktörler açısından ele alındığında güç kavramından iki farklı şekilde söz edilebilir. Birincisi, bir şeyi yapabilme kapasitesi veya yetenek olarak güç (*power to*) ve ikincisi, birisi üzerinde kontrol sağlanması olarak güçtür *(power over)*. Bu tartışmalar her iki anlamı da iç içe geçmiş bir şekilde kullanırken aslında gücü, başkaları ve onların davranışları üzerinde bir kontrol mekanizması olarak değerlendirmektedir.

Joseph S. Nye (2010: 5), *"Cyber Power"* adlı çalışmasında siber alan içinde sert ve yumuşak gücün, kaynakların kullanımına göre siber uzayda etkisinin farklı boyutlarda olduğunu tartışmaktadır. Siber kaynakların da siber uzay içerisinde sert güç olabileceğini vurgulayan Nye, geçmiş dönemde görülen örneklerde devletlerin fiziksel aktivitesinin bu güç vasıtasıyla durdurulma noktasına gelebileceğini yaptığı gruplandırmayla ortaya koymaya çalışmıştır. Bilgi araçları ve fiziksel araçları, siber uzayın içinde ve dışında farklı

şekillerde ayırarak sert ve yumuşak güç şeklinde örneklendirdiği gruplandırmada dikkat edilmesi gereken husus hedeflenilen unsurlardır.

Tablo 13: Siber Gücün Fiziksel ve Sanal Boyutu

	Siber Uzay İçinde	***Siber Uzay Dışında***
Bilgi Araçları	***Sert:*** *Servis Dışı Bırakma* ***Yumuşak:*** *Normların ve Standartların Ouşturulması*	***Sert:*** *SCADA Sistemlerine Saldırı* ***Yumuşak:*** *Kamu Diplomasisiyle Mücadele Fikirlere Hükmetme*
Fiziksel Araçlar	***Sert:*** *Şirketler üzerinden Devleti Kontrol etme* ***Yumuşak:*** *İnsan Hakları Aktivistlerine Yardım için Kritik Altyapı Oluşturma*	***Sert:*** *Yönlendiricileri (Routers) Bombalama veya Kabloları Kesme* ***Yumuşak:*** *Siber Tedarikçileri Protesto Etmek*

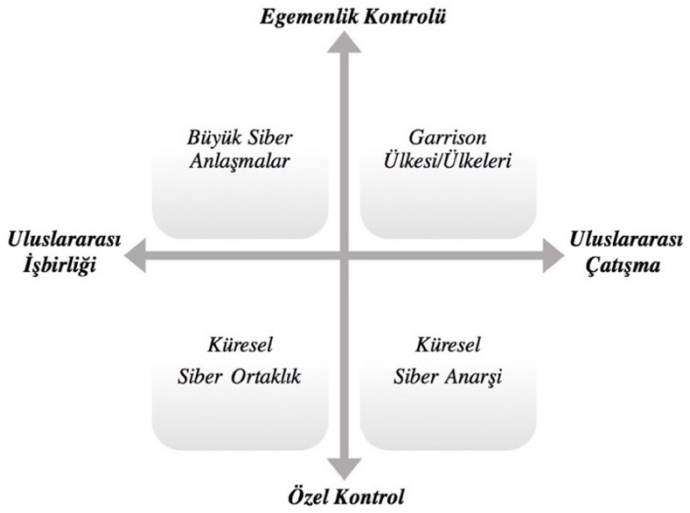
Kaynak: Nye, 2010: 5

Joseph S. Nye'ın yapmış olduğu gruplandırmaya paralel olarak, bilgi-iletişim alanındaki gelişmelerle birlikte, gücün ilişkisel yönü açısından iki kavram önem kazanmıştır ve siber güç kapasitesi ile birlikte tartışılması gereken hususlardır. Bunlar *kontrol* ve *etkidir*. Bu noktada siber güç kapasitesi itibariyle *kontrol* kavramından ne anlaşılması gerektiği ve bunun yorumu önemlidir. Siber güç kapasitesi açısından tartışılabilir bir nokta olan *etki* ise pratikteki sonuçlarıyla bizlere birtakım veriler sunmaktadır.

Siber güç kapasitesi açısından kontrol, klasik olarak güç yaklaşımına benzer şekilde kontrol edilecek unsurların farklılaşmasıyla ele alınabilir. Siber güç açısından eldeki altyapının ve vizyonun kontrolü, siber gücün uygulanması ile ortaya çıkacak kaynaklar ve sonuçlar, tartışılması gereken boyutlardan birisidir. Siber gücün kanalize edildiği alan, siber politikaların uluslararası ilişkiler açısından tartışıldığı boyutu da belirleyecektir. Uluslararası ilişkilerdeki potansiyel gelecek, Şekil 33'te görüldüğü üzere ya aşırılık ve kaos, ya da uyum yönünde seyir izleyecektir. Özellikle egemenlik ve çatışma alanlarının kesiştiği noktalarda

askeri planlar ve anarşik yapı kendini gösterirken, iş birliği ve kontrol noktasındaki ortaklıklar daha uyumlu bir yapıyı beraberinde getirebilir.

Şekil 33: Siber Politikaların Uluslararası İlişkilerde Potansiyel Geleceği[126]



Kaynak: Choucri, 2012: 235

Çalışma kapsamında ele alınan ittifak mantığında devletler arasındaki güç ilişkisi siber güç kapasitesi açısından ele alınacak, değerlendirilecek ve devletler arasında bir baskınlık oluşturacaktır. Günümüz ittifaklarında, gücün baskınlığıyla ittifak içinde lider devletler ortaya çıkabilmekte, kararlarda etkili olabilmekte ve ittifakın geleceğini belirleyebilmektedir. Siber güç kapasitesi açısından devletlerin oluşturacağı birlikteliklerde bu gücün ölçülmesinde verisel olarak hareketlilik ve devletin daha önceki siber saldırılarda hedefsel niteliği belirleyici olacaktır.

Siber güç; güç kavramının esasen yapılandığı kültürel ve politik noktalarda, siber alanın internet üzerindeki veri trafiğiyle form bulmaktadır (Jordan, 1999: 208). Bu noktada siber gücün uygulama bulabileceği siber savaşların bir limitinin olduğu ya da siber uzayda bu gücün sürdürülebilirliğinin oluşabilecek ittfaklarda yerinde anlaşılması gerekmektedir.

[126] Şekilde belirtilen *"Garrison Ülkesi (State)"* kavramı, siyaset bilimci ve sosyolog *Harold Laswell* tarafından 1941 yılında, *American Journal of Sociology* dergisinde aynı isimle yayımladığı makalenin de adıdır. Kavram temel önceliği olarak *askeri güvenliği* baz alan devlet örgütlenmesini ifade etmektedir.

Özellikle gelişmekte olan devletlerin bu sınırlarda nasıl hareket ettiği ve nasıl bir güç yapısıyla yoğrulduğu önemli hususlar arasındadır.

3.3.1.1. Siber Savaşın Limitleri

Devletlerin kullanmakta oldukları sunucular ve benzeri bilgi teknolojileri sistemleri aslında evlerde kullanılan bilgisayarlarla aynı özelliklere sahiptir. Bu sistemler de benzer şekilde virüs, bilgi hırsızlığı ve servis dışı kalma gibi tehditlerle karşı karşıya kalmaktadırlar. Siber saldırı yapabilmek için karmaşık sistemlere ihtiyaç yoktur. Kimi durumlarda tek bilgisayarla zararlar oluşturulabilir fakat devletlerin bireysel ya da ortak tutumlarında amaç savunma ve saldırı yönünde politik amaçların güdülmesidir.

Politik amaçlarını doğru noktalara kanalize edebilen gelişmiş ülkeler siber ordular oluşturmuş ve teknolojiye ayak uydurularak sistemler tamamen revize edilmiştir. *Komuta kontrol sistemleri, saldırı ve savunma sistemleri, istihbarat, keşif ve gözetleme sistemleri, muharebe sistemleri* gibi pek çok sistem artık elektronik ortamda, iletişim altyapısı üzerinde çalışmaktadır (Keleştemur, 2015: 167). Askeri sistemlerin siber uzayda korunmasının yanında siber savaşların gözetilmesi ve çıkarsal olarak çarpışmalar savunmadan daha çok saldırı kaynaklı olmaktadır.

Siber savaşlar açasından saldırı kapasitesi ve siber savaşın sonlanmasına ilişkin limitler ölçülemez düzeydedir. İstihbarat örgütleri, askeri birimler yanında suç ve terör örgütleriyle kimi zaman iş birliği yapabilmektedir fakat doğal olarak hiçbir devlet bu türden birliktelikleri kabul etmemektedir.

Bir ülkenin savaşma kapasitesi; sahip olduğu asker sayısı, askerlerin eğitim düzeyi, askeri sistem ve silahlarının gücü, bu sistem ve silahların savaş ve barış ortamlarında üretilebilmesi, kullanılabilme kabiliyetleri ile birlikte milli güç unsurları (teknoloji, ekonomi, sosyal durum, nüfus, coğrafya ve politka gibi) ele alınarak ölçülmektedir. Siber savaş kapasitesine ilişkin ise Keleştemur (2015: 169) devlet kurumları ve özel kurumlar bazında belirleyici bir sınıflandırma yapmıştır ve şu şekildedir:[127]

[127] ABD siber uzayda hem devlet kurumları hem de özel kurumlar anlamında yapılanması en önemli özellikleri bünyesinde barındıran aktörlerden birisidir. Yapısal olarak Rusya ve Çin'den farklılık göstermektedir. ABD,

Devlet kurumlarının siber savaş kabiliyetleri;

- *Aktif siber savaş unsurları,*
- *Uygulanan ve uygulanabilir siber savaş faaliyetleri,*
- *Siber olaylara müdahele ekipleri,*
- *Siber suç önleme ve araştırma ekipleri,*
- *Siber güvenlikle ilgili akademik çalışmalar,*
- *Devlet destekli bilgi teknolojileri projeleri,*
- *İstihbarat unsurları,*
- *Bilgi teknolojilerinin kullanımı,*
- *Bürokratik ve politik derecedeki kullanıcıların bilgi ve tedbir düzeyi,*
- *İnternet kullanıcılarının bilgi ve tedbir düzeyi,*

Özel kurumların siber savaş kabiliyetleri;

- *Aktif internet kullanıcı sayısı,*
- *İnternet kullanıcılarının bilgi ve tedbir düzeyi,*
- *Bilgi teknolojileri ve güvenliği ile ilgili bilgi,*
- *Bilgisayar güvenliği ile ilgili program ve projeler,*
- *Bilgi ve iletişim ağı alt yapısı,*
- *Yazılım geliştirme kapasitesi,*
- *Donanım geliştirme kapasitesi,*
- *Bilgi ve iletişim teknolojileri.*
- *Bilgi güvenliği uzmanları,*
- *Bilgi güvenliği şirketleri,*
- *İnternet servis sağlayıcı kapasitesi,*
- *GSM operatörleri kapasitesi,*
- *Uydu sayısı*
- *SCADA sistem geliştirme ve kullanma kapasitesi.*

Temel olarak sıralanan unsurların yanında, siber savaşın nitelikleri çerçevesinde farklı kapasiteler de belirleyici olabilir fakat siber savaşın hangi unsurlar üzerinde limitlerinin olabileceği hususu devletlerin amaçları ile ilgilidir. Özellikle kritik altyapılar

bu iki ülkenin aksine büyük saldırılar düzenleme yerine, daha komplike yazılımlar geliştirerek, belirli dönemlerde istihbari bilgi elde etmekte ya da sisteme beklenmedik bir anda zarar verebilmektedir.

açısından limitlerin belirsizliği, bireyler ve devletler bazında rahatsız edici bir husustur. Etkilenen fiziksel ortamın yol açabileceği tahribat ve zarar, risk toplumu algısı içerisinde değerlendirilebilecek siber savaşların limitleri açısından belirleyici olacaktır.

Lindsay (2013: 373), *Security Studies* dergisinde *"Stuxnet ve Siber Savaşın Limitleri (Stuxnet and the Limits of Cyber Warfare)"* adlı çalışmasında siber devrimle beraber siber silahların güçsüzlerin de bir seçeneği halini geldiğini vurgularken yaptığı tespitler yaşanan olaylarla birlikte bu alana ilişkin bir sınırsızlığı da gözler önüne sermektedir. Siber savaşın *"Dijital Pearl Harbour"* olarak nitelendirildiği husus, Stuxnet gibi ya da CIA'in 1982 yılında Rus boru hatlarına yapmış olduğu saldırılarla birlikte evrimini sürdürmektedir.

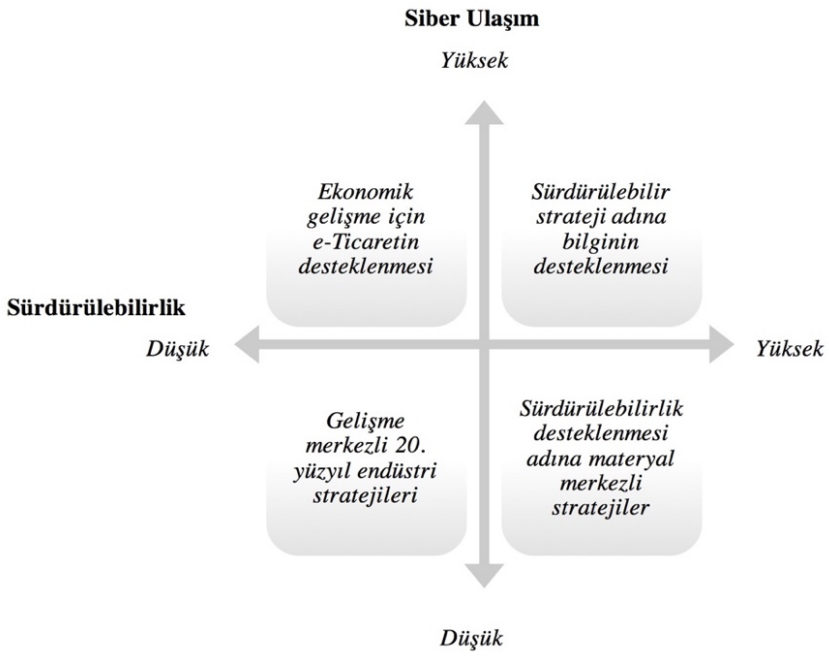
3.3.1.2. Siber Uzay ve Gücün Sürdürülebilirliği

Siber uzay ve bu ortamda gücün sürdürülebilirliği devletlerin bireysel ve ortak hareket etmelerindeki belirleyici unsurlara bağlıdır. Bu temel iki durumu dönemsel olarak karşımıza çıkarmaktadır. Bunlardan ilki sürdürülebilirliğin bireyler arasında genişletilerek devam etme ya da ettirilme arzusu diğeri ise amaçların gerçekleşmesinde aktörlere imkanlar sunulabilmesidir (Choucri, 2012: 205).

Siber uzayda gücün sürdürülebilirliğini, özellikle bu alanda gelişme arzusu içinde olan devletlerin birlikte hareket edebilmesi hususunda ayrıca ele almak gerekmektedir. Bunun nedeni, devletleri bu alanda belirleyici kılan unsurların kendi içerisindeki kompleks durumudur. Zaman zaman bu alanda gelişmiş ülkelere karşı yapılan siber saldırıların, irili ufaklı birçok ülke tarafından tekrarlandığını düşünürsek bu konudaki sürdürülebilirlik güç açısından artarak devam edebilecektir.

Şekil 34'te görüldüğü gibi özellikle siber gücün sürdürülebilirliğinin devam ettirilmesinde bilginin desteklenmesi ve istihbarat faaliyetlerine dönüştürülebilmesi, saldırı kabiliyeti yanında temel noktalardan biridir ve özellikle ekonomik, endüstriyel gelişim açısından da belirleyicidir. Temel olarak bu gelişimdeki deneysel nitelik, sürdürülebilirlik konusundaki durumun ekonomik gelişmeyle olan ilişkisindeki ikilemdir. Siber güvenliğe ilişkin stratejik yönelimlerde bu çok yönlülük belirleyici olmaktadır.

Şekil 34: Siber Uzay ve Sürdürülebilirliğin Stratejik Örneklemesi



Kaynak: Choucri, 2012: 207.

Ülke kapasitelerinin niteliğine bakılmaksızın sürdürülebilirlik açısından siber savunma adına belli unsurların göz önünde olması gerekmektedir. Özellikle hacktivist grupların yönelebileceği kritik altyapılar ve oluşturabileceği tehlike bu alandaki sürdürülebilirlik algısının tamamen değişmesine yol açacaktır. Temel prensip kapasitelerin ve gücün sürdürülebilirliğidir, savunma ve saldırı yönündeki uzun süreli rahatsız edici durum kendi içerisindeki kompleksliği daha da artıracaktır.

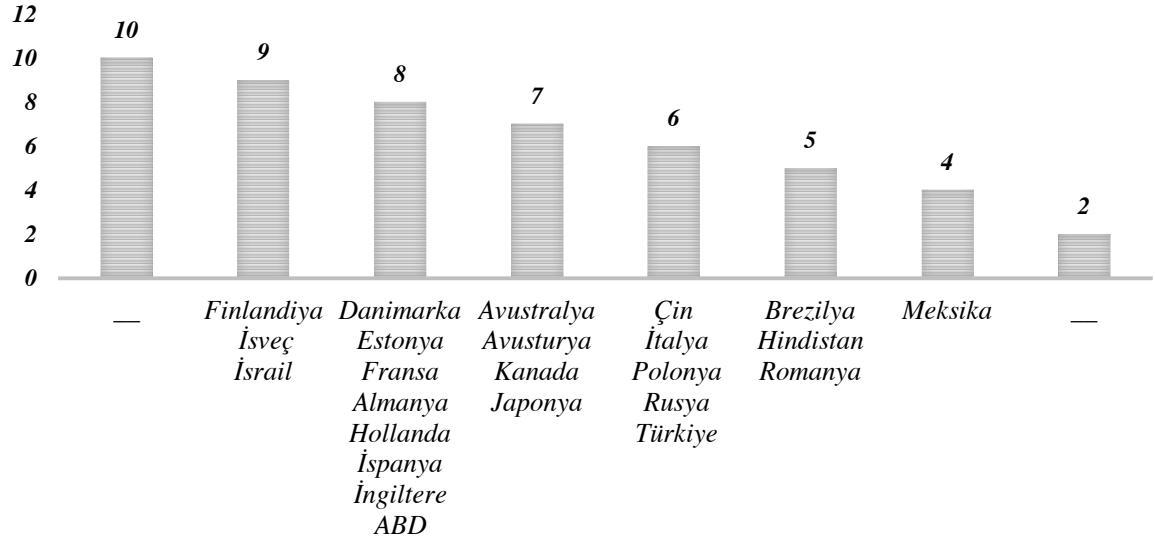
Artan komplekslik içinde siber politikaların, sürdürülebilir şekilde bilgi alanına dönüşmesi ve bu durumun gelişmesinde Choucri (2012: 217) üç temel noktaya dikkat çekmektedir. Bunlar *bilgi alanı ontolojisinin formüle edilmesi, bilgi ağının (networkun) geliştirilmesi* ve *çok yönlü kabiliyetin yaratılması* olarak tanımlanmıştır. Siber politikaların özellikle, uluslararası ilişkiler içindeki temel nitelikleri bu noktalar temelinde şekillendirilmelidir. Bilgi alanı ve ağına ilişkin çalışmalarda ortak noktalar, ülkelerin gelişim konseptlerine ve siber alanı algılayış biçimlerine göre geliştirilmelidir. Siber politikaların oluşturulmasında temel çerçeve ne kadar iyi kurgulanırsa kurgulansın ülkelerin siber alandaki açıkları doğru anlaşılmalıdır.

3.3.1.3. Siber Güç Kapasitesi Açısından Gelişmekte Olan Ülkeler

Siber güç kapasitesini belirlerken, ülkenin teknolojik altyapısının genişliği, aynı zamanda siber saldırıya karşı büyük bir hedef olduğu anlamına gelmektedir. Devletlerin gelişmişlik düzeyleri ile doğru orantılı olabilecek bir konvansiyonel ya da nükleer caydırıcılık kapasitesi siber savaşlar açısından daha da baş ağrıtıcı bir hal alabilir. İnternet teknolojilerinin ve altyapısının gelişmiş olması, kimi zaman ters yönde bir etki yaratabilmektedir.

Ters yönde etkinin yanında bu gelişmişliğin doğru orantılı bir şekilde ele alınabileceği husus siber savunma gücüne ilişkindir. Grafik 21'de yer alan bilgiler McAfee tarafından sunulan *Siber Güvenlik Raporu'*na aittir ve görüldüğü üzere tam kapasite güce sahip ülke mevcut değildir. Diğer taraftan Finlandiya, İsveç, İsrail gibi ülkelerin Rusya, Çin ve ABD gibi ülkelerin önünde siber savunma kabiliyetlerinin olduğu da dikkat çekicidir (Keleştemur, 2015: 171). Ülkelerin siber savunma güçleri her ne kadar karşılaşılan saldırı türleri ve maddi kayıplara göre oranlanılsa da saldırıların yöneliş biçimi ve hedeflenilen unsurlar bu tür sınıflandırmalarda belirleyici olmaktadır. Savunma gücünün siber alanda gelişmekte olan ülkeler açısından ne ifade ettiği denetlenebilir bir husus değildir.

Grafik 21: Ülkelerin Siber Savunma Güçleri



Kaynak: Keleştemur, 2015: 171

Ülkelerin siber saldırı ve savunma güç kapasiteleri açısından gelişmekte olan ülkeler adına belirleyici unsurlar daha çok sahip olunan özelliklerin dağılımıdır. Bu dağılım kendi içerisinde güç kapasitesini belirler ve ayrıştırır. Bu konuda Tablo 14'te görüldüğü üzere, belli özellikler dahilinde ülkeler farklı şekillerde gruplandırılabilmektedir. Birinci grup ülkelerin en ayırıcı özelliği siber güvenlik politikalarının oluşturulması ve bu konudaki yatırımların dağılımıdır. Türkiye'nin de içinde bulunduğu üçüncü grup ülkelerde farkındalık olmasına rağmen, öze ilişkin politikaların üretilemeyişi temel sorunlar arasındadır. Bunun altında yatan sebep, bu tarz ülkelerin siber saldırı ve savaş pozisyonları açısından denetime ihtiyaç duymalarıdır. Dikkat çekici diğer bir husus sınıflandırılan ülkelerin ekonomik gelişmişlik verileriyle doğru orantılı bir ilişkilendirilmenin siber savaş kabiliyetleri açısından yapılamadığıdır.

Tablo 14: Ülkelerin Siber Savaş Kabiliyetlerinin Sınıflandırılması

Grup	***Ülkeler***	***Özellikleri***
Birinci Grup	*ABD* *Çin* *Rusya*	*Siber güvenlik ve savunma geliştirme çabaları üzerine uluslararası politika üretme kabiliyetine sahip ülkelerdir. Bu ülkeler siber savunma konularına en büyük desteği vermekte, siber güvenlik politikaları oluşturma çabalarına en fazla kaynak ve insan desteği sağlamaktadır.*
İkinci Grup	*İngiltere* *Fransa, İsrail*	*Birinci gruptaki ülkeleri yakından takip etmektedirler. Ancak daha az personel ve daha kısıtlı altyapıya sahiptirler.*
Üçüncü Grup	*Türkiye, Hindistan* *Güney Kore* *Tayvan, Almanya* *Kuzey Kore*	*Siber güvenlik politikası ve savunma kabiliyetleri geliştirilmesi için önemli ölçüde kaynak tahsis eden ülkelerdir. Bu alanda lider ülke değildirler. Birçok durumda, birinci gruptaki ülkeleri taklit etmektedirler.*
Dördüncü Grup	*İsveç, Japonya, İran* *Avustralya, Hollanda* *Pakistan, Finlandiya*	*Siber güvenlik ve savunma kabiliyetlerine yönelik kısıtlı kaynak tahsis eden ülkelerdir.*

Kaynak: Çifçi, 2012: 26

Siber güç kapasitesi açısından, siber alanda gelişmekte olan devletler belli düzeyde iyi tanımlanmış kurum ve kuruluşlara sahip olsalar da, kurumsallaşma açısından gelişime duydukları ihtiyaç ortadadır. Bu tür devletler kapsamlı ve devamlı savunma faaliyetlerini kısmen sürdürebilmektedirler fakat saldırılara yönelik güdülerde daha zayıf oldukları gözden kaçırılmamalıdır. Güvenlik stratejileri açısından saldırı güdülerinin oluşturulmasında ittifaklar daha yapıcı gözükmektedir.

3.3.2. Güç Dengesi ve Siber Güvenlik

Hemen hemen her devlet komşusunun benzer nitelikteki fiili veya muhtemel çabalarını önlemek durumundadırlar. Bu nedenle, devletlerin başka devletçe dengelenene kadar gücünü yayma eğilimi içerisinde olacağı söylenebilir. Savaşın önemli nedenleri arasında olan güç dengesindeki bozulma, taraflardan birinde veya birkaçında ortaya çıkan nispi zayıflıklar bu duruma ilişkindir (Sönmezoğlu, 2014: 820). Gücün sosyal bilimler içerisinde, kavramsal yaklaşımlarda belli metaforların kullanılmayışı ve dönüşümdeki en önemli unsur oluşunun göz ardı edilişi *"güç dengesi"* gibi kilit unsurların anlaşılmasını zorlaştırmaktadır (Little, 2007: 19).

Savaşlar arasında bir ayrım yapmak bu noktada, zayıflık temelinde mümkün gözükmemektedir. Eğer bir ayrım yapılacaksa, anlamlı olup olmadığını tespit etmek için, farklı savaşların farklı sonuçları ve etkileri olup olmadığını deneysel olarak incelememiz gerekecektir. Özellikle günümüz çalışmalarına baktığımızda birçok araştırmacının bu konuda zorlandığını ve teorik olarak, *tipolojik anlamda*[128] bir sınıflandırmadan kaçındığını görmekteyiz. Bunun en önemli sebeplerinden birisi özellikle küresel anlamda savaşlar ile devletler-arası savaşların niteliğinin baş döndürücü şekilde değişmesidir.

Küresel savaşlar kamu harcamalarında ve vergi yükünde uzun vadeli artışlara yol açmaktadır ve konvansiyonel, nükleer caydırıcılık oluşturma adına atılan adımlar salt askeri amaçlar gözetildiği zaman ciddi bir ekonomik güce ihtiyaç duymaktadır. Bu düzlemde bakıldığı zaman daha az maliyetli ve daha etkili silahlara, ortak çıkarların uzun vadeli

[128] Vurgulanan tipoloji kavramı savaş tipolojileri açısından farklı yaklaşımlara işaret etmektedir. Savaşların sınıflandırılması açısından yapılan çalışmaların çerçevesi yakın geçmişe dayanmaktadır ve konunun çalışılmasında ciddi felsefi tartışmalar yer almaktadır.

sonuçlar doğurabileceği ittifak arayışlarına ihtiyaç duyulmaktadır. Bu durumun getirmiş olduğu yaklaşım ve kaygılar yakın geçmişte *siber savaşları ve terörizmi* karşımıza çıkarmıştır.

Gücün yoğunlaştığı nokta siber mücadelenin yaşandığı kaotik bir ortamla daha karmaşık bir hal almaktadır. *Güç dengesi*[129] ve *güç üstünlüğü* gibi modeller arasındaki mantıksal çelişkiler bu durumu ispatlar niteliktedir. Özellikle devletlerin güç elde etme konusunda başarı sağlaması, bunun baskın hale getirilmesi anlamında saldırgan bir niteliğe bürünmektedir.[130] ABD'nin siber gücün elde edilmesi konusundaki başarısı ve *ABD Siber Savunma Komutanlığı*'nın çok yönlü düzlemdeki atakları bu konuda tipik bir örnektir.

ABD Siber Savunma Komutanlığı'nın, askeri ve sivil ağları saldırılara karşı koruması ve kendi siber saldırı stratejilerini geliştirerek farklı ülkelerdeki grup ya da gruplarla iş birliği içinde çalışması, ittifak oluşturması, bu durumun önemli örneklerindendir. ABD içerisinde siber bir ordu haline gelen bu komutanlığın 2020 başlarına kadar, 135 farklı ekip içinde yaklaşık 7 bin kişilik askeri ve sivil teknik personele ulaşması beklenmektedir ve *güç dengesi* açısından farklı ülkeleri birbirlerine yakınlaştıracaktır. Özel bir ilgi alanı oluşturacak siber savaş resmi makamlarca daha çok anılacaktır.

Savaş mantığı içinde, devletlerin özellikle baskın güçlere karşı oluşturacakları *siber ittifaklar* eğer çıkarların çarpıştığı noktada kesişirse, siber terörizm dediğimiz olgu siber savaşla birlikte yeni bir sorunsalı oluşturabilir. Dengeyi sürdürmek için birbirine yakınlaşacak devletler veya gruplar gücün nispeten dağınık ve ittifakların esnek olduğu yapılanmada uluslararası sistem içerisinde kendine yer bulmaya çalışacaktır. Herhangi bir devletin atmış olduğu bir adıma karşı farklı devletlerin benzer yapılanmalara gitmesi ve askeri, taktiksel unsurlarla karşı karşıya gelmeleri, ittifak sistemleri içinde yakınlaşmaları

[129] *Güç dengesi* olarak belirtilen kavram, dünya politikasındaki güç mücadelesini süreklilik boyutuyla ele alır. Siber mücadeleye ilişkin uluslararası sistemin geldiği boyut özellikle süreklilik açısından bu durumla örtüşmektedir. Tehdit olgusu siber saldırılarla birlikte, bu tür kavramlar açısından çalışmaları daha da net şekillendirecektir.

[130] Uluslararası ilişkiler çalışmaları açısından devletlerin güç mücadelesi içerisinde temel aktör olarak ele alınması olağandır. Fakat devlet-dışı aktörlerin siber saldırılar açısından mağdur olduğu noktalar vardır. Bu aktörlerin nasıl tasnifleneceği ve siber mücadele açısından nasıl bir gruplandırma oluşturulacağı başlı başına bir tartışma konusudur. Farklı şirketlerin ve illegal oluşumların da iç içe girdiği siber alan, mücadelenin boyutunu ve karmaşıklığını gözler önüne sermektedir.

beraberinde getirecektir. Görünmeyen siber saldırılar caydırıcılık oluşturma adına, saldıran aktörlerin itiraflarıyla gövde gösterisine dönüşecektir.

Güç dengesi yaklaşımıyla oluşacak kutuplaşmalarda tıpkı konvansiyonel unsurların görsel şova dönüştüğü zamanlarda, siber saldırı kapasitelerine ve unsurlarına vurgu yapılması olağandır. Caydırıcı olabilme adına kurulan siber ordulara karşı güç dengesinin gözetilmesi kaçınılmaz durmaktadır ve gelecek kurgusu bu yöne kaymaktadır (Freedman, 1989: 201).[131]

Güç dengesinin, zorlayıcı tehditler ile kolay bir zafer elde etmenin çekiciliğini ortadan kaldıracağı düşünülebilir. Özellikle yakın gelecekte siber bir güç haline gelecek ve siber savaş kavramını tüm unsurlarıyla hissettirecek bir aktör tam anlamıyla bu başlık altında konuşulmaya başlanacaktır. Tek başına güç dengesinin veya göreli eşitliğin, taraflardan birinin diğerine saldırmasını önleyeceğine dair rasyonel bir gerekçe de yoktur.

3.3.3. Siber Güvenlikte Savunma Disiplini

Siber savunma faaliyetlerinde başarılı olabilmek için, ülke seviyesindeki devlet kurumlarının yapması gereken işler ve alması gereken tedbirler vardır. Bu şekilde, bir çeşit derinliğine savunma mekanizması ile katmanlı bir güvenlik yapısı kurulması ve saldırılara karşı daha emniyetli olunması sağlanmış olmaktadır. Oluşacak savunma disiplinine ilişkin veriler olaylara ve oluşabilecek ittifak çeşidine göre farklılık sağlamaktadır. Çifçi (2012: 215)'ye göre devlet birimlerinin siber savunmadaki görünür rolleri şu şekildedir:

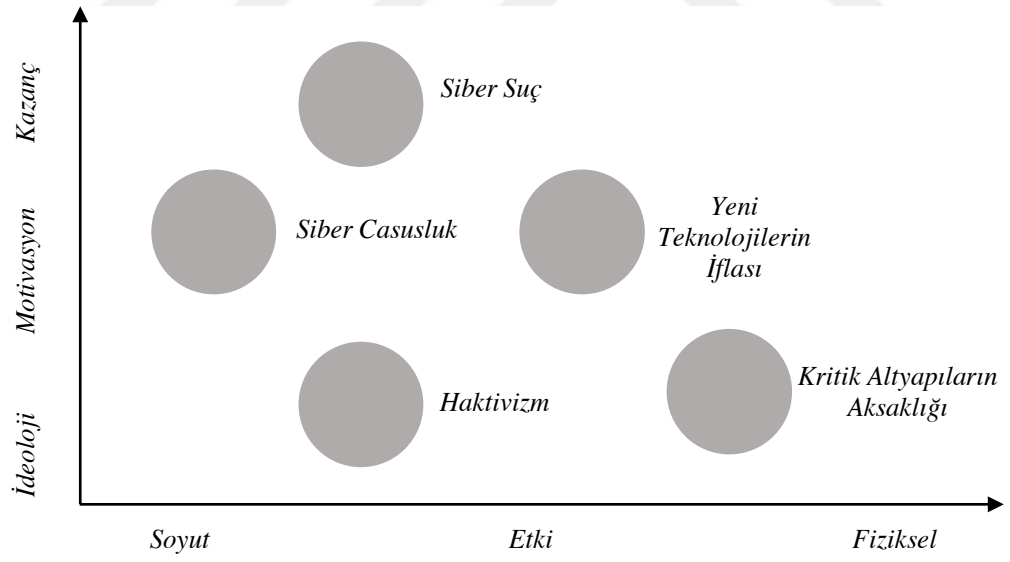
- *Bilgisayar ağ savunması ile ilgili hususlarda araştırma ve geliştirme faaliyetlerine destek olmak ve standartları oluşturmak,*
- *Özel sektörü, kendi sistemlerini emniyetli hale getirme konusunda teşvik etmek,*
- *Adli bilişim, tuzak kod analizi, balküpü tuzaklarının yerleştirilmesi gibi konulara yönelen kaynakları artırmak,*

[131] Wallerstein (2011: 106), güçlü devletler arasındaki rekabet ve yarı-çevre ülkelerinin statü ve güçlerini yükseltme çabalarını, süregiden bir devletlerarası rekabetle sonuçlandığını belirtmektedir. Bu rekabetin normalde güç dengesi denen bir biçim aldığını ve güç dengesinin devletlerarası arenada bazı devletlerin istemedeği, kendiliğinden yapamadığı bir duruma dönüştüğünü vurgulamaktadır.

- *Kamu, özel sektör ve üniversitelerdeki siber savunma ve bilgi sistemleri konularıyla iştigal edenler arasında bilgi paylaşımını teşvik etmek,*
- *Siber tehdit istihbaratının toplanması ve ilgili kurum ve kuruluşlarla paylaşılması için yatırım yapmak,*
- *Bilgisayar güvenliği uzmanlarının eğitimlerine mali destek sağlamak.*

Grafik 22'de görüldüğü üzere, siber savunma disiplini açısından hedeflenilen unsurlar, kullanılan araçlarla *motivasyon (ideoloji-motivasyon-kazanç)* bütünlüğünde, *etkisel (soyut-etki-fizik)* olarak bir ağırlığa sahiptir. Siber suçların motivasyon bütünlüğünde en çok kazanç sağladığı dikkat çekerken, fiziksel altyapılara ilişkin motivasyon etki oranında en fazla ağırlığa sahiptir. Kimi yaklaşımlara göre bu durum göreli bir husustur. Özellikle siber savaşın bir bütün olarak, günümüz gelişmelerinde motivasyon yönünde sağladığı toplam ağırlık ülkelerin ilgisini çekmektedir.[132]

Grafik 22: Motivasyon ve Etkiye Göre Siber Risk



Kaynak: Cyber Research Center-Industrial Control Systems, White Paper, 2016: 11

[132] Uluslararası bir yapılanma olarak NATO 2017 yılı içinde, siber savunma adına tüm devletler için daha da fazla uyum sürecini devreye sokmuştur. NATO üye ülkeler bazında, tatbikatlar ve bilgi güvenliği açısından en somut adımları atan örgütlenme olarak dikkat çekicidir. Yatırımların inavosyon yönüne kaydırılması ve eğitim düzeyinde, NATO bünyesinde başlatılan girişimler takdire değerdir.

Ülkedeki tüm bilgisayarları saldırılara karşı koruma imkanı gözükmemektedir fakat siber saldırganların hedef alabileceği bazı ağları, özellikle de kritik altyapıları, saldırılara karşı korumak şarttır. Savunma disiplini açısından askeri bilişim sistemlerinde kullanılan yazılım ve donanımlar, sivil ağlar ile çoğunlukla aynı olduğundan hemen hemen aynı zafiyetlere sahiptirler.

Siber saldırıların etkileri çoğunlukla geçici olduğundan, silahlı kuvvetlerin öncelikle yapması gereken, büyük ve etkili siber saldırılar sonrasında zarar gören sistemlerin zafiyetinden faydalanmak suretiyle fiziksel saldırıların gelip gelmeyeceğini anlamaktır. İkinci öncelik sistemi onarmak, üçüncü öncelik ise sistemi bozan saldırganın hala hedefi gözetlediği varsayımıyla hasarı az göstermeye çalışmaktır (Çifçi, 2012: 216).

İttifak algısı açısından savunma disiplininin temelinde siber ordularla ortak hareket edebilme ve oluşacak bir savunma mimarisi pratikteki algının artırılması açısından önemli konuların başında gelmektedir. Siber orduların harekat alanları ve oluşturulacak bir savunma mimarisi gelecek kurgusu açısından devletlerin birbirlerine olan güvenini artırmaktadır.

3.3.3.1. Siber Ordular ve Ortak Hareket Edebilme

ABD, Rusya ve Çin başta olmak üzere çoğu ülke siber ordulara yatırım yapmaktadır ve bu yatırımın gelecek 10 yılda, bugünkü gelişme kapasitesiyle 5 trilyon doları aşması beklenmektedir. Özellikle ordu düzeyinde, nitelikli personelin yetiştirilmesi ve istihdam edilmesi hususunda yatırımlar yapan ülkeler bu durumun giderek maliyetinin de arttığının farkındadırlar (Arnold ve diğerleri, 2013: 3).

Her ne kadar saldırı unsurlarının kimi zaman basit araçlarla gerçekleşmesi mümkün olsa da, bu araçların gerekli harekat kabiliyetinin hedefe yönelik olarak gelişitirilmesi konusunda, hem donanımlı hem de yetenekli personele ihtiyaç duyulmaktadır. Bu durumun farklı araçlarla, daha kompleks olması ve çıkarsal bütünlüğün farklı ülkelerin ortak hedeflerinde buluşması durumunda, ortak hareket edebilme becerisi ve uluslararası politika adına ittifak olgusu devreye girmektedir. Konuyla ilgili zemin uluslararası ilişkiler düzeyinde, alanın interdisipliner yönünden ayrı düşünülmemelidir.

Siber orduların kurulması ve geliştirilmesi hususunda, Türkiye gibi gelişmekte olan ülkelerin bu konudaki uzman açığının kapatılması yönünde bazı uzmanlar hacker grupları arasından seçilmektedir. Savunma kuvvetleri açısından, askeri yapılanma içerisinde eğitimle oluşturulması gereken orduların harekat alanı daha geniş olmaktadır ve daha kurumsal bir nitelik taşıyarak siber politikaların önü açılmaktadır.

ABD Siber Savunma Komutanlığı, Amerika'nın askeri ve bazı sivil ağlarını saldırılara karşı korumakta ve gerekirse kendi siber saldırı stratejilerini geliştirmektedir. Bu durum çevre ülkelerle olan ortak hareket edebilme güdüsünü geliştirip politikalar üretmesini sağlarken, diğer yandan gelişmişlik düzeyiyle karar alıcı olarak diğer devletleri etkileyebilmektedir ve personel ihtiyacı açısından örnek alınmaktadır (Austin, 2016: 8).

Endüstriyel sanayiye ihtiyaç duyan konvansiyonel silahların geliştirilmesinin mali boyutları, siber orduların yapılanmasını uzun vadede daha tercih edilir hale getirmektedir. Siber ittifakların oluşturulması, gelişmiş siber orduların devletler içerisinde oluşturulmasıyla daha kazançlı sonuçlar doğurmaktadır. Realistlerin, ittifakların ulusal çıkarla alışkanlığa dönüştüğü yönündeki savı siber ittifaklarla kendini ispatlama zemini bulmuştur fakat inşacı bakış açısının uluslararası sistemdeki tüm gelişmeleri dikkate alan atıfları bu durumu açıklamada daha gerçekçi durmaktadır.

Siber orduların kurulması hususunda kullanılabilecek silah geliştirme maliyetleri ve araştırma geliştirme faaliyetleri açısından geleneksel unsurların daha maliyetli olduğu bir gerçektir ve ortak hareket edebilmede devletleri seçici kılarak daha güçlüye yöneltmektedir. Oysa siber ordular ve ortak hareket edebilme açısından silah geliştirme maliyetleri daha uygun bütçelerle sağlandığı için bu unsur ortadan kalkabilecek ve devletler yakın coğrafyalardaki tüm ülkelerle ortak programlar ve ittifakler yürütebilecektir.

Tablo 15'te görüldüğü üzere askeri hedefler, sivil hedefler ve kritik altyapılara yönelik siber saldırı silahlarının geliştirilmesindeki maliyet devletler adına farklılık göstermektedir. Ekonomik anlamda devletlerin içerisinde bulunduğu kronik sorunlar siber orduların geliştirilmesinde ve ortak harekat güdüsünde itici güç olacaktır. Caydırıcılığını koruyan bazı konvansiyonel silahların geliştirilmesi ve nükleer anlamda gelişim, yine gelişmiş ülkeler adına masada bir kart olarak var olacaktır.

Tablo 15: Silah Geliştirme Maliyeti

Silah Sistemi	***Maliyet (USD)***	***Kimler Geliştirebilir?***
Görünmez Savaş Uçağı	*397 Milyar (F-35)*	*ABD, Çin, Rusya*
Nükleer Denizaltı	*11 Milyar*	*ABD, Rusya, İngiltere, Fransa, Çin, Hindistan*
Askeri Hedefler İçin Siber Silah programı	*1 Milyar*	*Gelişmiş Ülkeler*
Sivil Hedefler İçin Siber Silah Programı	*100 Milyon*	*Gelişmiş ve gelişmekte olan tüm ülkeler*
Kritik Bir Altyapıya Yönelik Siber Saldırı	*5 Milyon*	*Herkes (devlet, teröristler, organize suç örgütleri…)*
Ulusal Siber Güvenlik Programı (sivil)	*>1 Milyar*	*Politika, Strateji, İcra (5-10 sene)*

Kaynak: Taytaş, 2016

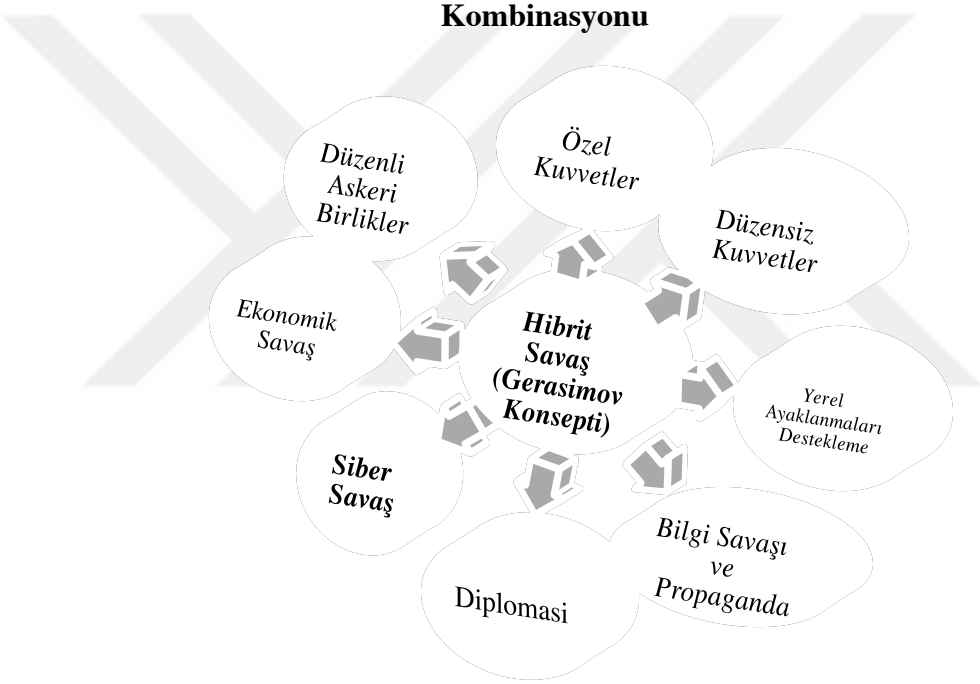
3.3.3.2. Ortak Siber Savunma Mimarisi

Herhangi bir kurumun (askeri, devlete ait ve özel) işlediği bilgiler farklı gizlilik derecesindedir. Devletlerin siber saldırılarda ve savunmada uyguladıkları strateji bütünlüğü, gözettikleri çıkarlar farklılık göstermektedir. Her kurumun, başkalarının eline geçmesini istemediği bilgileri olabilir ve bu konuda sürekli bir gizlilik temel alınabilir. Bunun yanında, başkaları ile paylaşılan bilgiler de vardır. Bazı hizmetleri alabilmek ve erişebilirliği sağlamak için kurumlar kendi bilgi sistemlerini internet gibi dış dünyaya bağlamak, bir yolla irtibat kurmak zorunda kalabilirler. Savunma mimarisi olarak üstesinden gelinmesi gereken noktalar şunlardır (Çifçi, 2012: 192):

- *Gizlilik dereceli ve gizliliği olmayan iletişim ağlarının birbirlerinden ayrılması,*
- *Gizlilik dereceli olmayan ağlar için de uygun bir şekilde güvenlik tedbirlerinin alınması,*
- *Gizlilik dereceli sistemlerin diğer sistemlerden gerçekten yalıtılmış olduğunun garanti altına alınması.*

Siber savunma mimarisinin oluşmasında her devlet kendi önceliklerini ve eksikliklerini analiz yeteneğine sahip olmalıdır. Şekil 35, Rusya bazında ele alınan *Hibrit Savaş (Gerasimov) Konsepti*'nde bu ayrımın ve önceliklerin temel unsurlarını göstermektedir. Gerasimov konsepti, siber savaş yanında ekonomik savaş, diplomasi, bilgi savaşı ve propaganda, düzenli askeri birlikler, özel kuvvetler, düzensiz kuvvetler ve hatta karşı taraftaki yerel ayaklanmaların desteklenmesini de aynı kategoriye alarak bir kombinasyon oluşturmuştur. Oluşturulacak her mimari ve devletlerin bu alandaki ortak noktaları özellikle yakın ittifakların kurulmasında çıkarsal kesişmeler doğurabilir.

Şekil 35: Konvansiyonel ve Konvansiyonel Olmayan Savaş Unsurlarının Çoklu Kombinasyonu



Kaynak: Ting, 2015

Ortak siber savunma mimarisi oluşturmada dikkate alınacak hususlardan birisi de devletlerin belli güç paydalarında buluşabilmeleri ve bunu orantılayabilmeleri ile ilgilidir. Siber kontrollü sistemleri daha fazla kullanması ve ulusal siber savunma sistemi eksikliklerinden dolayı ABD, günümüzde Rusya ya da Çin'e kıyasla, hatta siber alanda gelişmekte olan bir devlete göre saldırılara daha açık konumdadır. Özellikle uluslararası alanda, güvenlik temelli mücadelelerde geliştirilen her yön rakip kuvvetlerin temel hedefi haline dönüşebilmektedir. ABD siber savaş kapasitesi olmayan, ama yetenekli hacker

ekipleri kiralayabilecek devletler veya devlet sayılamayacak unsurlar tarafından tehdit bile edilebilir (Clarke ve Knake, 2010: 82).[133]

Tehdit edilme ve saldırılara açık olma durumu, savunma mimarisi oluşturma adına çıkar elde etmek isteyen devletlerle daha geri planda kalmaktadır. Ortak savunma sistemi oluşturmuş ve ittifak olgusunu güçlendirmiş devletlerin, olası bir saldırıyı etkisiz hale getireceği konusunda şüpheleri bulunan bir saldırgan için caydırıcılık oranı büyük ölçüde artacaktır. Bunun temel nedeni kontrol mekanizmasının çeşitliliği ve anlık veri paylaşımının önemidir.

3.3.4. Ad-hoc Siber İttifaklar

Uluslararası politika literatüründe, başka birçok konuda olduğu gibi ittifaklar açısından da genel kabul görmüş bir tipolojiden sözetmek mümkün gözükmemektedir. Konuyla ilgilenen birçok uzman, ittifakları sınıflandırmak için farklı kriterler önermekte, böylece ortaya çeşitli gruplandırmalar çıkmaktadır.[134] İttifaklar amaçları açısından *özdeş*, *tamamlayıcı* ve *ideolojik*; taraflara getirdiği yükümlülükler açısından *karşılıklı* ve *tek taraflı*; kapsamları açısından *genel* ve *sınırlı*; kapsadıkları süre açısından *sürekli* ve *geçici* türden sınıflandırmalara tabi tutulmaktadır (Sönmezoğlu, 2014: 429). Dedeoğlu (2003: 224) ise ittifak sistemlerini temel olarak şu şekilde sınıflandırmıştır:

> - *"Birinci türde geçici ittifaklar vardır. Devletler, belirli bir olgu, olay ya da aktör karşısında o olay, olgu ya da aktör bertaraf edilene kadar bir araya gelebilirler. Genellikle, savaşlar sırasında kurulan ittifaklar, belirli operasyonlar sırasında yapılan işbirlikleri, bu türe girmektedir.*
> - *İkinci tür ittifaklarda kollektif güvenlik esaslı yapılanma vardır. Üye devletlerin tüm güvenlik anlayışlarını ortaklarına göre değiştirmeleri beklenmemektedir. Belirli tehdit konularında aynı görüşleri paylaşan devletler, bu tehdide karşı güç birliği oluşturma konusunda anlaşmaktadırlar ve gerekli önlemleri birlikte alma kararı vermektedirler.*

[133] ABD başka ülkelere göre daha gelişmiş siber saldırı olanaklarına sahip olabilir fakat Çin, ABD'nin büyük kentlerindeki elektrik şebekelerini haftalarca arızaya uğratır, verilerini bozarak finans pazarlarının kapanmasına neden olur ve demiryolu hatlarında yönlendirme sistemlerini bozarak gıda ve parça sıkıntılarına yol açarsa, siber saldırı olanaklarınızın üstünlüğü işe yaramayacaktır.

[134] Michael Barnett (2014: 445) ittifakların prensipten ziyade amaca uygunluk tarafından yönlendirildiklerini, başlıca motivasyonlarının, bir takım yakın ya da uzak tehlikeler karşısında devlet güvenliğini artırmak olduğunu ve fikirsel, yerel menfaatlerin ikincil dereceden önemli olduğunu, bu konuda bir uluslararası ilişkiler mutabakatının varlığını özellikle vurgulamaktadır.

- *Üçüncü tür ittifaklarda ise ortak (commune) güvenlik söz konusudur. Bu tür güvenlik anlayışı, başka alanlarda ortaklık kurmuş olan devletlerin güvenlik ve savunma konusunda ortak politikalar yürütmeleri, tek bir strateji geliştirmeleri anlamı taşımaktadır."*[135]

Çalışma kapsamında vurgulanan ittifak biçimi, birinci türde ele alınan geçici ittifakların ve çalışma biçiminin siber diplomasi masalarıyla birlikte, ad-hoc yapıda işleyebilirliği ile ilgilidir. İttifakın ad-hoc niteliği, bu türden ittifakın tam olarak amaca yönelik kullanılması ile alakalıdır. İttifak türünün uygulanma biçimi ve etkinliği geçici bir çözüme ve saldırı biçimine göre yer almalıdır ve harekat yapısı buna göre şekillendirilebilir.

Ad-hoc siber ittifakın temel gelişim mantığı NATO ve benzeri yapılanmalar ile karıştırılmamalıdır. NATO'nun özellikle *alan dışılık (out of area)* tartışmalarıyla beraber temel konseptinin tartışılması siber politikalarda da kendini göstermiştir. Bu türden bir farklılaşma ile birlikte üye ülkeler arasındaki birliktelik siber politikalar ile birlikte kimi zaman ortak harekatlarla devam etse de, ad-hoc siber ittifaklarda durum daha farklı bir çerçevede ele alınmalıdır.

Özellikle Türkiye gibi ülkelerin çevre ülkelerle yaşadığı sorunlarda bu türden ittifakların kuruluşu zamana ve duruma göre farklılık gösterebilir. Belli ittifaklar dahilinde hareket eden kimi ülkeler bu durumun öncesinde ve sonrasında kimi örneklerde çatışmalı durumlardan çıkıp birliktelikler oluşturabilmektedirler. Çatışmalar derin yapıdaki çelişkiler ışığında ele alınarak değerlendirilmelidir (Galtung, 2009: 218).

Tablo 16 ve Tablo 17, hem ortak olmadan önce çatışmalı olma durumu, hem de kimi bölgelerde aynı entegrasyon dahilinde olup çatışmalı sorunları bulunan ülke gruplarını göstermektedir. İlk olarak tartışılabilecek hususlardan birisi bu tip entegrasyonların başarı niteliği ile ilgili olsa da, pratikte bir araya gelebilen bu türden ülkelerin ad-hoc siber ittifaklara olumlu bakacağı, saldırı kapasiteleri açısından bir gerçekliktir.

Tablo 16'da görüleceği üzere, ekonomik ortaklık kurabilen kimi ülkeler bu birliktelikler öncesinde kimi zaman ciddi çatışmalar yaşamışlardır ve bu durum birliktelik

[135] Birinci tür ittifaka *Kutsal İttifak*, ikinci türe *NATO* ve üçüncü türe *AB Güvenlik ve Savunma Politikası* örnek verilebilir.

oluşturmaya engel olmamıştır. Siber anlamda çıkar elde etme adına oluşturulacak ittifakların kuruluş süreci ve aşamaları daha kolay olacaktır. Özellikle Fransa ve Almanya, Yunanistan ve Türkiye, Güney Kore ve Japonya gibi ülkelerin yakın coğrafyalarda, güvenlik temeli de içeren işbirliklerinde yer almaları önemli örneklerdir. Her ne kadar genelde bir araya gelinmiş yakın coğrafyalardaki birliktelikler ekonomik amaçlar içerse de, askeri güvenlik perspektifinden düzenlemeler entegrasyon sonrasındaki süreçte gecikmemiştir.

Tablo 16: Bölgesel Ticaret Ortağı Olmadan Önce Devletlerarası Çatışmalı Sorunlara Sahip Olan Ülkeler

Çatışmalı Ülkeler	***İşbirliği Adı***
Ekvator-Peru	*Andean Topluluğu*
Fransa-Almanya	*AB*
Yugoslayvya-Bulgaristan	*COMECON*
Yunanistan-Türkiye	*KEİ*
Güney Kore-Japonya	*APEC, ASEAN+3*

Kaynak: Alkan, 2006: 27

Andean Topluluğu adına, her ne kadar ortak güvenlik alanında üye ülkeler arasındaki iletişim artmış olsa da, grubun nispeten küçük ve zayıf ekonomilerden oluşması askeri bir oluşumu gündem dışına itmiştir. AB'de, *AGSP* birliğe askeri ve sivil yetenekler sağlamaktadır. Bu durum, yakın coğrafyalarda hem çatışmalı ülkeler arasında, hem de diğer ülkelerle güvenlik alanındaki entegrasyona iyi bir örnektir. NATO ile çoğu konuda ortak harekat kabiliyetleri örgütün operasyonel alanını genişletmiştir. Dönemsel olarak sorunlar yaşayan *Türkiye, Bulgaristan, Gürcistan, Romanya, Rusya Federasyonu* ve *Ukrayna* gibi bölge ülkeleri arasında 2001 yılında oluşturulan *Karadeniz Deniz İş Birliği Görev Grubu (BLACKSEAFOR)* da askeri birliktelikler açısından, güvenlik temelinde işbirliklerinin oluşturulabileceğini, bu durumun daha fazla mikro niteliğe taşınması gerektiğini de ortaya koyan yapılanmalar arasında olmuştur.

Tablo 17, halihazırda aynı entegrasyon dahilinde olup, diğer taraftan sorunların yaşandığı ülke gruplarını ve bulundukları işbirliklerini göstermektedir. Gerek sınır sorunları,

gerekse tarihi süreçle gelen sorunların yaşandığı yakın coğrafyalardaki ülkeler, yine de ortak iş birliği çatıları altında yer almayı başarmaktadır. Her ne kadar başarıları tartışmalı da olsa teorik düzeyi aşıp pratikte, ortaklık içinde olan bu ülkeler kimi zaman güvenlik refleksi de gösterebilmektedir. Bu refleksler sadece dış politika temelli olmayıp, tarihsel sürece bağlı olarak iç sorunlarla da ilişkili olabilmektedir.

Tablo 17: Aynı Entegrasyon Dahilinde Olup Çatışmalı Sorunları Bulunan Ülkeler[136]

Çatışmalı Ülkeler	***İşbirliği Adı***
Şili-Arjantin	*Andean Topluluğu*
Fas-Cezayir	*Arap-Mağrep Birliği*
Benin-Nijerya	*ECOWAS*
Hindistan-Pakistan	*SAARC*
Tayland-Kuzey Vietnam	*ASEAN*

Kaynak: Alkan, 2006: 27

Aynı entegrasyon dahilinde olup sorunların devam etmesi, bölgesel olarak birbirlerini denetleme güdüsüyle hareket eden ülkeler açısından güvenlik ikilemini ortaya çıkarsa da geçici olarak kimi çıkarsal konularda devletleri birbirilerine yakınlaştırmaktadır. 1978 yılında Beagle sınır sorunuyla, savaşın bile eşiğine gelen Şili ve Arjantin, Andean Topluluğu içerisinde bu örneği oluşturmaktadır. Hatta Falkland Adaları'na ilişkin sorunda ve mücadelede Şili'nin 1982 yılında İngiltere'yi desteklemesinin altında bu neden yatmaktadır. Fas ile Cezayir arasında, 1994'te Marakeş'te yaşanan otel saldırısında Fas'ın Cezayir'i sorumlu tutması ile kapalı olan sınır sorunlarına rağmen, entegrasyon süreci ve zirvelerde ortak hareket etme dikkat çekmektedir. *SAARC* bünyesinde yer alan Hindistan ve Pakistan, bölgesel bir iş birliğinde kimi zaman güvenlik ve askeri sorunların yer aldığı zirvelerde bir araya gelebilmektedir. Verilen reaksiyonlar dönemsel nitelik gösterse de pratikte önemli örnekleri oluşturmaktadır.

[136] Şili ve Arjantin Andean Topluluğu içerisinde *"Associate Member"* olarak yer almaktadır. Kısmi antlaşmalara imza koyan her iki devlet çoğu düzenlemede aktif olarak da yer almaktadır. Andean Topluluğu'nun kurucu üyelerinden olan Şili, 1976 yılında birlik ülkeleri arasında yaşanan bir dizi sorundan sonra üyelikten çekilmiştir ve şu anda *"Associate Member"* statütüsündedir.

Gerek aynı entegrasyon dahilindeyken sorunları olan, gerekse entegrasyon öncesinde çatışmalar yaşamış ülkeler, güvenlik konularında hem denetim hem de çıkarsal bütünlük oluşturma adına bir araya gelebilmektedirler. Siber güvenliğin askeri boyutlara kaydığı alanlarda güvenlik ikilemi aşıldığı zaman ve güven ortamı olduğunda çıkarsal olarak geçici ortaklıkların kurulabileceği verisel olarak siber saldırıların gelişiminde gözlenebilmektedir (Brookes, 2015: 6).

Siber saldırı yeteneklerinin güçlendirilmesi ve oluşacak siber diplomasi kanatlarıyla birlikteliğin çıkarsal yönü tartışmaya açılabilir. Özellikle operasyonel unsurların oluşturulması, hedeflerin belirlenmesi ve zafiyet oluşturmama adına kritik altyapıların korunmasıyla bu birliktelikler ad-hoc nitelikte tekrarlanabilir. Devletlerin siber alana ilişkin oluşturdukları politikalar, tek başlarına oluşturacakları politik misyonla uzun vadede başarısızlığa uğrayabilecektir.

3.3.4.1. Siber Saldırı Yeteneklerinin Güçlendirilmesi

Siber savaşı etkin bir şekilde sürdürmek için destekleyici faaliyetlerin varlığına ihtiyaç duyulmaktadır ve sahip olunan yetenekler güçlendirilmelidir. Bu faaliyetler özel eğitim, özel işlem ve özel politikalar gerektirmektedir. Siber destek faaliyetlerini, siber savaşa *doğrudan destek olan* ve *dolaylı destek olan faaliyetler* olarak ikiye ayırmak mümkündür. Doğrudan destek faaliyetleri, siber savaşın yürütülmesine aktif ve açık bir katkı sağlarken, dolaylı olarak destek faaliyetleri, sonuçlar ve etkileri itibariyle siber savaşa katkıda bulunmaktadır (Çifçi, 2012: 11). Siber savaşa ilişkin, ittifak formasyonunda temel yaklaşım iç yönetim ile de alakalıdır ve hiyerarşik olarak desteklerin varlığı belli bir hukuksal dayanak gerektirmektedir (Libicki, 2007: 129).

Siber saldırı faaliyetlerinin kapsamı ve saldırı yetenekleri, destekleyici faaliyetler açısından daha kompleks bir hal almıştır. Birinci bölümde değinilen saldırı çeşitlerinin ve siber silahların yanında, siber saldırılar kendi içerisinde yetenek ve hiyerarşi de kazanmıştır. Şekil 36'da görüldüğü üzere, stratejik alana ilişkin farklı unsurlarda, farklı saldırı adımları ile hareket edilir bir sistem içerisinde, yeteneklerin de çeşitlendirilmesi gerekmektedir. Bu saldırı adımlarında teknik zeminin oturtulmasından sonra hareketlenmenin sağlanması ve hedefin belirlenmesine ilişkin gelişim temel olarak baz alınmalıdır.

Şekil 36: Stratejik Kurumlara Yönelik Saldırı Adımları

Kaynak: Başaran, 2014

Farklı basamak ve aşamalarda gelişim gösteren siber saldırı yetenekleri her adımda ayrı bir ilgi ve uzmanlık alanı gerektirmektedir. Sosyal ve teknik alanın buluşturulduğu siber güvenliğin interdisipliner boyutunda hem karar alıcıların örgütlenmesi, hem de teknik boyutun şekillendirilmesi vizyoner bir nitelik gerektirmektedir. Bu konudaki yatırım ve ekonomik yük her geçen gün artmaktadır.

Artan ekonomik yük ve yatırım bütçeleriyle birlikte, uluslararası örgütlenmeler ve devletlerin siber saldırı yetenekleri ciddi bir kapasiteye ulaşmıştır. Siber ittifak mantığıyla daha büyük yapılanmalar yerine ad-hoc siber ittifakların oluşturulmasında, araştırma geliştirme faaliyetlerinin siber güvenliğin özel alanlarına ve ihtiyaçlarına yoğunlaşması bu noktada ciddi bir avantaj sağlayabilir. Bunun farkında olan ABD, İngiltere ve İsrail gibi ülkeler gerek siber saldırı yetenekleri, gerekse savunma unsurlarının oluşturulmasında yatırımlarını artırmaktadırlar.

Tablo 18'de görüldüğü üzere, NATO bünyesindeki kimi birimlerin operasyonel yeteneklere kavuşturulmasında ciddi yatırımlar yapılmıştır. ABD kısa dönem planları yaparak farklı bütçe planları uygulamakta ve İngiltere, İsrail gibi ülkeler savunma boyutunda yatırımlar yapmaktadır. Savunma ve saldırı yeteneklerinin ortak bir noktada buluştuğu siber

güvenlik konsepti, halen gelişmekte olan ülkeler adına yatırımların kanalize edilemediği bir boyut olarak da siber ittifakları bu ülkeler adına gerekli kılmaktadır.

Tablo 18: Ülkelerin Siber Savaş Harcamaları

NATO	***2012***	*Siber savunma yeteneklerinin geliştirilmesi ve NATO NCIRC'ın operasyonel yeteneklere kavuşturulması*	***58 Milyon Euro***
ABD	***2013-2017***	*Belirtilen yıllar için ayrılan bütçedir. DARPA askeri ihtiyaçların, siber saldırı yeteneklerinin geliştirilmesi için odaklanmıştır.*	***1.54 Milyar Dolar***
Birleşik Krallık	***2012***	*Tehlikeli virüs ve hackerların karşısında caydırıcılığın arttırılmasında ekstra yatırımlar yapılmaktadır.*	***650 Milyon Euro***
İsrail	***2012-…***	*Siber savunma için gelecek yıllarda yeni teknolojilerin geliştirilmesi planlanmaktadır.*	***13 Milyon Dolar***
Çin	***-***	*PLA askeri giderlerinin belirlenmesi şeffaf olunmadığı için bilinmemektedir. 2011 giderlerine ve DoD tahminlerine göre askeri ilişkili harcama 120-180 milyar dolar arasıdır. Çin'in siber güvenlik pazarı gelecek yıllarda inanılmaz derecede artacaktır.*	***?***
İran	***2012***	*Tahran, siber savaş yeteneklerinin geliştirilmesi yönünde istekli davranmaktadır ve yeni teknolojilerle birlikte uzmanların yetiştirilmesi hedeflenmiştir.*	***1 Milyar Dolar***

Kaynak: Paganini, 2012b

NATO gibi örgütlerin siber politikaları, gelişmekte olan ülkeler adına oluşturulacak siber ittifaklara iyi bir örnektir. Siber saldırı yeteneklerine yönelik NATO'nun 2014 yılı Galler Zirvesi'nde kendi ağlarını koruma yönündeki belirgin vurgusu, savunma ve saldırı arasında oluşturulacak kurguda önemli bir noktaya işaret etmektedir. Uluslararası alanda savunma konsepti açısından en gerçekçi adımları atan NATO, özellikle bünyesindeki üye ülkeler açısından güven artırıcı bir profil çizmektedir. Teorik ve pratik alandaki çalışmaları birleştirerek kendi bünyesinde siber güvenlik alanında ciddi bir temel oluşturmuştur. Diğer bir öncelik olarak, üyelerin tek tek kendi saldırı-savunma yeteneklerinin ve kapasitelerinin

oluşturulmasına yardımcı olunması ve adeta bir danışmanlık şirketi gibi hareket etmesi siber ortamın ana akım olarak devamlılığının olacağına işaret etmektedir.[137]

Uluslararası aktörler arasında yer alan NATO, siber alana ilişkin konuları kamuya açık şekilde sürdürmektedir. BM, özel bir *Hükümet Uzmanları Grubu* vasıtasıyla devletlerin siber uzayda davranış normlarına ilişkin ilkeler üzerinde görüşmeler yapmaktadır. Rusya ve Çin tarafından desteklenen ve uzun zamandır beklemede kalan bu girişim siber uzayın kullanım şeklini düzenleyecek uluslararası bir anlaşmanın yapılması konusunu da tekrar canlandırmıştır. Böyle bir anlaşma otoriter rejimlere, internetteki eleştiri içerikli girişlere müdahale etmeleri ve sansür uygulamaları için daha geniş bir faaliyet alanı sunabilir.

AGİT siber alana ilişkin yeteneklerin farklılaşmasında, güven tesisi ile ilgili ikinci güven arttırıcı önlemler dizisini benimsemiştir. Bu önlemler bir dizi ortak adımlar atmayı kabul eden devletler arasındaki ilişkilerde, şeffaflığı arttırmayı hedeflemektedir. Bu konudaki samimiyet gelecek vizyonu açısından önemlidir.

AB, 28 üye ülke ve özel sektördeki siber güvenlik standartlarını yükseltmek için geniş bir yelpazede çaba gösteren önemli aktörlerden birisi haline gelmiştir. Faaliyetleri arasında sivil siber güvenlik için kapasite oluşturmak, eğitime destek vermek, siber suçlarla başa çıkabilmek için yürütülen yasal uygulamalar ve politika belirleme çalışmaları (bağlayıcı niteliği olan yasal araç vasıtaları da dahil olmak üzere) arasında iş birliğini artırmak da bulunmaktadır.

3.3.4.1.1. Siber Saldırılarda Karşılıklılık

Sanayi yönünden gelişmiş birçok ülke, güvenlik altyapılarına yapılan yıkıcı siber saldırılardan zarar görmeye devam etmektedir. Çoğu ülke siber saldırıların olası yıkıcı stratejik sonuçlarından çekindiğinden, taarruz içeren önleyici tedbirler konusunu gündeme getirmekten kaçınmaktadır. Siber ittifakların oluşması da bu yönden kısmi olarak zorlaşmaktadır.

---

[137] "*Siber Savunmaya İlişkin Teknik Anlaşma"*, 10 Şubat 2016'da AB'nin *Bilgisayar (Olaylarına) Acil Müdahale Timi (CERT-EU)* Başkanı Freddy Dezeure ve *NATO Siber Olaylara Mukabele Yeteneği (NCIRC)* Başkanı Ian West tarafından imzalanmıştır.

2011 yılında ABD, biri Libya'ya karşı *"Birleştirilmiş Koruyucu (Unified Protector)" Harekatı* esnasında, diğeri de Usame Bin Ladin'e karşı yapılan harekatı desteklemek amacıyla olmak üzere, iki defa yabancı hedeflere karşı siber saldırı yapmaktan vazgeçmiştir. Bu kararlar, ABD'nin yapacağı siber saldırıların Rusya ve Çin tarafından siber saldırıları başlatmak için emsal gösterileceğinden çekinilmesi sebebiyle alınmıştır (Çifçi, 2012: 321).

Siber saldırılarda karşılıklılık ve muhabere stratejisi açısından devletlerin tehdit algılamaları ve bunun siber tehdit algısındaki boyutu doğru şekilde karşılaştırılmalıdır. Örneğin; oluşacak ad-hoc yapıdaki mikro siber ittifaklarda tehdit algılamaları birçok gelişmiş ülkeye göre daha yerel düzeyde kalacağı için birliktelik oluşturmak daha kolay ve makul olacaktır. Tablo 19'da 2016 yılına ait ABD'nin tehdit algılamalarında farklı devletlerin ve olguların durumuna ilişkin bir derecelendirme yapılmıştır. Buna göre siber tehditlere ilişkin karşılıklılık ele alınırken aynı zamanda genele ilişkin algı da süreci etkileyecektir ve ülkeler arasında kırılganlık oluşturacaktır.

Tablo 19: 2016 Yılı ABD'nin Tehdit Algılaması

	Çok Yüksek	***Yüksek***	***Artıyor***	***Korunuyor***	***Düşük***
Rusya	-	*X*	-	-	-
İran	-	-	*X*	-	-
Orta Doğu/ Terörizm	-	-	*X*	-	-
Afganistan-Pakistan/ Terörizm	-	*X*	-	-	-
Çin	-	*X*	-	-	-
Kuzey Kore	*X*	-	-	-	-

Kaynak: Heritage Foundation, Index of US Military Strength, 2016

Siber saldırılarda, bir saldırının kendisinden sonraki saldırıların etkisini azaltmayacağını garanti etmek de mümkün değildir. Her saldırı sonrası kapatılan zafiyetler, bir sonraki saldırıyı zorlaştırmaktadır. Uygun hedefler baz alınıp saldırılar gerçekleşse dahi, devam eden süreçte saldırıya uğrayan zafiyetlerini gidermiş olarak faaliyetlerine devam edebilir (Kesler, 2011: 15).

Ad-hoc siber ittifaklarda karşılıklılık esası saldırıların ya da çıkarların buluştuğu noktada şiddet açısından farklılık göstermektedir. Türkiye ve yakın çevresinde siber güvenlik konusunda gelişmekte ya da gelişme arzusu içinde olan ülkelerde saldırı esasına göre tehdit algısı göz ardı edilebilir fakat karşılığında daha zor bir durumla yüzleşilebilir.

3.3.4.2. Siber Diplomasi Kanatları

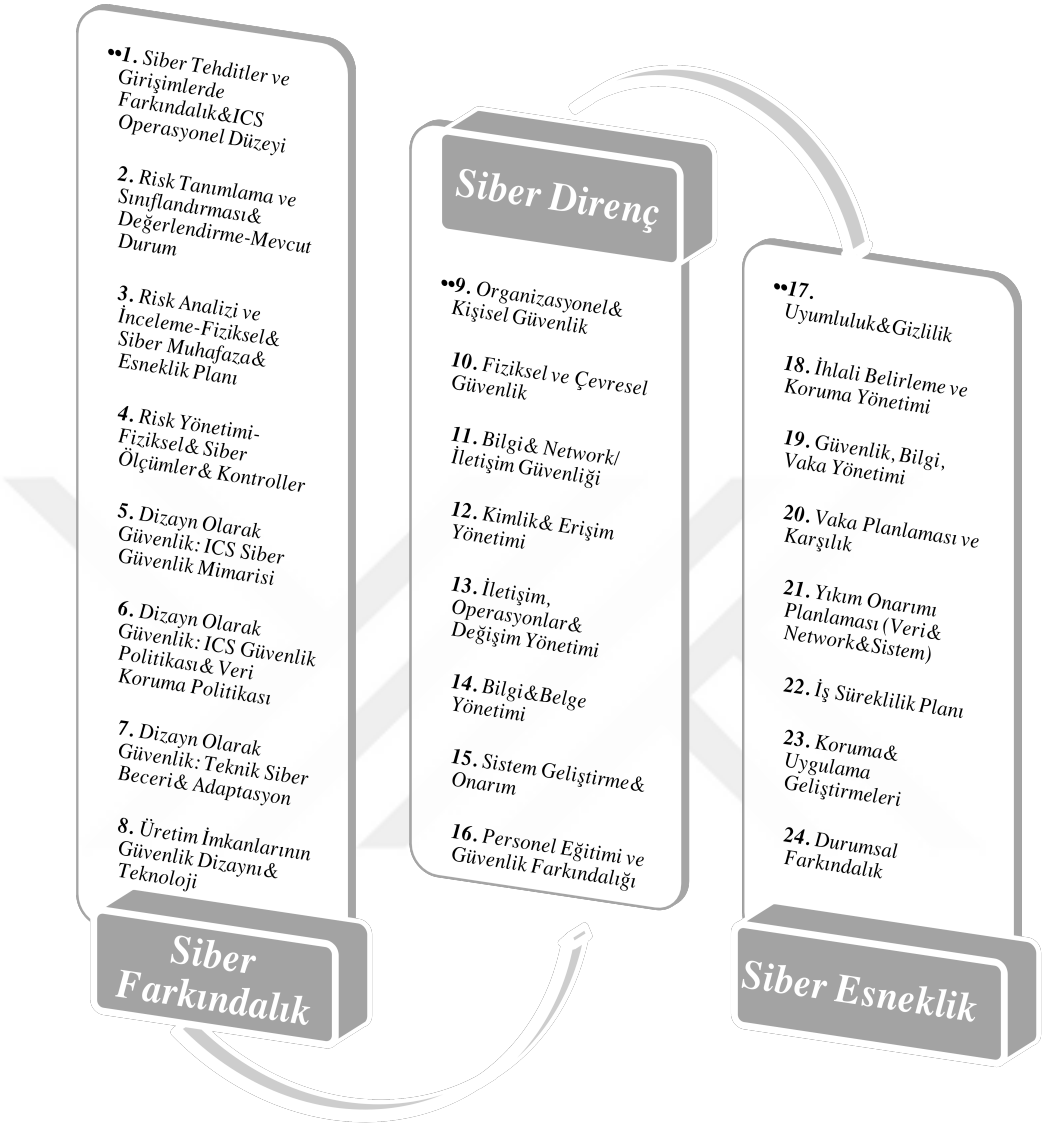
Diplomasi, devletler arasındaki ilişkilerde kullanılan, uluslararası düzenin oluşumuna ve istikrarına katkı sağlayan en eski yatay nitelikli kurumlardan biridir. En bilinen tanımıyla diplomasi, devletler arasındaki ilişkilerin barışçıl yollarla ve resmi temsilciler aracılığıyla yürütülmesidir. Diplomasinin tanımında devletler arasındaki ilişkiler, barışçıl yollar ve resmi temsilciler belirleyici unsurlardır (Ateş, 2013: 387).

Mikro siber ittifaklar için siber diplomasi kanatları önemli ve belirleyici bir kurum olarak karşımıza çıkmaktadır ve diplomasinin tanımında yer alan belirleyici unsurlardan, özellikle devletler arası ilişkilerde çıkarların kimi zaman müzakere edilmesinde kanat rolünü üstlenecektir. Türkiye gibi gelişmekte olan ülkeler adına siber diplomasi masalarının oluşturulması belli uzmanlıklarla birlikte varılacak hedefin, belirlenecek olası saldırının zamanını ve yerini belirleme misyonuna sahip olacaktır.

Siber diplomasi kanatları iki yönlü işletilmelidir. Bunlardan ilki ülke içerisinde kurulacak siber diplomasi masaları, diğeri ise kurulacak ittifaklarda sürecin müzakerelerini yürütecek kanatlardır. Hatta diplomatik misyonlara konuyla ilgili karşı ülkede faaliyetleri yürütecek ve müzakere edebilecek uzmanların yerleştirilmesi söz konusu olabilecektir.

Siber diplomasinin pratiğe geçmesinde Şekil 37, örnek bir siber yönetim modeli olarak ve basamaklandırılarak oluşturulmuştur. Diplomatik adımların sağlam bir zemine oturtulmasında ilk aşama olarak siber farkındalık önemli bir yere sahiptir. Risklerin belirlenmesi ve alandaki uzmanlaşma, bu aşamanın temel gerekliliklerindendir. Siber direnç ve siber esneklik verilerin yönetilmesi ve yönlendirilmesi, kullanılması aşamasında benzer modellerin önemli aşamalarını oluşturmaktadır. Bu aşamaların analizinde diplomatik misyonların veri alışverişi bir birikim sağlarken, oluşturulan diplomasi kanatları tek, güvenilir kaynaklar olacaktır ve iş birliği açısından gerekli samimiyeti sağlayacaktır.

Şekil 37: Endüstriyel Kontrol Sistemleri – Siber Yönetim Modeli



Kaynak: Industrial Control Systems – Cyber Governance Guide, 2016: 8

Oluşacak ittifaklarda ve ortak alınacak kararlarda ülkeler birbirlerine karşı tavır alıp ilişkileri koparsalar bile diplomatik bağ devam edecektir. İletişim özellikle siber alanda gerekli olduğu için ilişkiler hiçbir zaman tamamen koparılmayacaktır ve bu konudaki güven teatisi devam ettirilecektir. Siber ittifaklarda devletlerin birbirlerine olan zaafları çıkarların savunulmasını ortak bir düzende devamlı kılabilecektir. Diplomatların, askerler gibi aynı dış politikanın parçası olduğu uluslararası ortamda organik bir bağ her zaman vardır. Bu bakımdan siber alanda eğer ordular kurulup askeri harekatlar planlanıyorsa, bu alana ilişkin

farklı teorik yaklaşımlarla diplomasi çeşitlendirilmelidir. Siber diplomasi masalarının kurulması bu noktada önemli bir basamaktır.

Siber diplomasi masaları adına ele alınması gereken bir diğer husus diplomaside *ikinci yol (track two diplomacy)* olarak adlandırılan ilişkidir. Ülkeler adına, hükümetleri kapsamayan gayri resmi türden ilişkiler *mikro siber ittifak teorisi* içinde önemli bir ayaktır. Ülkelerin devlet aygıtı içerisinde yer almayan, özel kişi ya da gruplar bu sürecin aktörlerini oluşturmaktadır. Amaç olarak taraflar arasındaki iletişim düzeyi geliştirilmek ve mevcut olan çatışmalar yumuşatılmak istenmektedir. Her ne kadar yakın devletler arasında oluşturulacak ittifaklar iş birliğini gözetse de oluşabilecek sorunlara ilişkin hızlı adımların atılması ad-hoc ittifakların işlerliği açısından önemlidir.

ABD gibi ülkelerin siber güvenlik alanında oluşturduğu *"Siberalan Koordinatörlüğü"* gibi birimlerde yürütülen siber diplomaside özellikle Rusya, Çin ve Avrupa özelinde yürütülen faaliyetler dikkat çekicidir. *Christopher Painter'*ın[138] başına getirildiği koordinatörlük İngiltere, Almanya gibi ülkelerde benzer yapılanmaların oluşturulmasında model görevi üstlenmiştir. Türkiye gibi ülkelerde siber alandaki diplomatik ilişkileri, siberalan koordinatörlüğü seviyesinde yürütecek ve bu alanda olası uluslararası krize karşılık verebilecek bir yapılanmanın olmadığı görülmektedir.

3.3.4.2.1. Zorlayıcı Diplomasiye Dönüşen Siber Diplomasi

Bilimsel çalışmalara konu olan *"Siber politikalar (Cyberpolitics)"* kavramı siber alana ilişkin gündemin nasıl ve neden ortaya çıktığı ile ilgilidir ve eğer diplomatik bir kart olacaksa, *zorlayıcı diplomasi*[139] içerisinde yer alabilecek bir unsur olarak düşünülebileceği ile ilintilidir. Zorlayıcı diplomasinin askeri olmaktan çok diplomatik bir girişim olarak düşünülmesi, siber politikalar açısından belirleyici olabilir ve teorik alanın ötesine geçmeyi bilimsel çalışmalar açısından geçerli kılabilir.

---

[138] *Christopher Painter*, 2011 yılında Obama'nın Dışişleri Bakanlığı bünyesinde yapılandırdığı yeni bir bölüm olan *"Siberalan Koordinatörlüğü"*nün başına getirilmiştir. 2002 yılından beri ABD'yi siber güvenlikle ilgili çeşitli platformlarda temsil etmektedir.

[139] *"Zorlayıcı diplomasi"* en genel hatlarıyla kuvvet kullanma tehdidinden yararlanarak karşı tarafın gerçekleştirmiş olduğu fiili bir ihlali ya da zorlamayı durdurması veya geri adım atması yönündeki girişimleri ifade eder.

Siber saldırıların veya taktiklerin zorlayıcı diplomasi aracı olarak ele alınması *caydırıcılık kabiliyeti*[140] ve bu kavramın politik olarak hangi devlete ne ifade ettiğiyle alakalıdır. Özünde konvansiyonel nitelik taşımayan ve askeri olmayan bir strateji olarak gelişim gösteren siber saldırılar artık devletlerin savunma ve saldırı stratejilerinde yer alan ve askeri kurumların içerisinde örgütlenmelere giden bir niteliğe bürünmüştür. Diplomatik bir kart olarak karşımıza çıkışı bu türden gelişmelerle birlikte gündeme gelmiştir.

Tablo 20'de, savunmaya dayalı zorlayıcı diplomasi çeşitleri, rakibin reaksiyonlarına göre ele alınmıştır. Caydırma konseptiyle birlikte zorlayıcı diplomasi aracı olarak ele alınabilecek siber saldırı kapasitesi, bu kavram içerisinde rakibin amacını gerçekleştirmeden önce durmaya ikna etme konusunda nasıl bir etkiye sahip olabilecektir? Böyle bir kart devletlerin elinde bir seçenek olarak yer alabilecek midir? Siber güvenlik dediğimiz unsurun siber politikalar olarak çalışılmasının ve tartışılmasının sebebi de özünde bu soruların cevaplarının olgunlaştırılmasıyla ilgilidir.

Tabo 20: Savunmaya Dayalı Zorlayıcı Diplomasi Çeşitleri

Caydırma	***Zorlayıcı Diplomasi***		
	I	***II***	***II***
Rakibi henüz başlatmadığı bir eyleme girişmemeye ikna etmek	*Rakibi amacını gerçekleştirmeden önce durmaya ikna etmek*	*Rakibi henüz başlamış olduğu bir eylemden geri adım atmaya ikna etmek*	*Rakibi hükümetinde veya rejiminde değişiklik yapmaya ikna etmek*

Kaynak: Aksu, 2008: 28

Siber saldırılar ve oluşan siber caydırıcılığın teori ve pratikte birbiriyle uyuşmazlık içinde olduğunu ayrıca vurgulamakta fayda vardır. Bunun en önemli sebebi özellikle multidisipliner bir özellik gösteren uluslararası ilişkiler içerisine, çatışma boyutuna dahil

[140] Caydırıcı olma durumunun karşı tarafın eylemini ilk aşamada önlemeyi amaçladığını unutmamamız gerekmektedir. Örneğin; Rusya'nın çevre ülkelerden birine karşı siber bir müdahelede bulunma seçeneğine karşı, ya da ABD'nin yine ilgi alanı olan bir bölgeye karşı uygulayacağı siber saldırıya karşı, rakip tarafın bunu önlemeye ilişkin kapasitesi büyük olasılıkla kayıp verdikten sonra ortaya çıkacaktır. Bu durum maruz kalınan zararın en aza indirilmesi ile ilgili olacaktır.

oluşundan kaynaklanmaktadır. Zorlayıcı diplomasi unsuru olarak ele alınırken de daha geniş bir analize ve çalışma sürecine ihtiyaç duymasının ana sebebi budur (Schmitt, 2010: 153).

Siber saldırıların salt askeri bir boyutu yoktur. Diplomatik olarak hangi boyuttan ele alırsak alalım teori sorunsalı uzun vadede uluslararası ilişkiler disiplini içerisinde farklı şekillerde kendini gösterecektir. Günümüzdeki tartışmaların ve çalışmaların içerisindeki komplo teorileri veya olabilirlik yönündeki tahminler, analizler bunun en önemli ispatıdır. Zorlayıcı stratejilerin oluşturulmasında, siber güvenliğe ilişkin analizlerin gelişmekte olan ülkelerde pratiğe dönüşememesinin en önemli sebebi budur. Değişkenler hakkında karar vermek somut verileri gerektirmektedir ve zorlayıcı strateji oluşturma aşamasında ilk basamaktır.

Şekil 38: Zorlayıcı Strateji Oluşturma

Kaynak: Aksu, 2008: 38

Zorlayıcı diplomasi, olayların özgünlüğüne göre değişiklikler göstermektedir. Zorlayıcı diplomasi stratejisini uygulayacak olan devletin karar vericileri öncelikle kriz sırasında gerekli sorunlara en rasyonel cevabı da vermek zorundadır. Siber diplomasinin zorlayıcı diplomasiye dönüşmesi gelecekte oluşacak kriz anlarına ilişkindir ve siber alandaki faaliyetler arttıkça bu alandaki dönüşüm pratikte daha çok hissedilecektir.

3.3.4.2.2. Önleyici Diplomasiye Dönüşen Siber Diplomasi

Önleyici diplomasi kavramı, bir devlet içinde ya da iki devlet arasındaki politik uzlaşmazlıkların silahlı çatışmaya tırmanmasını önlemeyi amaçlayan kurumları ve alınacak tedbirleri kapsamaktadır. BM eski Genel Sekreteri Boutros-Ghali önleyici diplomasiyi şöyle tanımlamıştır: *"Taraflar arasında anlaşmazlıkların çıkmasını önlemek, taraflar arasındaki mevcut uyuşmazlıkların çatışmaya tırmanmasını önlemek ve çıkmış olan çatışmaların*

yayılmasını önlemek için kullanılan mekanizmalardır" (Özçelik, 2012: 430). Önleyici diplomasinin siber güvenliğe ilişkin kavramsal boyutu, küresel alana ilişkindir ve daha kapsayıcıdır.

Çatışmayı önleme kavramı, çatışmanın ortaya çıkmasından sonraki döneme tekabül etmektedir ve çatışmanın henüz kanlı bir hal almadığı durumu ifade etmektedir. Devam etmekte olan bir çatışmanın yayılmasını önlemek, *müdahaledir*.[141] Boyutsal olarak müdahale, başka bir ülkenin iç işlerine karışmak gibi yasal olmayan bir davranışa düşmemek için, *karmaşık ve insani bir olağanüstü durum (complex humanitarian emergency)* olarak algılanmaktadır. Bu aşamada çatışma, ortaya çıkan siyasi boşluktan dolayı tehlikeli bir düzeye erişmektedir (Hettne, 2012: 361). Siber alana ilişkin çatışma boyutunda benzer bir ilişkiden söz edilebilir. Siber diplomasinin önleyici boyutu oluşabilecek müdahele sonrasında fiziksel zararların varlığıyla açıklanabilir.

Uluslararası alanda aktörlerin birbilerine karşı tutumları, siber saldırıların niteliği ve kapsamı ile ilgilidir. Devletler bu konuda *kuvvet kullanma hakkına (jus ad bellum)* sahip olacaksa benzer uygulamalar siber diplomasiyi, önleyici diplomasiye dönüştürecektir ve siber ittifaklar bu konuda ciddi zararlar görebilecektir. Devletler arasında bir uzlaşmazlık aracı haline gelen siber saldırılar ve kapsamı çatışma ortamını tetikler ise önleyici diplomasi, zorlayıcı diplomasinin önüne geçecektir.[142]

Siber diplomasi eğer bir caydırıcılık kapasitesine sahipse, önleyici diplomasinin yerine geçebilir ve kendi içerisinde bir aracı haline dönüşebilir. Önleyici diplomasinin karakteristik özelliği çatışmaya erken müdahele etmesi sebebi ile en az karmaşık, en insancıl yöntemlerden biri olarak uluslararası çatışmaların çözümünde bir yoldur ve siber saldırılar, kritik altyapılar gibi fiziksel noktalara yönelmeden bir diplomatik araca dönüşecekse, önleyici diplomasi içerisinde yoğrulabilir.

---

[141] Uluslararası politika alanında müdahele, uluslararası bir aktörün bir diğerini etkileme sürecinde, belirli bir süre için, mevcut alışılagelmiş biçimlerden belirgin bir şekilde ayrılan, farklı bir tutuma yönelmesi ve esas olarak hedefin siyasal otorite yapısını değiştirmeyi veya korumayı amaçlayan bir nitelik taşımaktadır (Yılmaz, 2012)

[142] Tam anlamıyla önleyici ilk müdahele, AB tarafından 2003 yılında, Makedonya'da gerçekleştirilmiştir. Bu örnekte hiçbir aktif-önleme tedbiri alınmamıştır. Bu durum, o dönemde tek bir çatışma çözüm yöntemine olan aşırı eğilimi göstermektedir (Hettne, 2012: 361).

Zorlayıcı diplomasi, ciddi uzlaşmazlıkların barışçıl çözümü için uygulanan bir savunma stratejisidir ve temel olarak güç kullanmaya dayanmaktadır. En son çare olarak kullanılsa da siber diplomasinin dönüşüm olarak, bazı unsurlarla aracı haline gelebileceği zorlayıcı diplomasi, askeri ve ekonomik tehditler ile yaptırımlarla siber diplomasiden faydalanabilir. Önleyici diplomaside hedeflenilen unsurlara ve olayın kapsamına göre siber diplomasi bir araç haline gelebilir. Gelecekteki olaylar zorlayıcı ve önleyici diplomasi açısından siber diplomasinin dönüştüğü noktada doğru kurgulanırsa daha net sonuçlar alınır.

3.3.4.3. Operasyonel Unsurlar Oluşturma

"Operasyonel unsurlar" teknik konularda oluşturulacak birimlerle politikaların belirginleşmesinde ve alınacak kararlarda uygulamalara dönük uzantıları tanımlamak için kullanılmaktadır. Ad-hoc siber ittifakların temelinde operasyonel unsurların oluşturulması, tartışılması, tatbikatların yapılması gelmektedir.

Ülkeler hem kendi içerisinde yaptıkları düzenlemelerle, hem de uluslararası alana yaydıkları yaklaşımla operasyonel unsurlarını kimi zaman görünür, kimi zaman da gizli bir şekilde siber güvenlik alanında uygulamaktadır. Ad-hoc siber ittifaklarda operasyonel unsurlar dahilinde, amaçlanan hedefe göre ortak çalışmalar yapılabilir ve hedefler ulusal çıkarlara dönüştürülebilir. Doğru anlaşılması gereken nokta operasyonel unsurların sadece savunma amaçlı uygulanmasının yanı sıra saldırı temelinde faaliyetler yürütebilmesi ve bunu gerektiğinde şeffaf bir şekilde tartışılabilmesidir.

Ülkeler farklı alanlarda, farklı önceliklere göre operasyonel unsurlar oluşturmaktadır. Savunma ve saldırı disiplinine yönelik bu unsurlarda askeri yapılanmalar oldukça popüler hale gelirken ulusal anlamda gerek suçların ve suçluların takibinde gerekse dahili kaynaklara saldırılarda savunmaya yönelik tedbirler dikkat çekicidir. CERT yapılanmalarında siber alana ilişkin oluşturulan siber güvenlik stratejileri belirleyici olmaktadır ve kısa-uzun vadeli politikaları şekillendirmektedir. Tablo 21, ülkelerin operasyonel siber müdahele unsurlarını göstermektedir. Ülkelerin siber güvenlik stratejileri, bu unsurların oluşturulmasında temel çıkış noktasıdır ve CERT'lerin oluşturulması ile askeri alandaki gelişim stratejik algıya göre değişmektedir. Müdahele unsurlarının yapılanması paralelinde oluşturulacak kurumsal yapılarla birlikte siber ittifaklar daha da işlerlik kazanacaktır.

Tablo 21: Ülkelerin Operasyonel Siber Müdahele Unsurları

	Siber Güvenik Stratejisi	*Ulusal CERT*	*Diğer CERT*	*Siber Tatbikat*	*Siber Komutanlık*	*Kurum*
ABD	*X*	*X*	*X*	*X*	*X*	*NSA/ USCYBERCOM*
Almanya	*X*	*X*	*X*	*X*	-	-
Avustralya	*3X*	*X*	-	*X*	-	*Cyber-Security Operations Centre*
Brezilya	*X*	-	*X*	-	*X*	*Information Security Department*
Çin	*X*	*X*	*X*	*X*	*	*
Estonya	*X*	*X*	*X*	*X*	-	*CCDCOE (NATO)*
Finlandiya	-	*X*	-	*X*	-	-
Fransa	*X*	*X*	*X*	*X*	-	-
Hindistan	*Taslak*	*X*	*X*	*X*	*X*	*Cyber Command and Control Authority*
İngiltere	*X*	*X*	*X*	*X*	-	*Cyber-Security Operations Centre*
İsrail	*X*	*X*	*X*	-	*X*	*
Japonya	*X*	*X*	*X*	*X*	-	*National Information Security Centre*
Kanada	*X*	*X*	*X*	-	-	-
Rusya	*X*	*X*	*X*	-	*	-

Kaynak: Bakır, 2013

Tablo 21'de görüldüğü üzere ülkelerin konseptleri ve operasyonel unsurlarının kullanımı coğrafyaya, gelişmişliğe ve bu alana duyulan ilgiye göre şekillenmemiştir. Temel olarak tartışılması ve ele alınması gereken nokta bu unsurlara nasıl ve ne derece ihtiyaç duyulduğudur. Özellikle Türkiye gibi ülkeler açısından ad-hoc siber ittifakların oluşturulmasında siber güvenlik stratejisi ve kurumsal nitelikler gelişime ihtiyaç duymaktadır. Gelişimdeki zorluk, operasyonel özelliklerin iç ve dış politikanın gereklilikleri açısından tam olarak oturtulamamış olmasıdır.

Operasyonel unsurların nasıl ve ne şekilde, özellikle çerçevesi oturtulmaya çalışılan Micro-CAT içinde hangi yönde gidişat sergilediğini görmek için siber güvenlik tatbikatları olmazsa olmazlardandır. Tablo 22'de görüldüğü üzere katılımcılarının devletler olduğu tatbikatlarda, hedefler belirlendiği zaman oluşacak ad-hoc siber ittifakların operasyonel unsurlarının kapasiteleri test edilebilir ve sınıflandırılabilir.

Tablo 22: Siber Güvenlik Tatbikat Türleri

Sıra No.	***Tatbikat Türü***	***Tatbikat Alt Türü***
1.	*Konularına Göre*	*Alt Konu, Asıl Konu*
2.	*İcra Ediliş Şekillerine Göre*	*Yazı Tabanlı, Gerçek Saldırı*
3.	*Yapıldıkları Yere Göre*	*Merkezi Yapı, Dağıtık Yapı*
4.	*Katılımcılarına Göre*	*Kurum İçi, Kurumlar arası, Ülkeler arası*

Kaynak: Çifçi, 2012: 336.

Ad-hoc siber ittifaklarda olacağı gibi ülkeler arası tatbikatlarda, birden çok ülke bir araya gelerek tatbikat merkezi kurmaktadırlar ve katılımcı ülkeler kendi bölgelerinden yakın devletlerle merkeze gelmeden tatbikatı yürüterek operasyonel unsurlar oluşturabilir. Ülkelerin farklı zaman dilimlerinde bulunması, tatbikatın yoğun bir koordinasyon gerektirmesi, saldırı senaryolarında mutabakat sağlanması ve uygun iletişim altyapısının tesis edilmesi, bu tür tatbikatlarda karşılaşılan başlıca zorluklardır (Çifçi, 2012: 338).[143]

3.3.4.4. Hedef Belirleyebilme

Ad-hoc siber ittifaklarda operasyonel unsurların oluşturulması büyük önem taşırken bu unsurların hedeflediği amaçlar ve bu hedeflerin sonuçları ittifakın işlerliği bakımından önem kazanır. Siber alanda özel amaçlarla ve belli konular dahilinde, çıkarsal birlikteliklerle

[143] Siber güvenlik tatbikatı tasarımı, bu faaliyete katılacak olan tarafların planlama işini çok dikkatli bir şekilde yerine getirmelerini gerektirir. Herhangi bir siber güvenlik tatbikatı birçok farklı şekilde yapılabilse de bunların bazı temel ortak özellikleri bulunmaktadır. Tatbikatların amaçlarının tek tek belirlenmesi siber güvenlik tatbikatlarını tasarlamadaki ilk adımdır. Operasyonel unsurların savunma mı yoksa saldırı amaçlı mı olacağının doğru analiz edilmesi gerekir.

hareket kabiliyetine sahip ad-hoc siber ittifaklar hedefleri belirlenmiş olarak hareket edebilmelidir. Özellikle siber ittifaklarda belirlenebilen hedef sonrasında oluşabilecek saldırıda muhtemel etkilenenlerin de düşünülmesi gerekmektedir. İnsanların işlerinin ve hayatlarının kaybedildiği, birey güvenliğinin gözardı edildiği ve potansiyel saldırıların yapıldığı kritik altyapılara ilişkin müdahelelerde, uluslararası alanda yaptırım anlamında sorunlar doğabilecektir.

Ulusal alanda oluşturulan eylem planlarına benzer şekilde ad-hoc siber ittifaklarda da karşılıklı olarak eylem planları belirlenebilir. Eylem planında kurumların sorumluluklarının belirtilmesi önemli olmakla beraber kurumlar arasında tam bir iş birliğinin temel alınıyor olması planın gerçekleştirilebilirliğini artırmaktadır. Sistemin tam güvenliğinin sağlanması, sistem içindeki mekanizmaların ve alt sistemlerin her birinin güvenliğinin sağlanmasına bağlıdır. Bunun yanı sıra iş birliği, genel bilgi birikiminin ve kalitenin de artmasını sağlayacaktır (Yılmaz ve Sağıroğlu, 2013b: 330).

Hedeflerin belirlenmesinde siber saldırıların yoğunlaştığı bölgeler ve ülkeler de doğru analiz edilmelidir. Oluşan ittfaklarda özellikle bu konuda yoğunlaşılan yerler saldırı açısından daha tercih edilesi bölgelerdir ve rakibin belirlendiği noktaya göre değişkenlik göstermektedir (Sabillon ve diğerleri, 2016: 67). Oluşan bölgesel siber ittfaklarda saldırıların derecesinin yoğunlaştığı yerler çıkarsal olarak bir bütünlük oluşturabilir fakat bu yaklaşım ciddi derecede bir yoğunlaşma gerektirmektedir.

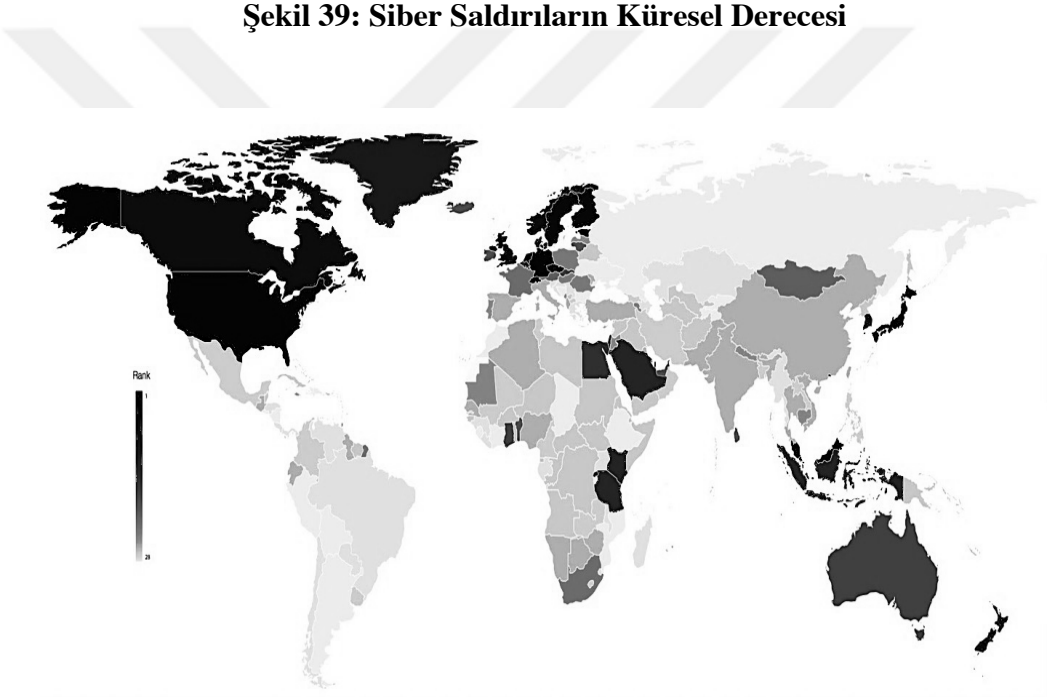
Hedef belirlemede, genel tehdit algılaması yönüne bakacak olursak *"Advanced Persistent Threats (APT)"*[144] yani, *"hedef odaklı saldırı"* ya da *"gelişmiş sürekli tehdit"* anlamlarıyla karşımıza çıkan saldırılarda hedef genellikle kamu kurumları, kritik altyapılar ve büyük şirketler olmaktadır. APT'ler genellikle ülkeler arasında gerçekleşmekte ve bilgi sızdırmak veya büyük ölçekli hasarlara sebep olmak amacıyla kullanılmaktadır. Bu saldırılarda hedef mümkün olduğu kadar çok geniş spektrumda etki yaratmak olduğundan, hangi kritik sistemin tercih edileceği ülkeden ülkeye değişmektedir. Bu saldırıların tek

[144] İngilizce karşılıktaki *"Advanced"*, saldırganın ileri seviye bilgisini ve kendi tekniklerini geliştirebileceğini; *"Persistent"*, saldırganın görevini yerine getirme niyetini; *"Threat"* ise saldırganın organize olduğunu, finansal olarak desteklendiğini ve motive edildiğini ifade etmektedir (Binde ve diğerleri, 2016).

sebebi aynı zamanda hayatı felç etmek değildir (STM, Türkiye Siber Tehdit Durum Raporu, 2016).

Şekil 39, dünyada siber saldırıların derecelendirilmesi açısından ülkelerin gelişmişliklerinin açık kapı bıraktığını ve siber ittifakların geçici olarak amaçlandırılmasında bir kıstas olduğunu gözler önüne sermektedir. Gelişmiş ülkelerin yumuşak karnı halina gelen siber alan bu konuda rakiplerin yeni ilgi alanıdır. ABD ve çevresi, Avrupa kıtası, Güney Asya, enerji nakil hatlarının siber alana verisel olarak bağlandığı Orta Doğu ülkeleri hedef durumundadırlar ve saldırıların ilgisi bu bölgelere kaymaktadır.

Şekil 39: Siber Saldırıların Küresel Derecesi



Kaynak: World Economic Forum, 2016: 77

Tablo 23'te APT'lerin yaşam döngüsü yer almaktadır. Farklı aşamaların yer aldığı fazlarda APT'nin döngüsü, sürecin tüm aktivitelerinin başarıya ulaşmasıyla ilerler. Öncelikli olarak hedefin belirlenmesi ve farklı şekillerdeki teknikler doğru analiz edilmelidir. Teknik detay gerektiren süreçlerin başarı şansı yüksektir fakat zaman ve başarı açısından genellikle daha kolay ve zahmetsiz yollara başvurulmaktadır. Hedeflenen süreçte verilerin elde edilmesi ve daha sonrasında iz bırakmadan APT'nin sistemden ayrılması beklenilen hususdur.

Tablo 23: APT Yaşam Döngüsü

	Aktivite	*Detaylar*
1. Faz	*Keşif, hedef belirleme*	*Hedefin ve hedefe ulaşabilecek yolların tespit edilmesi*
2. Faz	*Oltalama e-postasının gönderilmesi*	*Genellikle bu yöntem tercih edilmektedir (Daha az teknik detay gerektirir)*
3. Faz	*Hedefle irtibata geçme*	*Hedef sisteme arka kapı yükleme*
4. Faz	*Hak yükseltme, hedef alanını genişletme*	*Hedef sistemde daha yüksek yetkili kullanıcı haklarına geçiş, farklı ağları keşif*
5. Faz	*Veri kaçırma*	*Hedef sistemden ilgili verilerin şifrelenerek dışarı çıkartılması, yedeklenmesi*
6. Faz	*Erişimi kalıcı kılma*	*İstenildiğinde tekrar bağlanılabilecek bir yapıyı kurup, logların ve diğer delillerin silinmesi*

Kaynak: STM, Türkiye Siber Tehdit Durum Raporu, 2016

Ülkelerin kendi ulusal projelerinin, kritik görüşmelerinin ve istihbarat çalışmalarının ele geçirilmesi de APT'lerin hedefleri dahilindedir. Hedef belirlerken bu tür oluşumlarda sadece veri çalmak gibi amaçtan öte, stratejik öneme sahip bilgilere ulaşılması hedeflenmektedir. İran'ın nükleer programını hedef almış Stuxnet, hemen arkasından benzer kodlarla geliştirildiği düşünülen "Duqu" ve "Flame" APT saldırılarının bariz örnekleridir.

3.3.4.5. Kritik Altyapıların Korunması Önceliği

Ad-hoc siber ittifaklar açısından operasyonel unsurların oluşturulması ve hedeflerin belirlenmesi aşamalarıyla birlikte savunma hattındaki en büyük zafiyet kritik altyapıların korunmasında baş gösterecektir. Yapılan saldırılar ve müdaheleler çıkar elde etme amacıyla gerçekleşeceği için misilleme, karşı tarafı caydırma adına fiziksel unsurlara yönelecektir ve gözetilecek karşı ataklarda konvansiyonel unsurlara başvurulmayacaktır.

Kritik altyapılar, muhtelif sivil ve askeri tehditlere maruz kaldığından, ulusal düzeyde korunması gereken stratejik sistemler kapsamında değerlendirildiği için oluşacak ittifaklarda ve atılacak adımlarda hassas nokta olarak yer almaktadır. Siber ittifaklar

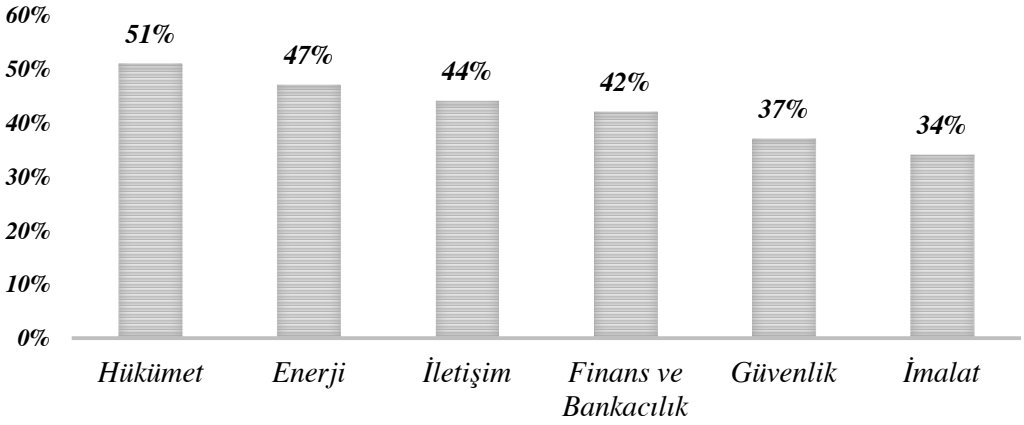
açısından, siber savunma kapsamında korunması gereken kritik altyapı ve sistemleri şu şekilde ifade edebiliriz:

- *Savunma sanayii,*
- *Tüm iletişim sistemleri,*
- *Bilgi sistemleri,*
- *Lojistik sistemler,*
- *Hava savunma ve komuta kontrol sistemleri,*
- *Kripto sistemleri,*
- *Seyrüsefer, yaklaşma, iniş, konumlama ve yön bulma sistemleri,*
- *Uydu ve yer sistemleri,*
- *Uzay sistemleri,*
- *İnsanlı ve insansız hava aracı sistemleri.*

Tüm bu sistemlerin bağlı olduğu bir uluslararası arenada siber saldırıları kullanarak devletlerin kritik altyapılarını çökertmek ve karşılıklı bağımlılık ilişkisine dayanan bir sistemin işleyişini çalışmaz hale getirmek günümüz siber savaş ortamında mümkün gözükmektedir. Operasyonel alanı hedef alan ve fiziksel dünyada çeşitli sonuçlar doğurabilecek saldırıların çoğu da IT sistemlerinin delinmesiyle başlamaktadır (Hemme, 2015: 25). Bu noktada özellikle siber ittfaklarda operasyonel teknolojiler ve bilgi teknolojileri dallarında çalışan ciddi bir uzman altyapısıyla siber güvenlik kültürü inşa etmenin gerekliliği kendini hissettirmektedir.

Grafik 23'te, organizasyon yapısına göre veri kaybına uğrayan kuruluşların ABD özelinde, 2015 yılı etkilenme oranları gösterilmektedir. Oranların temel olarak veri kaybı açısından işaret ettiği alanların başında hükümet, enerji, iletişim, finans, güvenlik ve imalat gelmektedir. Özellikle enerji ve iletişim özelinde gerek veri kaybı, gerekse veri kayıplarından oluşturulabilecek riskler, siber saldırıların kritik altyapılar üzerinde yoğunlaştığının ispatıdır. Gelişmekte olan ülkeler açısından enerji nakil hatlarının önemi düşünüldüğünde, fiziki olarak bu hatların korunması temel öncelik olarak siber ittifaklarda devletlerin önceliklerinden biri haline gelmektedir. Karşı taraf açısından amaçlanılan unsur verilerin ele geçirilmesi yanında fiziki zararlar olabilir.

Grafik 23: Organizasyon Yapısına Göre Veri Kaybına Uğrayan Kuruluşların Genel Etkilenme Oranları

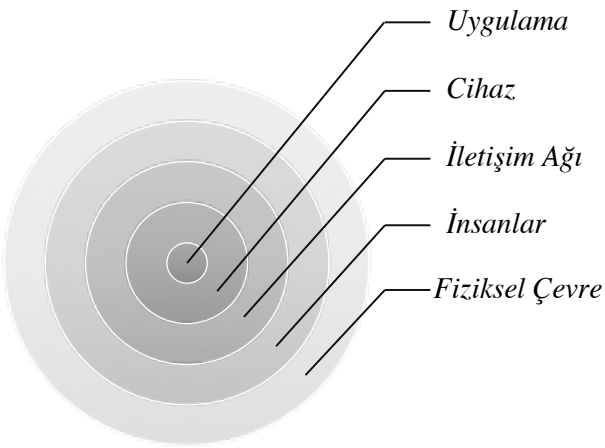


Kaynak: Report on Cybersecurity Critical Infrastructure in the Americas, 2015: 25

Enerji, telekomünikasyon, ulaşım ve su sistemleri gibi kritik altyapı sistemleri bilgi sistem otomasyonu ile idame ettirilmektedir. Bu sistemlerin bir ülke için stratejik öneme sahip olduğu düşünüldüğünde doğal hedefler haline dönüşmeleri kabul edilebilir bir durumdur. Bir ülkeye zarar vermek, kaos yaratmak ya da ekonomisini alt üst etmek için sistemlere gerçekleştirilecek bir siber saldırı yeterli olabilir (Yılmaz ve Sağıroğlu, 2013b: 324). Bu hedefler arasında basınç sistemiyle çalışan enerji nakil hatları sistemlerin besleyici birimi olarak ciddi tehlike altındadır. Genel olarak eğilim özellikle bu hatların siber alana bağlı olması yönündedir.

Başta enerji olmak üzere, nükleer alanda faaliyet gösteren tesislere etki eden ve literatüre *"Blended Attacks"* olarak geçen saldırıların fiziksel dünyada yıkıcı sonuçlar doğurabileceği, 2010 yılındaki Stuxnet olayıyla ispatlanmıştır. 2015 Aralık ayında Ukrayna'da siber silahları kullanarak ülkeyi karanlığa gömen etki bu olaylardan sadece birkaçıdır. Oluşan ittfakların amaçları geçici olsa da, birlikteliğin sürdüğü süre zarfında bu tür olaylara müdahil olunabilmesi anlık veri alışverişi bakımından ve tehdidin karşılıklı olarak tespiti açısından önemli bir yere sahiptir. Savunma kısmında kritik altyapıların kapsadığı fiziksel çevre Şekil 40'ta anlaşılacağı üzere bireylerin, iletişim ağlarının, cihazların ve uygulama alanlarının devamlılığında üst bir niteliktir.

Şekil 40: Derinliğine Savunmanın Unsurları



Kaynak: Çifçi, 2012: 194

3.3.5. Micro-CAT İle Siber Politikalarda Çıkar Elde Etme

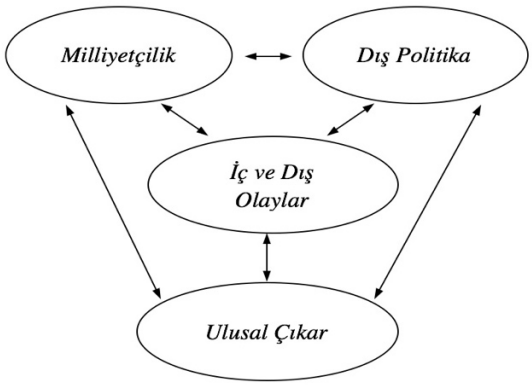
Çıkar kavramına önem kazandıran, ulusal çıkar olarak uluslararası politika alanındaki ilk genel teori oluşturma çabasının sahibi Hans Morgenthau olmuştur. Uluslararası politika alanında *gerçekçilik* olarak adlandırdığı bir genel teori kurma çabasına giriştiği çalışmalarında anahtar kavram güç ile ifade edilen çıkar olmuştur. Thomas Robinson, F.S. Norhedge, Joseph Frankel gibi düşünürler de farklı tipolojilerle ulusal çıkar kavramını geliştirerek günümüze ulaştırmışlardır (Sönmezoğlu, 2014: 349).

Özellikle son yıllarda devletlerin temel aktör olma konumuna karşı ortaya atılan gelişmelerle, ulusal çıkar kavramının klasik algılanışı ve bu alana ilişkin çalışmalar farklılaşmıştır. Soyut bir düzeyde, güç ve güvenliğin önemli ulusal çıkar unsurları olduğu hususunda anlaşan araştırmacılar bunları sağlayacak somut politikalar konusunda çok sık anlaşmazlığa da düşmektedirler (Nye ve Welch, 2009: 67).

Siber alanın uluslararası sistemde ulusal çıkarla buluştuğu noktada, olaylar döngüsü ve tanımsal özelliklerden ziyade küresel anlayıştaki farklılık ve dış politika, milliyetçilik, iç ve dış olaylarla ulusal çıkar arasındaki bağıntı kendi karakteristik özelliğini ortaya çıkarmıştır. Dış politikada siber ittifakın arayış içerisine gireceği alanlarda, yakın coğrafyalardaki kültürel özellikler devletleri birbirlerine yakınlaştıran unsurlar arasında

gözükse de, dış politikaya ilişkin temel olaylar ulusal çıkarın bu döngüde yerini almasını sağlamaktadır.

Şekil 41: İç ve Dış Olayların Çıkar İlişkilerinde Merkeziliği



Micro-CAT temel çerçevesi ile siber politikalar oluşturmak mümkündür. Temel sorunlardan bir tanesi bu teorik çerçeve ile çıkarlar sağlanıp sağlanamayacağı hususudur. Bu temelde çıkarların yakın coğrafyalardaki ülkeler adına temellendirilmesi kronik sorunlarla bağdaştırılmamalıdır.

Kimi ülkeler yakın coğrafyalarda birbirleriyle olan ilişkilerinde tarihi derinlik ve uluslararası ilişkilere dayalı sorunları günümüz ve gelecek vizyonuna dahil etmektedir. Micro-CAT ile oluşturulacak politikalarda bu türden yaklaşımların hem diplomatik ilişkilere zarar vereceği hem de ittifakı zarara uğratacağı bir gerçekliktir. Küresel sistem, politika yapıcılara sadece ulusal çıkarları tehdit eden unsurlar yanında dış politika amaçlarının belirlenmesini etkileyecek fırsatlar da sunmaktadır (Viotti ve Kauppi, 2014: 192). Savaş stratejileri eninde sonunda savaşın bitirilmesi konusuyla ilgilenmektedir, oysa siber savaşlar karşıdaki düşmanı silahsızlandırmak veya onu tamamen etkisiz hale getirerek sonlandırabilecek bir savaş çeşidi değildir.

SONUÇ VE ÖNERİLER

Siber güvenlik perspektifi ve alana ilişkin çalışmalar, uluslararası ilişkiler temelinde yeni bir boyutu ortaya çıkarmıştır. Çalışma boyunca inşacı bir yaklaşımla tartışılan boyut, farklı saldırı ve savunma teknikleriyle gelecek açısından bir vizyon oluşturmaktadır. Teorik bir zemine de oturtulmaya çalışılan siber güvenlik ve devletlerin bu yöndeki algıları politik alanda geliştirilmeye oldukça müsait gözükmektedir. Sunulan veriler de bu durumun devletlere ilişkin yönünü gözler önüne sermiştir.

Siber güvenlik çalışmalarının uluslararası güvenlik perspektifine kattıkları yanında, uygulama alanına ilişkin yaptığı katkı önemli gözükmektedir. Uluslararası ilişkiler ve güvenlik ile ilgili temel yaklaşımlarda, Soğuk Savaş'ın bitimiyle birlikte, büyük güçlerin çatışma alanlarının azalacağı gibi bir tutumun siber alanın ele alındığı bütünlük içerisinde anlamsız olduğu ortaya konulmuştur.

11 Eylül olaylarının yeni tehditleri beraberinde getirdiği yaklaşımda, hem siber güvenlik anlayışındaki hem de siber alandaki çeşitlilik benzer çalışmaların da konseptini oluşturmuştur. Siber alandaki savunma ve saldırı çeşitliliği güçlü ülkelerin her an tetikte olmaları gerektiğini göstermiştir. Birçok devlet için ise Soğuk Savaş'ın bitimi, güvenlik sorunları bağlamında çözümleri zor paradoksları oluşturmuştur. Siber kapasiteye dayandırılan unsurlar için ekonomik çıkar ve düşmanı zarara uğratma gibi arayışlar kendini hissettirmeye başlamıştır.

Siber güvenlik kavramının dahil olduğu uluslararası güvenlik temelinde, nükleer caydırıcılığın hala ulusal güvenlik konusunda en büyük tehlike olduğu ortadadır. Nükleer, kimyasal ve biyolojik kitle imha silahlarının yaygın olduğu sorunlarla birlikte, farklı sorunların devletleri meşgul ettiği süreçte güvenlik yaklaşımı ve yaklaşımın çeşitlendiği siber alandaki tehditsel durum her geçen gün artmakta ve bu durum politik girişimlerin rasyonelliğinin tartışılmasını gerekli kılmaktadır. Farklı alanlarda olduğu gibi devletler güvenlik temelindeki tehlikeleri bertaraf etmek için rasyonel olduklarını zannettikleri birçok

konuda, çoğu zaman ittifak arayışlarına girmektedir. Tartışmaları da alevlendiren husus, uluslararası alanda ortak güvenlik oluşturulacaksa, bu anlayışın samimiyeti ve tarafsızlığı yönündeki atıflar olmaktadır. Ortak bir uluslararası aklın ortaya çıkamamasındaki temel nedenler zaten karmaşıkken siber güvenlik gibi bir konunun alana dahil olması kartları çeşitlendirmiştir.

Sürecin geldiği boyut farklı şekilleriyle anılırken güvenlik temelinin birçok noktasıyla Soğuk Savaş ile ilişkilendirilmesi, dönüşümü devletler bazında kısır bir noktaya sıkıştırmaktadır. Süreç kendi içerisinde, teknolojik gelişmelerle ortaya çıkan farklı imgeleri özgün bir şekilde alana ilişkin olarak üretmiştir. Bu sürecin hissedildiği nokta 11 Eylül olmuş, fakat dinamikler kendini özgün nitelikleriyle kurgulamıştır. Siber güvenliğin geldiği noktada devletlerin illegal yapılarla iş birliği içerisinde olması ve güvenlik algısının şaşırtıcı alt başlıklar halinde çeşitlenmesinde bu neden etkili olmuştur.

Uluslararası ilişkiler adına farklı teorik yaklaşımlar ve bu yaklaşımların uluslararası düzenin başdöndürücü bir şekilde artan başlıklarına ilişkin yorumları kendi içerisinde tutarsızlaşmaya başlamıştır. Devletlerin uluslararası sistemde dış politika toplamı olarak ele alınmadığı gerçeği, kendi geleceğini garanti altına almakla sorumlu devlet yaklaşımıyla çok yönlü bir sorunsala dönüşmüştür. Sistemin kurallarını belirleyebilme yetisinden çıkan devletler çıkar mücadelesini kaotik bir sürece sürüklemiştir.

Uluslararası alandaki ilişkilerin sadece çatışmacı bir ortamda ilerlemediği günümüzde, siber alanda yaşanan atılım hegemonun dikte ettiği bir üretim ve tüketim algısını beraberinde getirmiştir. Bu algı, aktörler düzeyindeki karmaşık ilişkiyi uluslararası ilişkiler boyutuna, siber güvenlik düzeyine çatışmacı boyutta taşımıştır. Siber alanının çatışmacı boyutunu açıklamaya ilişkin oluşturulacak uluslararası politikada, inşacı yaklaşım daha rasyonel bir perspektif sunmaktadır. Bireysel ve toplumsal beklentiler, dalgalanmalar siber güvenlik alanındaki strateji düzeyinde çoğu zaman belirleyici olabilmektedir.

Uluslararası güvenlik çalışmaları perspektifinde strateji oluşturulmasına ilişkin oluşturulacak ajandalar, bu alanda atılım yapmak isteyen ülkeler adına kaçınılmaz gözükmektedir. Strateji oluşturulmasına ilişkin siber alanın gelişimi uzun vadeli politikalarla desteklenmezse, veri kayıplarının olması ve ekonomik zararların hissedilmesi kaçınılmaz

gözükmektedir. Atılacak adımların uluslararası ilişkiler temelinde, uzmanlık alanlarının oluşturulmasıyla gerçekleşeceği açık bir şekilde hissedilmektedir. Farklı kurumlar aracılığıyla oluşturulan yapılanmalar bu durumun en açık örnekleri haline gelmiştir.

Strateji belgelerinin yanında, çalışmanın temelindeki ittifak oluşturma ya da oluşturabilme kurgusu tercih edilebilir bir alternatiftir. Bunun en önemli verisel bütünlüğü, devletlerin farklı başlıklar altında sınıflandırıldığı raporlar olmuştur. Bazı güvenlik şirketlerinin son yıllarda ortaya koyduğu veriler yol gösterici niteliktedir ve gözlerden kaçırılmamalıdır. Siber caydırıcılık açısından, uzun vadeli ittifakların oluşturulması siber güvenlik alanında oldukça zor gözükürken, bazı temel konularda ad-hoc birliktelikler çıkar bütünlüğü sağlayabilecektir.

İttifak olgusunun teorik düzleminin oluşturulduğu çalışma dahilinde, öze ilişkin sunulan modellemede ilkesel bir bütünlük konulmuştur. Siber uzayın aktörleri haline gelen devletlerin ilkesel davranış içinde olması ve bu konuda somut adımlar atmaları beklenmemektedir. Gelişime açık olarak sunulan modellemede, güç potansiyellerinin ölçümüyle siber suçların bertaraf edilmesinin yanında rakip unsurlara kaşı ortak hareket edebilme perspektifi sunulmuştur. Tehdit potansiyelinin artışı bu birliktelikleri gerekli kılmıştır ve tartışılan nokta bu temel düzeyinde kalmıştır. Siber güvenlik ve temelindeki olaylar siber terörizm dahilinde devletlerin ajandalarında yer alması gereken hususlardır. Ortaya konulan veriler, siber alana kısmen de olsa bağlı olan devletlerin konuyla uzaktan ve yakından ilişkili olduğu ile ilgilidir. Farklı olayların incelendiği kurgusal bütünlük dahilinde çalışma boyunca bu duruma atıflar yapılmıştır. Siber alana artan bağlılık tehditsel bütünlüğü genişletmektedir.

Siber güvenlik temelindeki gelişmelerle birlikte askeri teknolojilerin belirli noktalara taşındığı kara, hava, deniz unsurlarında ve nükleer mücadelede kendini hissettiren siber alandaki çıkar birliktelikleri, hedef unsurlara karşı özgüveni artırmaktadır. Siber alanın güç mücadelesinde, ülkelerin savunma sistemlerine saldıracak ve etki edecek daha gelişmiş yöntemler üzerinde tartışmalar sürmektedir. Bu yaklaşımlar dahilinde, klasik olarak güç algısı yerine farklı araçlarla gücün kapsamını artırma, yeni teorik bir yaklaşımın çıkış noktası olarak dikkate değerdir.

ABD bünyesinde siber alandaki sektörel destek ve konuya ilişkin çalışmalar kısa vadede saha çalışmalarını yönledirecek yetkinliğe ulaşmıştır. Özellikle uzmanlık alanlarının oluşturulması ve ar-ge faaliyetlerinin yoğunlaştırıldığı siber alanda gelişmekte olan ülkeler için ajandalar sunulması gerekmektedir. Dikkate alınırlığı tartışılabilir fakat özgün bölgesel yaklaşımların önemi, siber alandaki zafiyetlerle daha çok hissedilecektir. Karar alıcıların etkilendiği farklı raporlarla yıldızını parlatan ABD gibi güçler uluslararası ilişkilerin teorik altyapısını bu alandaki yükselişiyle kurgulamaktadır.

AB ve NATO gibi örgütlerin bünyesinde yer alan sertifika ve uzmanlık programları, siber güvenlik alanında farklı konulara yönelmektedir. Uluslararası ilişkiler alanında, siber güvenlik özelinde risk yönetimi ve karar alıcıların yönlendirilmesi konularında yer alan uzmanlık programları dikkat çekici bir şekilde artış göstermektedir. Özellikle bölgesel düzeyde siber sorunların yer aldığı bu türden programlarda uluslararası ilişkilerin temel çerçevesinde yapılan çalışmalar teorik alana katkı sağlamaktadır.

Siber güvenlik ve kendi özüne ilişkin çalışmaların varlık boyutu sadece uluslararası politika temelinde değerlendirilmemelidir. Akademik ve profesyonel düzlemde farklı alanlarda oluşmaya başlayan baskınlık bir güç mücadelesine dönüşmüştür. Teknik alandaki gelişim ve başdöndürücü hız devletleri karşı karşıya getirmekte ve ciddi bir veri trafiği oluşmaktadır. İnterdisipliner bir yön gösteren bu çeşitlilik, siber suç olgusunu beraberinde getirerek uluslararası hukuk boyutunda bir farkındalığı oluşturmuştur.

Vurgulanan boyutsal farkındalık ve farklılık siber güvenliğin nasıl tartışıldığı veya tartışılması gerektiği hususunda çeşitliliği sağlayarak inşacı yaklaşım açısından bir zemini kuvvetlendirmektedir. Uluslararası ilişkiler ve onun özelinde hızla tırmanışta olan siber güvenlik çalışmaları, günümüze en yakın teorik yaklaşımlarla birlikte kendine yer bulabilmektedir. Uluslararası ilişkilerin kendi özündeki bütünlük açısından inşacı yaklaşım, aktörlerin sosyal etkileşimde bulunduğu yapıya odaklanması ile siber güvenlik açısından bir düzey oluşturulmasına yardımcı olmaktadır.

Siber silahların, fiziksel etki doğuran silahlara göre sınıflandırılması sorunsalı ve devletlerin siber alanda gelişiminde caydırıcılık oluşturmasına ilişkin veriler, inşacılık perspektifinde bir fikir bütünlüğünü kolaylaştırmıştır. Silahlanma yarışının siber alanda

teknik bir boyutta geliştiği süreç, kurgulunacak model dahilinde, devletleri yeni bir savaş alanına iterek *siber savaşları* tartışma alanına sokmuştur. İç politikanın etkilenmesi ve oluşturulması konusunda *güvenlikleştirme kuramları* gibi yaklaşımlarla siber alanı açıklama isteği artar hale gelmiştir. Ulusal çıkarların tehdit algısına dönüştüğü siber savaş ortamı etkileşimi artırmıştır.

Siber savaş ortamındaki etkileşim, ekonomik açıdan yük getirmeyen zararlı yazılımların ortaya çıkışını ve nitelikli personelin tedariki hususundaki süreci hızlandırmıştır. Uluslararası güvenlik adına siber tehditler, güvenlikleştirme modeli açısından iç politikanın etkilenmesinde kendisine yer edinmeye başlamıştır. İç politikanın etkilenmesi ve ulusal çıkarın farklılaştırdığı tehdit algısı ile birlikte siber caydırıcılık açısından dış politikada çıktılar üretilmeye başlanmıştır. İnşacılığın güvenlikleştirme süreciyle buluştuğu noktada, siber politikalar üretebilen uzmanlara duyulan ihtiyaç ve bu konudaki acil eylem planları farklı alanlarla etkileşimi zorunlu kılmaktadır.

Siber uzayın uluslararası güvenlik açısından tartışılması ve beraberindeki etkileşim, devletlerin dış politikada ve iç politikada sahip olduğu çıktılara dair nedensel bir düzlem sağlamaştır. Siber alanın uluslararası ilişkiler açısından bir savaş alanı olup olmadığına dair eleştiriler olsa da, dijital ortamdaki kaynakların sonlandırılması imkansıza dönüştüğü için yersiz kalmaktadır. Siber alanın beslendiği tüm kaynaklar son bulsa da, verilerin görünmeyen bir sanal ortamda varlığını sürdüreceği gözlerden kaçırılmamalıdır.

Bilişim teknolojilerindeki gelişme, toplum ile karar alıcılar arasında iki yönlü bir iletişim kanalını ortaya çıkarmıştır. Bu iletişim kanalı bireylerin karar alıcılara etki edebilmesi ile igilidir ve bu hususstaki ilgi de artış içindedir. Sibernetik toplum ve karar alıcılar arasındaki yönetim biçimi bu geniş çalışma içinde otokontrol, bilgi aktarımı, bilişsellik gibi unsurlarla interdisipliner bir hal almıştır. Bu konudaki gelişim tahmin edilemeyecek bir boyuta ulaşarak devletler arasında bir yarış durumuna dönüşmüştür.

Siber güvenlik ve onun kapsadığı bilgi teknolojileri, karar alıcılar açısından toplumsal tepkinin ölçülmesi ve takip edilmesi adına önemli bir araç haline gelmiştir. Devletler bir dizi amaçsal nitelikler dahilinde uzman ekipler kurarak süreci manipüle etmeye başlamıştır. Bu alan içerisine askeri unsurların dahil olması, organizasyonel bir gerekliliği

gündeme getirmiştir. Siber uzayda stratejistler ve karar alıcıların caydırıcı olma adına taktiksel unsurlar geliştirmesi, toplumsal değişimi sağlamıştır.

Toplumsal ve bireyler düzeyindeki değişikliklerle siber terörizmin beslendiği nokta ve harekat bulma süreci politika üretme zorunluluğunu ortaya çıkarmıştır. Siber tehdit yöntemleri ve ortaya çıkış süreci verisel ortamı etkiledikten sonra maddi ve manevi sonuçlar doğurmaktadır. Uğratılan zarar sonunda telafisi zor gelişmeler yaşanmaktadır. Oluşan suçların etkileyici olmaları bireysel olmalarına, kurumsal bir etki oluşturmasına ya da devlet gibi uluslararası aktörlere etki edişine göre farklılaşmaktadır. Devletlerin müdahil olduğu siber olaylar çoğu zaman organizasyonel suçlardan daha etkili sonuçlar doğurabilmektedir.

Etkili sonuçların doğabileceği siber olaylarda, siber saldırının nasıl ve nereden gerçekleştiğinin bilinmezliği siber caydırıcılık kavramına yapılan en önemli eleştirilerin başında gelmektedir. Siber savunma kabiliyetinin niteliği siber saldırıları boş bir çaba olarak gösterebilmektedir. Savunmanın da bir strateji haline dönüştüğü siber alanda güvenlik açıklarının tespiti daha maliyetli bir hal alabilir. Bu konuda devletlerin farklı alanlarda tecrübelerini paylaşması önemli bir politik manevra oluşturulmasına yardımcı olmaktadır.

Siber güvenlik ve özelindeki kullanıcıların güvenlik özelliklerinin, siber ortamda bulunan güvenlik risklerine karşı koyabilecek şekilde oluşturulmasına yönelik birtakım araçların varlığına ihtiyaç duyulmaktadır. Bu araçlarla birlikte gelişen siber ortamda, baskı oluşturmak adına siber saldırı türleri çeşitlenmiştir. Siber alanda politikalar üretilmesi ve uluslarası ilişkiler içerisinde tüm bireylerin ve aktörlerin etkileşimde olduğu bir alanın hissedilmesi, alandaki çalışmaların temeline risk analizini de eklemiştir.

Siber uzayın tartışıldığı ve konumlandığı alanda, siber müdahele araçları politik düzlemde tartışılmaya başlanmış ve bu konudaki veriler geliştirilmiştir. Siber silahların kullanımına ilişkin verilerin oluşması, bunların politik manevralarda kullanılması siber istihbarat gibi yeni ve özgün çalışma alanlarını ortaya çıkarmıştır. Uluslararası alanda, siber suçlara ilişkin atılacak adımlarda ve bu konudaki suçluların organizasyonlarında ortak hareket algısının arttığı verilerle ortaya konulmuştur. Siber alandaki saldırı kabiliyetleri, oluşan istihbarat birimleri adına bir avantaj ve kolaylık sağlamaktadır.

Siber silahların kullanımı ve verilerin ele geçirilmesine yönelik olarak, istihbarat temelinde hedeflerin varlığı farklı düzeylerde kendini göstermektedir. Bu durumun tartışıldığı boyut karakteristik bir düzlem oluşturamamıştır. Bu durumun sebebi siber alandaki mücadelenin kendi içerisinde özgün olaylar dahilinde gerçekleşmesidir. Devletler operasyonel unsurlar oluştururken bu konuda bir sınıflandırmaya gidememektedir. Bu durum siber alandaki mücadeleyi anlık verilerle, değişken bir şekilde karşımıza çıkarmaktadır.

Devletlerin siber alanı farklı şekillerde müdahil olarak kullanabileceği çerçeve, uluslararası politikada aktör olma sorununu gündeme taşımıştır. Analiz düzeyi ve teorik sorunlar bu konuda en önemli noktayı oluşturmaktadır. Siber politikalar ve uluslararası düzeyde tüm aktörlerin yer aldığı bir uyum, uluslararası ilişkilerin kendi doğasında dahi zorlaşırkan siber alanda imkansıza yakın durmaktadır. Uluslararası aktörlerin bu noktada belirli niteliklerle sıralanması ve uluslararası platformlar oluşması makro düzeyde oldukça zor gözükmektedir.

Uluslararası politikanın bütünlüğü açısından oluşturulan siber ordular ve siber güvenlik algısının çeşitlendiği yön, konuya ilişkin uzmanlık alanını farklı aktörlerle inceleme boyutuna çekmiştir. Oluşturulacak siber ordular ve etkileşimde olduğu tüm askeri unsurlar devletlerin yeni bir caydırıcılık alanında ilerleyişini sağlayacaktır. Uluslararası alanda oluşacak illegal yapılar ve bağlı olacakları resmi kurum ve kuruluşlar, çıkarsal işbirlikleri ile birlikte devletleri savaş eşiğine getirebilir ve siber ordular görev sorumluluğunu konvansiyonel unsurlara bırakabilir. Bu konudaki vizyon uluslararası alanda alınacak kararların gerçekçiliğine bağlıdır.

Siber uzayda baskın olma isteği ve bu durumun devletlere olan zararı, egemenlik haklarının tartışıldığı bir alanı belirginleştirmiştir. Gerçek bir sınırsal bütünlüğe sahip olmayan siber alanda hakimiyet kurma boyutu sınırsız kalmaktadır. Bu durumda, siber alanda silahlanma yarışı ve tırmanma uzunca bir dönem adından söz ettirecektir. Devletlerin içerisinde olduğu müdahil alan, çıkarsal bir bütünlük oluşturamasa da rakibe zarar verme adına bir artı katmaktadır. Siber alandaki değişimin nasıl takip edileceği ve verisel olarak analizi siber ordular düzeyinde belirleyici olmaktadır.

Uluslararası alanda hukuksal bir bütünlüğün oluşması ve siber alanın kurallarının belirlenmesi kısa vadede acil bir durum niteliği taşımaktadır. Uluslararası hukukun değersel bütünlüğü, tüm ülkeler adına eşit düzeyde olmasa da kurallar bütününün oluşturulması gerekmektedir. Siber alandaki faaliyetlerin fiziksel zararları kritik altyapıların hedeflenilmesi ile hissedilir bir boyuta ulaşmıştır. Siber saldırılar sonucunda fiziksel zararların oluşması ve kuvvete başvurma gibi bir durum konunun geldiği boyutta tartışılır bir hal almıştır. ABD ve özelindeki NATO bünyesinde, kuvvet kullanma konusunda ciddi bir istek hissedilmektedir.

Günümüzde savaşların sadece askerler ve askeri teknolojiler yardımıyla yapılmadığı artan siber olaylarla birlikte ortaya konulmuştur. Kamu hizmetleri, ulaşım, iletişim ve enerji gibi kritik endüstrileri aksatan veya yok eden silahlandırılmış bilgisayar programlarının, farklı coğrafyalardan serbest bırakılmasıyla ciddi bir karmaşıklık devletlerin gündemine eklenmiştir. Bu tip saldırılar askeri unsurların hareketlerini, savaş uçaklarının rotalarını ve savaş gemilerinin komuta kontrolünü sağlayan ağları da etkisiz hale getirir bir hal almıştır.

Rakip unsurların etkisiz hale getirilmesi ya da verilen maddi zararlar zamanla uluslararası aktörlerin iştahını kabartmıştır. Özellikle devletlerin bu konudaki mücadelesi ve siber alanın vermiş olduğu avantaj, aktörleri şeffaf olma konusunda zorlamamaktadır. Siber terörizmin ortaya çıkışı ve bu konudaki başıboşluğun temelinde bu husus yer almaktadır. Bu sürecin hızlandığı zaman dilimi Soğuk Savaş ve sonrasındaki dönem olmuştur. Soğuk Savaş sonrasındaki askeri-stratejik ortamın değişimi önemli göstergelerle karşımıza çıkmaktadır.

Mücadele araçları içerisinde, gelişimini ve farklılaşmasını kendi temelinde siber saldırı araçlarına dönüştüren alan, geleneksel tehdit anlayışını yeni güvenlik yaklaşımı içerisinde belirginleştirmiştir. NATO'nun tehdit tanımlamaları, ABD'nin özellikle siber güvenlik alanında vermiş olduğu öncelik ve yeni bir harekat alanı oluşturan siber savaş bu temel değişim içerisinde en somut tespitlerdir. Çalışmanın temelinde ele alınan ittifak anlayışı bu yaklaşımın getirdiği bakış açısıyla oluşturulmaya çalışılmıştır. Yakın çevredeki tarihi ve psikolojik bütünlük bu bakış açısının çıkış noktasını oluşturmaktadır.

Siber güvenlik içerisinde zaman ve mekan algısının klasik çatışmalara göre farklı şekillerde ortaya çıkışı, saldırgan profillerinin farklı düzeylerde ve amaçlarda faaliyetlerini

sürdürüşü güvenlik yaklaşımı oluşturmada zorlaştırıcı unsurlardır. Konuya ilişkin ortak hareket edebilme güdüsü bu temelde ele alınmıştır. Siber güvenlik bireylerin sınırlı teknik kaynaklarıyla oluşturdukları saldırıları, devlet destekli unsurlarla çok daha geniş bir alana yaymıştır. Farklı düzeylerdeki aktörlerin çatışma kültürü içinde siber güvenlik alanındaki çıkar mücadeleleri, profillerin daha da çeşitleneceği imajını ortaya koymaktadır.

Yakın coğrafyalarda kimi devletlerin kritik altyapılar düzeyinde, özellikle enerji nakil hatlarına bağlılıkları siber tehdidin dönüşümünde ve ittifak oluşturulmasında önemli bir stratejiyi oluşturmaktadır. Siber alanda gelişen devletlerin kritik altyapılarının korunmasına ilişkin ittifak arayışları, diplomasi unsurlarıyla birlikte daha küçük yapılanmaların avantajını ortaya koymaktadır. Siber ittifakların oluşturacağı caydırıcılık pozitif bir değer katacaktır.

Yeni bir politik yaklaşım oluşturma gayretiyle ele alınan verilerde, siber alanda yaklaşım geliştirebilme ve güvenliğin daha fazla anlam ifade edebilmesi adına yeni politikalar sunabilme, amaçsal bir bütünlük gerektirmektedir. Özellikle Türkiye gibi *"siber güvenlik"* alanında gelişme arzusu duyan devletlerin atabilecekleri adımlara ilişkin perspektif, özgün bir niteliğe sahip olacağı düşünülen *Mikro Siber İttifak Teorisi (Micro Cyber Alliance Theory, Micro-CAT)* ile birlikte tartışılmıştır. Çalışma kapsamında ele alınan bu yaklaşım, geçici ittifakların ve çalışma biçiminin siber diplomasi masalarıyla birlikte, ad-hoc yapıda işleyebilirliği ile ilgilidir. Ad-hoc nitelik, ittifak yaklaşımının amaca yönelik kullanılması kapsamında ele alınmıştır. İttifak türünün uygulanma biçimi ve etkinliği geçici bir çözüme ve saldırı biçimine göre yer almalıdır ve harekat yapısı buna göre şekillendirilebilir.

Mikro siber ittifaklar için siber diplomasi kanatları ve bu birimler dahilinde oluşturulacak takımlar belirleyici, yönlendirici bir unsur olarak müzakere alanında ve devletler arasında kararların hızlandırılmasında önemli bir görev üstlenecektir. Varılacak hedef ve kısa vadeli programların belirlenmesi siber alanda önemli bir yere sahiptir. Bu konudaki temeli ise siber diplomasi masaları oluşturacaktır. Türkiye gibi gelişme arzusu içinde olan ülkeler adına siber diplomasi masalarının oluşturulması, belli uzmanlıklarla birlikte varılacak hedefin, belirlenecek olası saldırının zamanını ve yerini belirleme misyonuna sahip olacaktır.

Siber diplomasi kanatları iki yönlü işletilmelidir. Bunlardan ilki ülke içerisinde kurulacak siber diplomasi masaları, diğeri ise kurulacak ittifaklarda sürecin müzakerelerini yürütecek kanatlardır. Hatta diplomatik misyonlara konuyla ilgili, karşı ülkede faaliyetleri yürütecek ve müzakere edebilecek uzmanların yerleştirilmesi söz konusu olabilecektir. Siber diplomasi eğer bir caydırıcılık kapasitesine sahip olursa, teorik olarak önleyici diplomasinin yerine geçebilecektir. Kritik altyapılara yönelecek herhangi bir saldırı öncesinde siber diplomasi ve onun özelinde oluşturulacak birimler karakteristik bir hal alabilir. Önleyici diplomasinin karakteristik özelliği çatışmaya erken müdahele etmesi sebebi ile en az karmaşık, en insancıl yöntemlerden biri olarak uluslararası çatışmaların çözümünde bir yoldur. Siber saldırılar, kritik altyapılar gibi fiziksel noktalara yönelmeden bir diplomatik araca dönüşecekse, önleyici diplomasi içerisinde yoğrulabilir.

Devletlerin siber alanı ittifak algısına dönüştürmesiyle operasyonel unsurların oluşturulması hız kazanacaktır. Ad-hoc siber ittifaklarda operasyonel unsurlar dahilinde, amaçlanan hedefe göre ortak çalışmalar yapılabilir ve hedefler ulusal çıkarlara dönüştürülebilir. Fakat operasyonel unsurlar sadece savunma amaçlı düşünülmemelidir. Sahip olunan yetenek siber saldırıların önünü de açmalıdır. Siber alanda özel amaçlarla ve belli konular dahilinde, çıkarsal birlikteliklerle hareket kabiliyetine sahip ad-hoc siber ittifaklar hedefleri belirlenmiş olarak hareket edebilmelidir. Ad-hoc siber ittifaklar açısından operasyonel unsurların oluşturulması ve hedeflerin belirlenmesi aşamalarıyla birlikte savunma hattındaki en büyük zafiyet kritik altyapıların korunmasında karşımıza çıkacaktır.

YARARLANILAN KAYNAKLAR

Açıkmeşe, Sinem Akgül (2012a), "Strateji ve Güvenlik Kavramları", Mustafa Aydın ve Ahmet Haluk Atalay (Ed.), **Strateji ve Güvenlik**, 1. Baskı *içinde* (2-22), Eskişehir: Anadolu Üniversitesi Yayınları.

———————— (2012b), "Stratejik Çalışmalar", Mustafa Aydın ve Ahmet Haluk Atalay (Ed.), **Strateji ve Güvenlik**, 1. Baskı *içinde* (22-40), Eskişehir: Anadolu Üniversitesi Yayınları.

Ağır, Bülent Sarper (2011), "Güvenlik Kavramını Yeniden Düşünmek: Küreselleşme, Kimlik ve Değişen Güvenlik Algısı", **Güvenlik Stratejileri Dergisi**, Sayı 22, 97-131.

Aksu, Fuat (2008), **Türk Dış Politikasında Zorlayıcı Diplomasi**, İstanbul: Bağlam Yayınları.

Aksu, Muharrem ve Turhan Faruk (2012), "Yeni Tehditler, Güvenliğin Genişleme Boyutları ve İnsani Güvenlik", **Uluslararası Alanya İşletme Fakültesi Dergisi**, 4(2), 69-80.

Al-Rawi, Ahmed K. (2014), "Cyber Warriors in The Middle East: The Case of The Syrian Electronic Army", **Public Relations Review**, 40, 420-428.

Altunok, Taner ve Avcı, Engin (2009), "Siber Tehditlerin Geleceği ve Alınması Gereken Önlemler", Haydar Çakmak ve Taner Altunok (Ed.), **Suç, Terör ve Savaş Üçgeninde Siber Dünya**, 1. Baskı *içinde* (209-232), Ankara: Barış Platin Kitabevi.

Altunok, Taner ve Kaya, Zeynep (2009), "Siber Tehditlerle Mücadele", Haydar Çakmak ve Taner Altunok (Ed.), **Suç, Terör ve Savaş Üçgeninde Siber Dünya**, 1. Baskı *içinde* (137-162), Ankara: Barış Platin Kitabevi.

Aral, Berdal (2007), "Asimetrik Saldırı Savaşları, Siyaset ve Uluslararası Hukuk", **Uluslararası İlişkiler Dergisi**, 4(14), 39-83.

Aras, Bülent ve diğerleri (2010), **SETA Rapor, Araştırma Merkezlerinin Yükselişi: Türkiye'de Dış Politika ve Ulusal Güvenlik Kültürü**, Ankara: SETA Yayınları

Arnold, Todd ve diğerleri (2013), "Professionalizing The Army's Cyber Army's Cyber Officer Force", **Army Cyber Center**, http://www.gregconti.com/publications/pro_cyber.pdf (13.04.2016).

Ateş, Davut (2013), **Uluslararası Politika: Dünyayı Anlamak ve Anlatmak**, Bursa: Dora Yayıncılık.

Austin, Greg (2016), "Middle Powers and Cyber-Enabled Warfare: The Imperative of Collective Security", **Australian Centre for Cyber Security**, https://www.unsw.adfa.edu.au/australian-centre-for-cyber-security/sites/accs/files/uploads/DISCUSSION%20PAPER%20Middle%20Powers%20REARMED%2027%20Jan%202016.pdf (18.08.2016).

Bakır, Emre (2013), **5. Boyutta Savaş: Siber Savaşlar**, https://www.bilgiguvenligi.gov.tr/siber-savunma/5.-boyutta-savas-siber-savaslar-ii.html (10.05.2016).

Barnett, Michael (2014), "Ortadoğu'da Kimlik ve İttifaklar", Peter J. Katzenstein (Ed.), **Milli Güvenlik Kültürü Dünya Siyasetinde Normlar ve Kimlik**, 1. Baskı *içinde* (445-495), Sakarya: Sakarya Üniversitesi Kültür Yayınları.

Barnum, Sean (2014), "Standardizing Cyber Threat Intelligence Information with The Structured Threat Information Expression", **STIX Whitepaper,** (1.1) http://stixproject.github.io/getting-started/whitepaper/ (12.04.2016).

Başaran, Alper (2014), "Tehlike Bir Tık Ötede", **Siber Savaş Cephesinden Notlar**, http://securitist.blogspot.com.tr/2014/12/verizon-bilgi-guvenligi-olaylar-raporu.html (13.07.2016).

Bayık Ü. ve diğerleri (2013), "Ulusal Siber güvenliğin Sağlanmasında NATO'nun Olumlu Etkilerinin Artırılması İçin Yaklaşım Modeli", **6. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı Bildiriler Kitabı**, 1. Baskı *içinde* (341-344), Ankara: Bilgi Güvenliği Derneği.

Baylis, John (2008), "Uluslararası İlişkilerde Güvenlik Kavramı", **Uluslararası İlişkiler Dergisi**, 5(18), 69-85.

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

Beck, Ulrich (2009), **World at Risk**, Cambridge: Polity Press.

Bejtlich, Richard (2015), "Strategic Defence in Cyber Space: Beyond Tools and Tactics", Kenneth Geers (Ed.), **Cyber War in Perspective: Russian Aggression against Ukraine**, 1. Baskı *içinde* (159-170), Tallinn: NATO CCD COE Publications.

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

Bendrath, Ralf ve diğerleri (2007), "From 'Cyberterrorism' to 'Cyberwar', back and forth: How The United States Securitized Cyberspace", Johan Eriksson ve Giampiero Giacomello (Ed.), **International Relations and Security in The Digital Age**, 1. Baskı *içinde* (57-83), New York: Routledge Publishing.

Berber, Leyla Keser (2012), **Siber Güvenlik Raporu**, İstanbul: İstanbul Bilgi Üniversitesi, Bilişim ve Teknoloji Hukuku Enstitüsü.

Bıçakçı, Salih (2012), "Yeni Savaş ve Siber Güvenlik Arasında NATO'nun Yeniden Doğuşu", **Uluslararası İlişkiler Dergisi**, 9(34), 205-226.

——————— (2014), "NATO'nun Gelişen Tehdit Algısı: 21. Yüzyılda Siber Güvenlik", **Uluslararası İlişkiler Dergisi**, 10(40), 101-130.

Bilgen, Ela (2016), "Offshore Kıyıya Vurdu: Panama Belgeleri", **ATAUM E-Bülten**, Yıl 8, Sayı 91, 1-4.

BİLGESAM, Dış Politika ve Savunma Araştırmaları Grubu (2010), "Başlangıcından Bugüne NATO Stratejik Konseptinin Geçirdiği Evreler", http://www.bilgesam.org/incele/1221/-baslangicindan-bugune-nato-stratejik-konseptinin-gecirdigi-evreler/#.V8R64mXwyuU (08.05.2016).

Bilgiç, Ali (2012), "Güvenlik İkilemini Yeniden Düşünmek: Güvenlik Çalışmalarında Yeni Bir Perspektif", Mustafa Aydın ve diğerleri (Ed.), **Uluslararası İlişkilerde Çatışmadan Güvenliğe**, 1. Baskı içinde (337-352), İstanbul: İstanbul Bilgi Üniversitesi Yayınları

Binde, Beth E. ve diğerleri (2016), "Assessing Outbound Traffic to Uncover Advanced Persistent Threat", **SANS Technology Institute**, https://www.sans.edu/student-files/projects/JWP-Binde-McRee-OConnor-slideswnote.pdf (08.08.2016).

Birdişli, Fikret (2016), **Teori ve Pratikte Uluslararası Güvenlik: Kavram-Teori-Uygulama**, Ankara: Seçkin Yayıncılık.

Botezatu, Bogda (2011), "H1 E-Threat Landscape Report: Malware, Spam and Phishing Trends", **Bitdefender**, http://www.bitdefender.com/media/materials/e-threats/en/H1_2011_E-Threats_Landscape_Report.pdf (06.07.2016).

Booth, Ken (2014), **Dünya Güvenliği Kuramı**, (Çev. Çağdaş Üngör), İstanbul, Küre Yayınları.

Boyraz, Mehmet (2015), "NATO'nun Siber Güvenlik Politikası: Tarihsel Süreç ve Kırılma Noktaları", **Research Turkey, Türkiye Politika ve Araştırma Merkezi**, http://researchturkey.org/tr/natos-cyber-security-policy-the-historical-process-and-critical-junctures/ (22.07.2016).

Broadhurst, Roderic ve diğerleri (2014), "Organizations and Cyber Crime: An Analysis of The Nature of Groups Engaged in Cyber Crime", **International Journal of Cyber Criminology**, 8(1), 1-20.

Brookes, Chris (2015), "Cyber Seucrity: Time for an Integrated Whole-of-nation Approach in Australia", **Indo-Pacific Strategic Papers**, http://www.defence.gov.au/ADC/Publications/IndoPac/150327%20Brookes%20IPS%20paper%20-%20cyber%20(PDF%20final).pdf (10.08.2016).

Brown, Gary D., Tullow, Owen W. (2012), "On the Spectrum of Cyber Space Operations", **Small War Journals**, http://smallwarsjournal.com/jrnl/art/on-the-spectrum-of-cyberspace-operations (04.02.2016).

Bucci, Steven (2009), "The Confluence of Cyber Crime and Terrorism", **Lecture#1123 on National Security and Defence**, http://www.heritage.org/research/lecture/the-confluence-of-cyber-crime-and-terrorism (13.01.2016).

Burgess, Heidi ve Guy M. Burgess (1997), **Encyclopedia of Conflict Resolution**, California: ABC-CLIO, Santa Barbara, California.

Buzan, Barry ve Hansen, Lene (2009), **The Evolution of Security Studies**, Cambridge: Cambridge University Press.

Buzan, Barry (1991), **People, States & Fear: An Agenda For International Security Studies in the Post Cold War Era**, 2nd Ed., Hemel Hampstead: Harvester Wheatsheaf Publishing.

Caşın, Mesut Hakkı (2008), **Uluslararası Terörizm**, Ankara: Nobel Yayın Dağıtım.

Carr, Jeffrey (2012), **Inside Cyber Warfare**, 2nd Ed. Sebastopol: O'Reilly Publishing.

Cavelty, Myriam Dunn (2008), **Cyber-Security and Threat Politics: US Efforts to Secure The Information Age**, New York: Routledge Publishing.

CB Insights (2016), "Deals to Cybersecurity Startups are Increasingly Global with Israel in The Lead", https://www.cbinsights.com/blog/cybersecurity-funding-geographic-trends/ (12.08.2016).

Charmonman, Srisakdi ve Trichachawanwong, Chatpawee (2014), "Training of Interdisciplinary Cyber Warriors", **International Journal of The Computer, The Internet and Management**, 22(2), 7-12.

Chatterjee, Bela Bonita (2014), "International Law and Cyber Warfare: An Agenda for Future Research", **Lancaster University Law School, Security Lancaster**, https://www.lancaster.ac.uk/media/lancaster-university/content-assets/documents/security-lancaster/tallinn_report_final[1].pdf (04.07.2016).

Chigas, Diana 2003, **Track II (Citizen) Diplomacy**, Beyond Intractability, http://www.beyondintractability.org/essay/track2-diplomacy (26.03.2016).

Choucri, Nazli (2012), **Cyberpolitics in International Relations**, Cambridge: MIT Press.

Choucri, Nazli (2013), "Co-Evolution of Cyberspace and International Relations: New Challenges for the Social Sciences", **World Social Science Forum**, http://ecir.mit.edu/images/stories/WSSF%20Co-evolution%20of%20cyberspace%20and%20IR%20final.pdf (08.08.2016)

Choucri, Nazli ve diğerleri (2013), "Institutions for Cyber Security: International Responses and Global Imperatives", **Information Technology for Development**, 20(2), 96-121.

Clarke, Richard A. ve Knake, Robert K. (2011), **Siber Savaş: Ulusal Güvenliğe Yönelik Yeni Tehdit**, (Çev. Murat Erduran), İstanbul, İKÜ Yayınevi.

Col, Muhterem ve Sagbansua, Lutfu (2015), "Role of The Exercises in Cyber Security Policy: Turkey Case", **The 2015 WEI International Academic Conference Proceedings**, 1. Baskı *içinde* (45-58), Prague: The West East Institute.

Commission of The European Communities (2001), **Network and Information Security: Proposal for A European Policy Approach**, http://eur-lex.europa.eu/LexUriServ/site/en/com/2001/com2001_0298en01.pdf (14.02.2016).

Corix Partners (2016), "Cyber Security Strategy & Governance", http://corixpartners.com/information-governance-and-strategy/ (12.08.2016).

Cornish, Paul ve diğerleri (2010), "On Cyber Warfare", **A Chatham House Report**, https://www.chathamhouse.org/sites/files/chathamhouse/public/Research/International%20Security/r1110_cyberwarfare.pdf (02.08.2016).

Cyber Research Center-Industrial Control Systems (2016), **Cyber Space: The Fifth Domain of War, White Paper**, http://www.crcics.net/documents/CRCICS2015_CyberSpace_the_fith_domain_of_war_2015v2.6.pdf (19.06.2016).

Çakmak, Haydar ve Demir, Cenker Korhan (2009), "Siber Dünyadaki Tehdit ve Kavramlar", Haydar Çakmak ve Taner Altınok (Ed.), **Suç, Terör ve Savaş Üçgeninde Siber Dünya**, 1. Baskı *içinde* (23-55), Anakara: Barış Platin Kitabevi.

Çakmak, Haydar ve Katman, Filiz (2009), "Siber Tehditlerin Uluslararası ve İç Hukuktaki Yeri", Haydar Çakmak ve Taner Altınok (Ed.), **Suç, Terör ve Savaş Üçgeninde Siber Dünya**, 1. Baskı *içinde* (162-209), Ankara: Barış Platin Kitabevi.

Çelik, Minhaç (2015), "Siber Ordu Kurmak İçin Devletler Özel Sektör İle Çalışıyor", **TMMOB Bilgisayar Mühendisleri Odası Dergisi**, Sayı 5, 32-34.

Çelik, Şener (2013), "Stuxnet Saldırısı ve ABD'nin Siber Savaş Stratejisi: Uluslararası Hukukta Kuvvet Kullanmaktan Kaçınma İlkesi Çerçevesinde Bir Değerlendirme", **Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi**, 15(1), 137-175.

Çetinkaya, Şeref (2012), "Güvenlik Algılaması ve Uluslararası İlişkiler Teorilerinin Güvenliğe Bakış Açıları", **21. Yüzyılda Sosyal Bilimler**, Sayı 2, 241-260.

Çifçi, Hasan (2012), **Her Yönüyle Siber Savaş**, Ankara: TÜBİTAK Bilim Kitapları.

Çiçekçi, Ceyhun (2012), **Uluslararası Güvenlik Çalışmaları**, İstanbul: Kriter Yayınevi.

Cyber Research Center-Industrial Control Systems (2016), "Cyber Practical Guide" http://www.crc-ics.net/documents/CRC-ICS-2016_Industrial-Control-System-Cyber-Governance-Guide-v3.7.pdf (30.08.2016).

Darcan, Emirhan (2015), "Siber Suçlarda Suçlunun karar Verme Süreci", Fatih Tombul ve diğerleri (Ed.), **Siber Suçlar: Tehditler, Farkındalık ve Mücadele**, 1. Baskı *içinde* (315-333), Ankara: Global Politika ve Strateji Yayınları.

Dedeoğlu, Beril (2003), **Uluslararası Güvenlik ve Strateji**, İstanbul: Derin Yayınları.

Delibasis, Dimitrios (2008), "Information Warfare Operations within The Concept of Individual Self-Defence", Athina Karatzogianni (Ed.), **Cyber Conflict and Global Politics**, 1. Baskı *içinde* (95-113), London: Routledge Chapman Hall.

Denning, Dorothy E. (2012), "Stuxnet: What has Changed?", **Future Internet**, Volume 4, 672-687.

Der Derian, James (2009), **Critical Practices of International Theory Selected Essays**, New York: Routledge Publishing.

Dewar, Robert S. (2014), "The 'Triptych of Cyber Security': A Classification of Active Cyber Defence", P. Brangetto ve diğerleri (Ed.), **6th. International Conference on Cyber Politics Proceedings**, 1. Baskı *içinde* (7-21), Tallinn: NATO CCD COE Publications.

Doğru, Murat (t.y.), **Siber Harekatın Uluslararası Hukuk Çerçevesinde Analizi**, http://ab.org.tr/ab16/bildiri/106.pdf (24.04.2016).

Dreyfus, Pablo Gabriel (2002), **Border Spillover Drug Trafficking and National Security in South America**, Yayınlanmamış Doktora Tezi, Universite de Geneve, Institut Universitaire de Hautes Etudes Internationales.

Dunn, Myriam A. (2007), "Securing The Digital Age: The Challenges of Complexity for Critical Infrastructure Protection and IR Theory", Johan Eriksson and Giampiero Giacomello (Ed.), **International Relations and Security in the Digital Age**, 1. Baskı *içinde* (85-106), New York: Routledge Publishing.

Ekstedt, Victoria ve diğerleri (2012), "Commitments, Mechanisms & Governance", Alexander Klimburg (Ed.), **National Cyber Security: Framework Manual**, 1. Baskı *içinde* (146-190), Tallinn: NATO CCD COE Publication.

Elman, Colin (2007), "Realism", Martin Griffiths (Ed.), **International Relations Theory for The Twenty-First Century: An Introduction**, 1. Baskı *içinde* (11-21), New York: Routledge Publishing.

Elmas, M. Salih (2013), **Modern Toplumun Güvenlik Çıkmazı: Tehdit, Risk ve Risk Toplumu Perspektifinden Güvenlik**, Ankara: USAK Yayınları.

Erdağ, Ali İhsan (2010), "Bilişim Alanında Suçlar (Türk ve Alman Ceza Hukukunda)", **Gazi Üniversitesi Hukuk Fakültesi Dergisi**, 14(2), 275-303.

Erdoğan, İbrahim (2013), "Küreselleşme Bağlamında Yeni Güvenlik Algısı", **Gazi Akademik Bakış Dergisi**, 6(12), 265-292.

Ergün, Oğuzhan (2014), "Güvenlik Kavramında Gelişmeler ve Asimetrik-Hibrit Savaşlar", **21. Yüzyılda Sosyal Bilimler Dergisi**, Sayı 8.

Eriksson, Johan ve Giacomello, Giampiero (2007), **International Relations and Security in The Digital Age**, New York, Routledge Publishing.

Esat, Yalçın (2014), **Türkiye'de Siber Güvenliğin Mevzuattaki Yeri ve Yapılan Çalışmalar**, https://www.bilgiguvenligi.gov.tr/mevzuat/turkiye-de-siber-guvenligin-mevzuattaki-yeri-ve-yapilan-calismalar.html (07.05.2016).

Follath, Erich ve Stark, Holger (2009), "The Story of Operation Orchyard", **Spiegel Online**, http://www.jmhinternational.com/news/news/selectednews/files/2009/11/20091103_SpiegelOnline_TheStoryOfOperationOrchard.pdf (16.08.2016)

Freedman, Lawrence (1989), "General Deterrence and The Balance of Power", **Review of International Studies**, 15(2), 199-210.

Fukuyama, Francis (1992), **The End of History and the Last Man**, New York: Avon Books.

Gallo, Giorgio ve Marzano, Arturo (2009), "The Dynamics of Asymmetric Conflicts: The Israeli-Palestinian Case", **The Journal of Conflict Studies**, Volume 29.

Galtung, Johan (2009), **Çatışmaları Aşarak Dönüştürmek: Çatışma Çözümüne Giriş**, (Çev. Havva Kök), Ankara: USAK Yayınları.

Gartzke, Erik (2013), "The Myth of Cyberwar: Bringing War in Cyberspace back down to Earth", **International Security**, 38(2), 41-73.

Geers, Kenneth (t.y.), "Cyberspace and The Changing Nature of Warfare", **U.S. Representative Cooperative Cyber Defence Center of Excellence**,

https://www.blackhat.com/presentations/bh-jp-08/bh-jp-08-Geers/BlackHat-Japan-08-Geers-Cyber-Warfare-Whitepaper.pdf (12.06.2016).

Giddens, Anthony (1998), **Ulus Devlet ve Şiddet**, (Çev. Cumhur Atay), İstanbul: Kalkedon Yayınları.

Gray, Colin S. (2007), **War, Peace and International Relations: An Introduction to Strategic History**, New York: Routledge Publishing.

Griffiths, Martin ve diğerleri (2011), **Uluslararası İlişkilerde Temel Düşünürler ve Teoriler**, (Çev. CESRAN), Ankara: Nobel Yayınevi.

Gücüyener, Ayhan (2015), **Enerji Güvenliğinde Yeni Bir Arayış**, https://www.linkedin.com/pulse/enerji-güvenliğinde-yeni-bir-arayış-ayhan-gucuyener?forceNoSplash=true (15.06.2015).

Güngör, Murat (2015), **Ulusal Bilgi Güvenliği: Strateji ve Kurumsal Yapılanma**, Ankara: Bilgi Toplumu Dairesi Başkanlığı.

Güntay, Vahit (2015), "Uluslararası İlişkiler Bağlamında Güvenlik Algısı ve Siber Güvenlik: Akdeniz, Karadeniz ve Avrupa Bölgeleri Üzerine Bir Değerlendirme", **The Journal of Academic Social Science Studies**, Number 37, 477-489.

Gürcan, Metin (2016), **Rusya'nın Bulanık Savaş Konsepti**, https://www.academia.edu/11069073/RUSYANIN_BULANIK_SAVAŞ_KONSEPTİ (03.05.2016).

Gürkaynak, Muharrem ve İren, Adem Ali (2011) "Reel Dünyada Sanal Açmaz, Siber Alanda Uluslararası İlişkiler", **Süleyman Demirel Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi**, 16(2), 263-279.

Haberleşme Genel Müdürlüğü (2014), "Ulusal Siber Güvenlik Çalışmaları, http://slideplayer.biz.tr/slide/2785253/ (03.05.2016).

Hansen, Lene ve Nissenbaum, Helen (2009), "Digital Disaster, Cyber Security and The Copenhagen School", **International Studies Quarterly**, Volume 53, 1155-1175.

Hare, Forrest (2010), "The Cyber Threat to National Security: Why can't We Agree?", C. Czosseck ve K. Podins (Ed.), **Conference on Cyber Conflict Proceedings**, 1. Baskı *içinde* (211-225), Tallinn:CCD COE Publications.

Hathaway, Melissa E. ve Klimburg, Alexander (2012), "Preliminary Considerations: On national Cyber Security", Alexander Klimburg (Ed.), **National Cyber Security: Framework Manual**, 1. Baskı *içinde* (1-44), Tallinn: NATO CCD COE Publication.

Hayes, Richard E ve Alberts, David S. (1995), "Information Warfare and Deterrence: Appendix B. The Realm of Information Dominance: Beyond Information War", **Federation of American Scientists**, http://fas.org/irp/threat/cyber/docs/iwd/appb.html (08.01.2016).

Healey, Jason ve Jordan, Klara Tothova (2014), "NATO's Cyber Capabilities: Yesterday, Today and Tomorrow", Atlantic Council, https://www.files.ethz.ch/isn/183476/NATOs_Cyber_Capabilities.pdf (12.07.2016).

Hemme, Kris (2015), "Critical Infrastructure Protection: Maintenance is National Security", **Journal of Strategic Security**, 5(8), 25-39.

Heritage Foundation (2016), "Index of US Military Strength", http://index.heritage.org/military/2016/assessments (18.03.2016).

Hettne, Björn (2012), "Teori ve Pratikte Güvenliğin Bölgeselleşmesi", Mustafa Aydın ve diğerleri (Ed.), **Uluslararası İlişkilerde Çatışmadan Güvenliğe,** 1. Baskı *içinde* (353-365), İstanbul: İstanbul Bilgi Üniversitesi Yayınları.

Hosein, Ian ve Eriksson, Johan (2007), "International Policy Dynamics and The Regulation of Dataflows: Bypassing Domestic Restrictions", Johan Eriksson ve Giampiero Giacomello (Ed.), **International Relations and Security in The Digital Age**, 1. Baskı *içinde* (158-172), New York: Routledge Publishing.

Hoskins, Andrew ve O'Loughlin, Ben (2008), "The Internet as a Weapon of War? Radicalisation, Publics and Legitimacy", Athina Karatzogiannni (Ed.), **Cyber Conflict and Global Politics**, 1. Baskı *içinde* (31-48), London: Routledge Chapman Hall.

Hunter, Eve ve Pernik, Piret (2015), **The Challenges of Hybrid Warfare**, Tallinn: ICDS Analysis.

İduğ Y. ve diğerleri (2013), "Siber Caydırıcılık ve Türkiye'nin İmkan ve Kabiliyeti", **6. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı Bildiriler Kitabı**, 1. Baskı *içinde* (287-290), Ankara: Bilgi Güvenliği Derneği.

Jabri, Vivienne (2008), "Reflections on the Study of International Relations", Trevor C. Salmon ve Mark F. Imber (Ed.), **Issues in International Relations**, 2. Baskı *içinde* (11-32), New York: Routledge Publishing.

Jervis, Robert (1978), "Cooperation Under the Security Dilemma", **World Politics**, 30(2), 167-214.

Jordan, Tim (1999), **Cyberpower: The Culture and Politics of Cyberspace and The Internet**, New York: Routledge Publishing.

Kaminski, Ryan T. (2010), "Escaping The Cyber State of Nature: Cyber Deterrence and International Institutions", **Conference on Cyber Conflict Proceedings**, 1. Baskı *içinde* (79-94), Tallinn:CCD COE Publications.

Karabulut, Bilal (2015), **Güvenlik: Küreselleşme Sürecinde Güvenliği Yeniden Düşünmek**, Ankara: Barış Kitabevi.

Kaspersky Lab. (2015), "Kaspersky Security Bulletin", https://securelist.com/files/2015/12/Kaspersky-Security-Bulletin2015_FINAL_EN.pdf (13.07.2016).

Keleştemur, Atalay (2015), **Siber İstihbarat**, İstanbul: Level Kitap.

Kesler, Brent (2011), "The Vulnerability of Nuclear Facilities to Cyber Attacks", **Strategic Insights**, 10(1), 15-25.

Kılıç, Şükrü Oktay (2015), "Panama Belgelerinin Yaptığı Etki Şaşırtıcı", **Aljazeera Turk**, http://www.aljazeera.com.tr/al-jazeera-ozel/panama-belgelerinin-yarattigi-etki-sasirtici (09.05.2016).

Kırdı, Gökhan (2015), "Türkiye'de ve Dünyada Siber Güvenlik Alanında Yapılan Çalışmalar",**SASAM**,http://sahipkiran.org/2015/01/14/siber-guvenlik/(02.02.2016).

Kilroy, Richard J. (2008), "The U.S. Military Response to Cyber Warfare", Lech J. Janczewski ve Andrew M. Colarik (Ed.), **Cyber Warfare and Cyber Terrorism**, 1. Baskın *içinde* (439-445), Hershey: Information Science Reference.

Klimburg, Alexander ve Healey, Jason (2012), "Strategic Goals & Stakeholders", Alexander Klimburg (Ed.), **National Cyber Security: Framework Manual**, 1. Baskı *içinde* (66-107), Tallinn, NATO CCD COE Publication.

Knutsen, Torbjon L. (2006), **Uluslararası İlişkiler Teorisi Tarihi**, İstanbul: Açılım Kitap.

Kolojziej, Edward A. (2005), **Security and International Relations**, Cambridge: Cambridge University Press.

Krebs, Brian (2009), "Cyber Security Community Joins Forces to Defeat Conficker Worm", **The Washington Post**, http://www.csl.sri.com/users/porras/public/WP-Conficker-2-13-09.pdf (10.02.2016).

Krickovic, Andrej (2016), "Catalyzing Conflict: The Internal Dimension of the Security Dilemma", **Journal of Global Security Studies,** 1(2), 111-126.

Kurki, Milja (2008), **Causation in International Relations: Reclaiming Causal Analysis**, Cambridge, Cambridge University Press.

Kurtdarcan, Bleda ve Mumcu, Özgür (2014), **Geleceğin Savaşları ve Silahları: Yeni Silah Teknolojilerinin Silahlı Çatışmalar Hukuku Işığında İncelenmesi**, Ankara: Umag Vakfı Yayınları.

Ladani, Behrouz Tork ve Berenjkoub Mehdi (2006), **A Comparative Study on National Information Security Strategies in Finland, US and Iran,** http://engold.ui.ac.ir/~ladani/Papers/2006/WITID06-Comparison.pdf (14.01.2016).

Libicki, Martin C. (2007), **Conquest in Cyberspace: National Security and Information Warfare**, Cambridge: Cambridge University Press.

——————— (2009), **Cyberdeterrence and Cyberwar**, Santa Monica: Rand Corporation.

Lindstrom, Gustav ve Luiijf, Eric (2012), "Political Aims & Policy Methods", Alexander Klimburg (Ed.), **National Cyber Security: Framework Manual**, 1. Baskı *içinde* (44-66), Tallinn, NATO CCD COE Publication.

Little, Richard (2007), **The Balance of Power in International Relations: Metaphors, Myths and Models**, Cambridge: Cambridge University Press.

Lupovici, Amir (2011), "Cyber Warfare and Deterrence: Trends and Challenges in Research", **Military and Strategic Affairs**, 3(3), 49-62.

Lutz, James M. ve Lutz, Brenda J (2008), **Global Terrorism**, New York: Roudledge Publishing.

McAfee Labs (2015), "Threat Report, August 2015", http://www.mcafee.com/mx/resources/reports/rp-quarterly-threats-aug-2015.pdf (11.02.2016).

——————— (2015), "Threats Report, May 2015", http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q1-2015.pdf (10.02.2016).

McQuade, Samuel C. (2009), **Encyclopedia of Cybercrime**, London: Greenwood Press.

McSweeney, Bill (1999), Security, Identity and Interests, Cambridge, Cambridge University Press.

Melzer, Nils (2011), "Cyberwarfare and International Law", **Ideas for Peace and Security**, http://unidir.org/files/publications/pdfs/cyberwarfare-and-international-law-382.pdf (08.13.2016).

Merrick, Kathryn ve diğerleri (2016), "A Survey of Game Theoretic Approaches to Modelling Decision-Making in Information Warfare Scenarios", **Future Internet**, 8 (3), 1-29.

Meulen, Nicole van der ve diğerleri (2015), **Cybersecurity in The European Union and Beyond: Exploring The Threats and Policy Responses**, Brussels: European Parliament.

Mintz, Alex ve DeRouen, Karl (2010), **Understanding Foreign Policy Decision Making**, Cambridge, Cambridge University Press.

Morgenthau, Hans (2004), "'The Balance of Power','Different Methods of The Balance of Power' and 'Evaluation of The Balance of Power' from Politics Among Nations: The Struggle for Power and Peace", Karen A. Mingst ve Jack L. Snyder (Ed.), **Essential Readings in World Politics**, 2. Baskı *içinde* (124-130), New York: Norton Publishing.

Nath, Sanghamitra (2012), "What Military Deterrence Can not Do, Cyber Deterrence Can Do to Iran: Exploring The Implications of Manipulative Incessant Usage of The Term 'Pre- Emptive'", **International Journal of Social Sciences and Humanity Studies**, 4(1), 313-323.

Nye, Joseph S. (2010), **Cyber Power**, Cambridge: Harvard Kennedy School, Belfer Center for Science and International Affairs.

Nye, Joseph S. ve Welch, David A. (2009), **Küresel Çatışmayı ve İşbirliğini Anlamak**, (Çev. Renan Akman), İstanbul: Türkiye İş Bankası Kültür Yayınları.

O'Connell, Mary Ellen (2012), "Cyber Security without Cyber War", **Journal of Conflict & Security Law**, 17(2), 187-209.

Öğün, Mehmet Nasip ve Kaya, Adem (2013), "Siber Güvenliğin Milli Güvenlik Açısından Önemi ve Alınabilecek Tedbirler", **Güvenlik Stratejileri Dergisi**, 9(18), 145-181.

Önen, Nilüfer (2015), "Küreselleşme Ekseninde Değişen Güvenlik Algısı", **Akademik Perspektif**, http://akademikperspektif.com/2015/03/16/kuresellesme-ekseninde-degisen-guvenlik-algisi/ (10.04.2016).

Özçelik, Sezai (2012), "Önleyici Diplomasi Pratiği ve Teorisi", Mustafa Aydın ve diğerleri (Ed.), **Uluslararası İlişkilerde Çatışmadan Güvenliğe**, Baskı *içinde* (429-445), İstanbul: İstanbul Bilgi Üniversitesi Yayınları.

Özdemir, Haluk (2008), "Uluslararası İlişkilerde Güç: Çok Boyutlu Bir Değerlendirme" **Ankara Üniversitesi SBF Dergisi**, 63(3), 113-144.

Paganini, Pierluigi (2012a), "US Cybersecurity Capability: National Preparedness Report", **INFOSEC Island**, http://www.infosecisland.com/blogview/21241-US-Cybersecurity-Capability-National-Preparedness-Report-.html (10.07.2016).

——————— (2012b), "The Rise of Cyber Weapons and Relative Impact on Cyberspace", **INFOSEC Institute**, http://resources.infosecinstitute.com/the-rise-of-cyber-weapons-and-relative-impact-on-cyberspace/ (14.07.2016).

Paker, Evren Balta (2012), **Küresel Güvenlik Kompleksi: Uluslararası Siyaset ve Güvenlik**, İstanbul: İletişim Yayıncılık.

Passeri, Paolo (2016), "June 2016 Cyber Attacks Statistics", **Hackmageddon Information Security Timelines and Statistics**, http://www.hackmageddon.com/2016/07/25/16-30-june-2016-cyber-attacks-statistics/ (03.06.2016).

Peterson, Dale (2013), "Offensive Cyber Weapons: Construction, Development and Employment", **Journal of Strategic Studies**, 36(1), 120-124).

Platform (2015), "Internet Security Report Shows Spike in Cyber Threats", https://www.ncta.com/platform/broadband-internet/internet-security-report-shows-spike-in-cyber-threats/ (09.05.2016).

Ponemon Institute (2014), "2014 Best Schools for Cybersecurity", http://www.ponemon.org/local/upload/file/2014%20Best%20Schools%20Report%20FINAL%202.pdf (06.02.2016).

——————— (2015a), "2015 Cost of Cyber Crime Study: Global", http://www.ponemon.org/blog/2015-cost-of-cyber-crime-united-states (06.02.2016).

——————— (2015b), "2015 Cost of Cyber Crime Study: United Kingdom", http://cybersecuritysummit.co.uk/wp-content/uploads/2015/06/2015-UK-CCC-FINAL-3.pdf (01.02.2016).

Pizzi, Michael (2014), "Cyberwarfare Greater Threat to US than Terrorism, Say Security Experts", **Aljazeera America**, http://america.aljazeera.com/articles/2014/1/7/defense-leaders-saycyberwarfaregreatestthreattous.html (10.12.2015).

Rawnsley, Gary D. (2008), "The Laws of The Playground: Information Warfare and Propaganda Across The Taiwan Strait", Athina Karatzogianni (Ed.), **Cyber Conflict and Global Politics**, 1. Baskı *içinde* (79-94), London: Routledge Chapman Hall.

Renard, Thomas (2014), **The Rise of Cyber-Diplomacy: The EU, Its Strategic Partners and Cyber-Security**, Working Paper 7, Madrid: European Strategic Partnerships Observatory.

Rid, Thomas ve McBurney, Peter (2012), "Cyber Weapons", **The RUSI Journal**, 157(1), 6-13.

Rosecrance, Richard ve Steiner, Zara (2010), "History and Neorealism Reconsidered", Ernest R. May ve diğerleri (Ed.), **History and Neorealism**, 1. Baskı *içinde* (341-365), Cambridge: Cambridge University Press.

Roskin, Michael G. ve Berry, Nicholas O. (2014), **Uluslararası İlişkiler, Uİ'nin Yeni Dünyası**, (Çev. Özlem Şimşek), Ankara: Adres Yayınları.

Rupert, Mark (2007), "Marxism", Martin Griffiths (Ed.), **International Relations Theory for The Twenty-First Century: An Introduction**, 1. Baskı *içinde* (35-47), New York: Routledge Publishing.

Sabillon, Regner ve diğerleri (2016), "National Cyber Security Strategies: Global Trends in Cyberspace", **International Journal of Computer Science and Software Engineering**, 5(5), 67-81.

Sandvik, Kristin Bergtora (2012), "Cyberwar as an Issue of International Law", **Prio Policy Brief**, Volume 4, 1-4.

Sard, Michael (2014), "Cyber-Politics: The Technological Arms Race between States and Citizens", **Eurasia Group**, https://www.pwc.com/jp/en/japan-knowledge/archive/assets/pdf/cyber-politics-1408.pdf (14.06.2016).

Saygılı, İsmail (2015), **Siber Suç Coğrafyası – 2014'te neler yaşandı?**, http://h4cktimes.com/analiz-makaleler/siber-suc-cografyasi-2014te-neler-yasandi.html (12.11.2015).

Schalhoub, Zeinab Karake ve Al Qasimi, Sheikha Lubna (2010), **Cyber Law and Cyber Security in Developing and Emerging Economies**, Cheltenham: Edward Elgar Publishing.

Scheuerman, William E. (2007), "Carl Schmitt and Hans Morgenthau: Realism and Beyond", Michael C. Williams (Ed.), **Realism Reconsidered: The Legacy of Hans Morgenthau in International Relations**, 1. Baskı *içinde* (62-92), Oxford: Oxford University Press.

Schmitt, Michael N. (2010), "Cyber Operations in International Law: The Use of Force, Collective Security, Self-Defense and Armed Conflicts", **Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy**, 1. Baskı *içinde* (151-178), The National Academies.

Schmitt, Michael N. (2012), "International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed", **Harvard International Law Journal**, Volume 54, 13-37.

Schmitt, Michael N. ve Vihul Liis (2014), "The Nature of International Law Cyber Norms", **The Tallinn Papers**, Paper No. 5, Special Expanded Issue.

Shaw, Malcom N. (2008), **International Law**, 6th Edition, Cambridge: Cambridge University Press.

Singer, J. David (1979), **The Correlates of War**, New York: Free Press.

Singer, P.W. ve Friedman, Allan (2015), **Siber Güvenlik ve Siber Savaş**, (Çev. Ali Atav), Ankara: Buzdağı Yayınları.

Smith, Steve ve diğerleri (1994), Strategic Studies and World Order, Cambridge, Cambridge University Press.

Sönmezoğlu, Faruk (2000), **Uluslararası Politika ve Dış Politika Analizi**, İstanbul: Filiz Kitabevi.

——————— (2014), **Uluslararası Politika ve Dış Poltiika Analizi**, 6. Baskı, Der İstanbul: Der Yayınları.

Spidalieri, Franesca (2015), "State of The States on Cybersecurity", **Salve Regina University Pell Center**, http://pellcenter.org/wp-content/uploads/2015/11/Pell-Center-State-of-the-States-Report.pdf (12.05.2016).

Stevens, Tim (2012), "A Cyberwar of Ideas? Deterrence and Norms in Cyberspace", **Contemporary Security Policy**, 33(1), 148-170.

STM (2016), "Türkiye Siber Tehdit Durumu Raporu", https://www.stm.com.tr/yayinlar/2016-SG/2016-turkiye-raporu.html (06.04.2016).

Stone, Alec (1994), "What is Supranational Constitution? An Essay in International Relations Theory" **The Review of Politics**, 56(3), 441-474.

Stone, John (2012), "Cyber War will Take Place", **Journal of Strategic Studies**, 36(1), 101-108.

Tang, Shiping (2009), "The Security Dilemma: A Conceptual Analysis", **Security Studies**, 18(3), 587-623.

Taytaş, Firuze (2016), **Türkiye Cumhuriyeti Siber Silah Geliştirmeli mi?**, https://www.linkedin.com/pulse/türkiye-cumhuriyeti-siber-silah-geliştirmeli-mi-firuze-taytaş (25.04.2016).

The Statistics Portal (2016a), "Amount of Monetary Damage Caused by Reported Cyber Crime to the IC3 from 2001 to 2015", http://www.statista.com/statistics/267132/total-damage-caused-by-by-cyber-crime-in-the-us/ (03.05.2016).

——————— (2016b), "Average Annual Costs Caused by Cyber Crime in the United States as of August 2015, by Industry Sector", http://www.statista.com/statistics /193436/average-annual-costs-caused-by-cyber-crime-in-the-us/ (02.07.2016).

The Texas Politics Project (2016), "Policy Making and Policy Implementation", https://texaspolitics.utexas.edu/archive/html/bur/features/0303_01/policy.html (09.06.2016).

Ting, Teo Jing (2015), **Never Take Our Peace for Granted: Dr Ng**, https://www.mindef.gov.sg/imindef/resourcelibrary/cyberpioneer/topics/articles/news/2015/mar/05mar15_news.html#.V6wveGXwyuV (06.03.2016).

Toptaş, Ergüder (2009), **21. Yüzyılda Savaş**, Ankara: Kripto Yayınları.

Trend Micro Incorporated (2015), "Report on Cybersecurity and Critical Infrastructure in the Americas", http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/rep orts/critical-infrastructures-west-hemisphere.pdf (03.04.2016).

Turgut, Arzu (2011), "Wikileaks belgelerinde Türkiye ve Yakın Çevresi: Türkiye, Rusya, Güney Kafkasya ve Orta Doğu ile İlgili Belgeler", **USAK Raporları**, Rapor No: 11-03, Ankara: USAK Yayınları.

Türkiye Cumhuriyeti Ulaştırma Denizcilik ve Haberleşme Bakanlığı (t.y.), "2013-2014 Siber Güvenlik Eylem Planı", http://www.udhb.gov.tr/doc/siberg/SOME_2013-2014_EylemPlani.pdf (08.09.2015).

United States Government Accountability Office (2010), **Briefing to the Subcommittee on Terrorism: Unconventional Threats and Capabilities**, Washington DC: Committee on Armed Services, House of Representatives.

URL, "İngiltere'nin Yeni Ulusal Güvenlik Yaklaşımı" (t.y.), http://www.mgk.gov.tr/calismalar/calismalar/006_ingilterenin_yeni_guvenlik_yaklasimi.pdf (04.03.2016).

Varlık, Ali Bilgin (2013), "Savaşı Tanımlamak, Terminolojik Bir Yaklaşım", **Avrasya Terim Dergisi**, 1(2), 114-129.

Vasquez, John A. (2015), **Savaş Bulmacası**, (Çev. Haluk Özdemir), İstanbul: Uluslararası İlişkiler Kütüphanesi Yayınları.

Vellone, Luigi (2006), "From Data to Knowledge: How Intelligence and Security Tools can Help", Fernando Duarte Carvalho ve Eduardo Mateus da Silva (Ed.), **Cyberwar-Netwar: Security in The Information Age**, 1. Baskı *içinde* (115-130), Amsterdam: IOS Press.

Vinnakota T. (2013), "Understanding of Cyberspace Using Cybernetics: An Imperative need for Cybersecurity of Enterprises", **IEEEXplore**, http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6865791 (18.01.2016).

Viotti, Paul R. ve Kauppi, Mark V. (2014), **Uluslararası İlişkiler ve Dünya Siyaseti**, (Çev. Ayşe Özbay Erozan), Ankara: Nobel Yayıncılk.

Walker, R.B.J. (2007), "Secuirty, Sovereignty and The Challenge of World Politics", Barry Buzan ve Lene Hansen (Ed.), **International Security Volume II: The Transition to The Post-Cold War Security Agenda**, 1. Baskı *içinde* (146-166), London: SAGE Publications.

Wallace, Ian (2014), "Ulusal Siber Güvenlik Stratejilerinin Geliştirilmesi", **Analist**, http://www.analistdergisi.com/sayi/2014/06/ulusal-siber-guvenlik-stratejilerinin-gelistirilmesi (13.12.2015).

Wallerstein, Immanuel (2004), "The Rise and Future Demise of the World Capitalist System: Concepts for Comparative Analysis", Karen A. Mingst ve Jack L. Snyder (Ed.), **Essential Readings in World Politics**, 2. Baskı *içinde* (130-138), New York: Norton Publishing.

——————— (2011), **Dünya Sistemleri Analizi: Bir Giriş**, 2011, (Çev. Ender Abadoğlu ve Nuri Ersoy), İstanbul: Bgst Yayıncılık.

Walt, Stephen M. (2003), "Güvenlik Çalışmalarının Rönesansı", **Avrasya Dosyası**, 9(2), 71-107.

——————— (2004), "International Relations: One World, Many Theories", Karen A. Mingst ve Jack L. Snyder (Ed.), **Essential Readings in World Politics**, 2. Baskı *içinde* (4-11), New York: Norton Publishing.

Waltz, Kenneth (1959), **Man, The State and The War: A Theoretical analysis**, New York: Columbia University Press

Weber, Cynthia (2010), **International Relations Theory: A Critical Introduction**, 3rd Edition, New York: Routledge Publishing.

Wiener, Norbert (1948), **Cybernetics, or Control and Communication in the Animal and the Machine**, Cambridge: MIT Press.

Williams Michael (2005), **The Politics of Risk: The US, Europe and Proactive Security in the 21st Century**, http://citation.allacademic.com/meta/p_mla_apa_research_citation/ 0/7/1/0/6/pages71061/p71061-1.php (09.08.2016).

World Economic Forum (2016), "The Global Risks Report 2016, 11th Edition", http://wef.ch/risks2016 (11.08.2016).

Yayla, Mehmet (2013), "Uluslararası Hukukta Siber Saldırılara Karşı Kuvvet Kullanma", **TBB Dergisi**, Sayı 107, 199-220.

Yeşilyurt, Hamdi (2015), "Ulusal Güvenlik Perspektifinde Siber Güvenlik", Fatih Tombul ve diğerleri (Ed.), **Siber Suçlar: Tehditler, Farkındalık ve Mücadele**, 1. Baskı *içinde* (169-195), Ankara: Global Politika ve Strateji Yayınları.

Yılmaz, Sait (2006), **21. Yüzyılda Güvenlk ve İstihbarat**, İstanbul: Alfa yayınları.

——————— (2012), "Uluslararası Müdahele ve Meşruiyet", **21. Yüzyıl Türkiye Enstitüsü**, http://www.21yyte.org/tr/arastirma/politik-sosyal-kulturel-arastirmalar-merkezi/2012/03/01/6512/uluslararasi-mudahale-ve-mesruiyet (12.11.2015).

——————— (2014), **Uzay Güvenliği**, İstanbul: Milenyum Yayınları.

——————— (2015), **Dünyanın Çivisi Neden Çıktı?**, http://www.ulusalkanal.com.tr/dunyanin-civisi-neden-cikti-makale,5016.html (17.05.2016)

——————— (2016), **Savaş ve General**, http://www.ulusalkanal.com.tr/savas-ve-general-makale,5307.html (19.05.2016).

Yılmaz, Sait ve Salcan, Olay (2008), **Siber Uzay'da Güvenlik ve Türkiye**, İstanbul: Milenyum Yayınları.

Yılmaz, Seda ve Sağıroğlu, Şeref (2013a), "Siber Güvenlik Risk Analizi, Tehdit ve Hazırlık Seviyeleri", **6. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı Bildiriler Kitabı**, 1. Baskı *içinde* (158-166), Ankara: Bilgi Güvenliği Derneği.

——————— (2013b), "Siber Saldırı Hedefleri ve Türkiye'de Siber Güvenlik Stratejisi", **6. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı Bildiriler Kitabı**, 1. Baskı *içinde* (323-331), Ankara: Bilgi Güvenliği Derneği.

Yılmaz, Sefer (2011), "11 Eylül Sonrasında ABD ve Türkiye'deki İç Güvenlik Yeniden Yapılanmalarının Karşılaştırılması", **Ç.Ü. Sosyal Bilimler Enstitüsü Dergisi**, 20(3), 361-380.

Yorulmaz, Murat (2014), "Değişen Uluslararası Güvenlik Algılamaları Bağlamında Türkiye-Yunanistan İlişkilerinde Değişmeyen Güvenlik Paradoksu", **Balkan Araştırma Enstitüsü Dergisi**, 3(1), 103-135.

Zagare, Frank C. ve Kilgour, D. Marc (2000), **Prefect Deterrence**, Cambridge, Cambridge University Press.

ÖZGEÇMİŞ

Vahit GÜNTAY, 20.12.1984 tarihinde Kırşehir'de doğdu. İlköğrenimini Mucur Hürriyet İlkokulu'nda, orta öğrenimini Kırşehir Hacı Fatma Erdemir Anadolu Lisesi'nde, lisans eğitmini ise 2004-2008 yılları arasında Gazi Üniversitesi, İktisadi ve İdari Bilimler Fakültesi, Uluslararası İlişkiler Bölümü'nde tamamladı. 2009 yılında Karadeniz Teknik Üniversitesi, Sosyal Bilimler Enstitüsü, Uluslararası İlişkiler Anabilim Dalı'nda başladığı yüksek lisans eğitimini 2012 yılında *"Türk Dış Politikasında Güncel Yaklaşımlar ve Eksen Kayması Tartışmaları (2002-2012)"* başlıklı teziyle tamamladı.

GÜNTAY, 2009 yılından beri Karadeniz Teknik Üniversitesi, İktisadi ve İdari Bilimler Fakültesi, Uluslararası İlişkiler Anabilim Dalında araştırma görevlisi olarak görev yapmaktadır. Yurtiçi ve yurtdışında siber güvenlik ile ilgili birçok farklı çalışmaya ve projeye katkı sağlamıştır. Yabancı dillere de ilgili olan GÜNTAY iyi derecede İngilizce, orta düzeyde Almanca ve İspanyolca, başlangıç düzeyinde Rusça ve Çince bilmektedir.