T.C.
KARA HARP OKULU
SAVUNMA BİLİMLERİ ENSTİTÜSÜ
GÜVENLİK BİLİMLERİ ANABİLİM DALI

ASİMETRİK TEHDİT KAVRAMI BAĞLAMINDA, 11 EYLÜL 2001 SONRASI DÖNEMDE AMERİKA BİRLEŞİK DEVLETLERİ'NDEKİ SİBER TEHDİT ALGILAMASININ VE GELİŞTİRİLEN GÜVENLİK POLİTİKALARININ İNCELENMESİ

YÜKSEK LİSANS TEZİ

Hazırlayan
Murat DEMİREL

Tez Danışmanı
Yrd.Doç.Dr. Muammer KETİZMEN

ANKARA – 2012

TEZ TANITIM FORMU

TEZİN TARİHİ : 28.06.2012

TEZİN TİPİ : Yüksek Lisans Tezi

TEZİN BAŞLIĞI : Asimetrik Tehdit Kavramı Bağlamında, 11 Eylül 2001 Sonrası Dönemde Amerika Birleşik Devletleri'ndeki Siber Tehdit Algılamasının ve Geliştirilen Güvenlik Politikalarının İncelenmesi

TEZİN YAPILDIĞI BİRİM : Kara Harp Okulu Savunma Bilimleri Enstitüsü Güvenlik Bilimleri Anabilim Dalı

SPONSOR KURULUŞ : –

DAĞITIM LİSTESİ : Kara Harp Okulu Savunma Bilimleri Enstitüsü Tez Hazırlama, Onay, Dağıtım ve Muhafaza Esasları Kılavuzunda belirtilen yerlere

TEZİN ÖZETİ : 11 Eylül 2001 tarihinde ABD hedeflerine yönelik düzenlemiş olan terör saldırıları, ABD kamuoyunda özellikle asimetrik tehditlere ilişkin olarak önceden var olan ulusal güvenlik kaygılarını ciddi bir biçimde kuvvetlendirmiştir. 11 Eylül Saldırıları sonrasındaki süreçte; bir yandan mevcut ulusal güvenlik yapılanmasının sahip olduğu yetkileri ciddi biçimde arttıran "ABD Vatanseverlik Yasası (USA PATRIOT Act)" ve "İç Güvenlik Yasası (HSA)" gibi kanunlar yürürlüğe konulurken, diğer yandan bahse konu ulusal güvenlik yapılanması, İç Güvenlik Bakanlığı (DHS)'nın ortaya çıkışı örneğinde olduğu gibi, asimetrik tehditleri ABD içerisinde de karşılayabilecek biçimde federal seviyede yeniden şekillendirilmiştir.

ANAHTAR KELİMELER : Siber Güvenlik, Asimetrik Tehdit, 11 Eylül Saldırıları, ABD Vatanseverlik Yasası, İç Güvenlik Yasası, Kritik Altyapı Güvenliği.

SAYFA SAYISI : 182

GİZLİLİK DERECESİ : Tasnif Dışı

T.C.
KARA HARP OKULU
SAVUNMA BİLİMLERİ ENSTİTÜSÜ
GÜVENLİK BİLİMLERİ ANABİLİM DALI

ASİMETRİK TEHDİT KAVRAMI BAĞLAMINDA, 11 EYLÜL 2001 SONRASI DÖNEMDE AMERİKA BİRLEŞİK DEVLETLERİ'NDEKİ SİBER TEHDİT ALGILAMASININ VE GELİŞTİRİLEN GÜVENLİK POLİTİKALARININ İNCELENMESİ

YÜKSEK LİSANS TEZİ

Hazırlayan
Murat DEMİREL

Tez Danışmanı
Yrd.Doç.Dr. Muammer KETİZMEN

ANKARA – 2012

KARA HARP OKULU

SAVUNMA BİLİMLERİ ENSTİTÜSÜ MÜDÜRLÜĞÜNE

Murat DEMİREL'in, "Asimetrik Tehdit Kavramı Bağlamında, 11 Eylül 2001 Sonrası Dönemde Amerika Birleşik Devletleri'ndeki Siber Tehdit Algılamasının ve Geliştirilen Güvenlik Politikalarının İncelenmesi" konulu tez çalışması, jürimiz tarafından GÜVENLİK BİLİMLERİ Anabilim Dalında YÜKSEK LİSANS tezi olarak kabul edilmiştir.

Başkan ----------
Yrd.Doç.Dr. Muammer KETİZMEN
(Danışman)

Üye ----------
Yrd.Doç.Dr.Mu.Bnb. Olgun DEĞİRMENCİ

Üye ----------
Dr.J.Yb. Gökhan SARI

ONAY

Yukarıdaki imzaların, adı geçen öğretim üyelerine ait olduğunu onaylarım.

25. / 07 / 2012

Ali IŞIK
Yrd.Doç.Dr.Öğ.Alb.
Svn.Bil.Enst.Md. V.

TEŞEKKÜR

11 Eylül 2001 tarihinde ABD hedeflerine yönelik olarak gerçekleştirilen terörist saldırıların ardından, asimetrik tehdit kavramı bağlamında ABD'de ortaya çıkan siber tehdit algısına ve geliştirilen siber güvenlik politikalarına ilişkin olarak yapmış olduğum tez çalışmasında; fikir ve eleştirileri ile bana yol gösterici olan tez danışmanım Yrd.Doç.Dr. Muammer KETİZMEN'e; başta Kara Harp Okulu Komutanı Tümgeneral Ferit GÜLER, Savunma Bilimleri Enstitüsü Müdürü Yrd.Doç.Dr.Öğ.Alb. Ali IŞIK ve Güvenlik Bilimleri Anabilim Dalı Başkanı Dr.J.Yb. Gökhan SARI ve personeli olmak üzere, tüm Savunma Bilimleri Enstitüsü çalışanlarına ve tez savunmamda yer alan jüri üyesi Yrd.Doç.Dr.Mu.Bnb. Olgun DEĞİRMENCİ'ye son derece değerli destek ve katkılarından dolayı teşekkürlerimi sunmayı bir borç bilirim.

T.C.
KARA HARP OKULU
SAVUNMA BİLİMLERİ ENSTİTÜSÜ
GÜVENLİK BİLİMLERİ ANABİLİM DALI
ANKARA 2012

ASİMETRİK TEHDİT KAVRAMI BAĞLAMINDA, 11 EYLÜL 2001 SONRASI DÖNEMDE AMERİKA BİRLEŞİK DEVLETLERİ'NDEKİ SİBER TEHDİT ALGILAMASININ VE GELİŞTİRİLEN GÜVENLİK POLİTİKALARININ İNCELENMESİ

YÜKSEK LİSANS TEZİ

Murat DEMİREL

ÖZET

İletişim ve enformasyon teknolojilerini kullanan cihazların hayatımızın vazgeçilmez bir parçası haline geldiği günümüzde, ortaya çıkan her yeni teknolojik gelişme, insanlık tarihinin önceki dönemlerinde de olduğu gibi hem hayatı kolaylaştırıcı yeni fırsatlar, hem de bu fırsatların art niyetli kullanımından doğan yeni tehditler yaratmaktadır.

Günümüz dünyasında oldukça sık karşılaşılan, "enformasyon" olarak tanımlanan ve daha ziyade 21.nci Yüzyıla özgü olarak algılanan yeni bilgi türü; Francis Bacon'un *"Bilgi Güç'tür"* sözünde ifade edildiği haliyle, yalnızca karşı zeka üzerinde basit bir üstünlük kurma aracı olmanın ötesine geçmiştir. Bu yeni bilgi türü, somutlaştığı elektronik sistemler ve onların dilindeki ifadesi olan "veri" kimliği ile, bilginin önceki tanımlarından ve işlevlerinden çok daha fazlasını ifade etmektedir.

"Küreselleşme", "postmodernite" ve "dördüncü nesil savaş" olgularının bir araya gelmesinden doğan politik-sosyal-askeri

yoğunlaşma'nın sinerjik karakteri ise; gerek ulusal, gerekse de uluslararası seviyedeki güvenlik aktörleri ile onların politika ve stratejilerinden oluşan varsayımsal bir çevre olan "güvenlik uzayı"nı uzun vadeli ve kökten bir şekilde değiştirmektedir. Bu değişimde başrolü oynayan olguların doğaları ve ortaya çıkardıkları değişimlerin karakteristikleri göz önüne alındığında; ulusal güvenlik karar alıcılarının algılamalarında, asimetrik savaş ve onun politik bir türevi olarak terörizmin, güç kazanan güvenlik tehditleri olarak ön plana çıktıkları görülmektedir. Enformasyon teknolojilerindeki hızlı ve kesintisiz gelişimin yanı sıra 11 Eylül Saldırıları gibi güvenlik tehditlerindeki yadsınamayacak gerçekleşmeler ise, hızlandırıcı mahiyetteki tali dinamikler olarak bu değişim sürecine dahil olmaktadırlar. Bu çerçevede, arka planda çalışan söz konusu asli ve tali dinamiklerin nihai birer ürünü olarak; gerek "siber uzay", gerekse de onun güvenliğini sağlama kaygısını yansıtan "siber güvenlik" kavramlarıyla günlük hayatta çok daha sık bir biçimde karşılaşılmaktadır.

ABD'nin İkinci Dünya Savaşı'na girmesine yol açan Pearl Harbor Saldırısı ile sıklıkla kıyaslanan, 11 Eylül 2001 tarihinde ABD hedeflerine yönelik olarak düzenlemiş olan terör saldırıları, ABD kamuoyunda özellikle asimetrik tehditlere ilişkin olarak önceden var olan ulusal güvenlik kaygılarını ciddi bir biçimde kuvvetlendirmiştir. 11 Eylül Saldırıları sonrasındaki süreçte; bir yandan mevcut ulusal güvenlik yapılanmasının sahip olduğu yetkileri ciddi biçimde arttıran "ABD Vatanseverlik Yasası (USA PATRIOT Act)" ve "İç Güvenlik Yasası (HSA)" gibi kanunlar yürürlüğe konulurken, diğer yandan bahse konu ulusal güvenlik yapılanması, İç Güvenlik Bakanlığı (DHS)'nın ortaya çıkışı örneğinde olduğu gibi, asimetrik tehditleri ABD içerisinde de karşılayabilecek biçimde federal seviyede yeniden şekillendirilmiştir.

Bu süreç içerisinde sürekli olarak daha da fazla önem kazanmış olan "siber güvenlik" olgusu ise; "enformasyon operasyonları" ve "asimetrik tehdit" odaklı olarak ABD'de ortaya çıkan yeni güvenlik algı ve yapısı içerisinde, özellikle iletişim, enformasyon ve enerji

sektörlerindeki kritik altyapı tesislerinin, gerek fiziksel, gerekse de sanal varlıklarının korunmasına odaklanan çabaları içermektedir.

Herhangi bir hipotez geliştirme kaygısı taşımayan bu çalışma, bir durum ve olgu tespiti niteliğinde olup; 11 Eylül Saldırıları sonrasında, asimetrik tehdit bağlamında ABD'de ortaya çıkmış olan siber güvenlik algısının genel bir resmini ortaya koymaya çalışmaktadır.

Anahtar Kelimeler : Siber Güvenlik, Asimetrik Tehdit, 11 Eylül Saldırıları, ABD Vatanseverlik Yasası, İç Güvenlik Yasası, Kritik Altyapı Güvenliği.

Tez Yöneticisi : Yrd.Doç.Dr. Muammer KETİZMEN

Sayfa Sayısı : 182

T.R.
TURKISH MILITARY ACADEMY
DEFENSE SCIENCES INSTITUTE
SECURITY SCIENCES DEPARTMENT
ANKARA 2012

ANALYSIS OF CYBER THREATS PERCEPTION AND CYBERSECURITY POLICIES DEVELOPED IN THE UNITED STATES WITHIN THE PERIOD AFTER SEPTEMBER 11TH, 2001 IN THE CONTEXT OF ASYMMETRIC THREAT CONCEPT

MASTER'S THESIS

Murat DEMİREL

ABSTRACT

Nowadays, during which devices based on communication and information technologies have become an indispensable part of our lives, each new technological development creates not only new opportunities to make life easier, but also new threats arising from malevolent use of these opportunities as in previous eras of human history.

Frequently encountered in today's world, the new kind of knowledge, defined as "information" and perceived more often as peculiar to the 21st Century, has transcended becoming just a simple apparatus for establishing a superiority over rival intelligence as in Francis Bacon's famous expression, "Knowledge is Power". This new kind of knowledge implies much more than previous definitions and functions of knowledge through the electronic systems that concretize it and the identity of "data" as its expression in the language of electronic systems.

In the long term, the synergic character of political-social-military concentration, which arised from the aggregation of "globalization", "postmodernity" and "fourth generation warfare", has fundamentally changed "security space" as a hypothetical enviroment that is consisting of security actors in both national and international level, and their policies and strategies. When the intrinsic characteristics of the phenomena, which play key roles in this transformation, are considered; it is realized that asymmetric warfare and terrorism as a political derivative of it stand out as security threats that have been gaining strength in the perceptions of national security decision makers. Besides the rapid and incessant development of information technologies, the undeniable occurrences of security threats -- as in the case of the September 11 Attacks -- involve to this transformation period as secondary dynamics that accelerate process. In this frame, as the final products of the primary and secondary dynamics run in the background, it is more often in daily life to come upon the concepts of "cyberspace" and "cybersecurity" which reflects the concern of ensuring the security of cyberspace.

Held on the 11th of September 2001 against the U.S. targets, the terrorist attacks, often compared with the Attack on Pearl Harbor that led the United States go to the Second World War, strengthened seriously the existing national security concerns of the U.S. public particularly against the asymmetric threats. In the period after the September 11 Attacks, on the one hand, some laws -- such as "USA PATRIOT Act" and "Homeland Security Act (HSA)" -- which seriously increased the existing authorities of the national security structure -- were enacted; on the other hand, as in the case of the emergence of Department of Homeland Security (DHS), the national security structure was reshaped at the federal level against the asymmetric threats within the United States.

The phenomenon of cybersecurity, which has steadly gained more importance within this process, contains the efforts that focus on

the protection of both physical and virtual existences of critical infrastructure -- particularly in communication, information and energy sectors -- within the frame of new security perception and structure that emerged focusing on "the information operations" and "the asymmetric threat" in the United States.

Without any concern for developing any hypothesis, this study as a determination of situations and phenomena tries to manifest the panorama of the cybersecurity perception in the context of asymmetric threats, emerged in the United States after the September 11 Attacks.

Keywords : Cybersecurity, Asymmetric Threat, the September 11 Attacks, USA PATRIOT Act, Homeland Security Act, Critical Infrastructure Security.

Advisor : Assoc.Prof. Muammer KETIZMEN

Number of Pages : 182

İÇİNDEKİLER

TEŞEKKÜR i
ÖZET ii
ABSTRACT v
İÇİNDEKİLER viii
KISALTMALAR LİSTESİ xii
ÖN SÖZ xviii
GİRİŞ 1

BİRİNCİ BÖLÜM
KAVRAMSAL VE KURAMSAL ÇERÇEVE

1. KAVRAMSAL ÇERÇEVE 13
   a. Küreselleşme, Postmodernite ve Dördüncü Nesil Savaş 13
      (1) Küreselleşme *(Globalization)* 13
      (2) Postmodernite *(Postmodernity)* 16
      (3) Dördüncü Nesil Savaş *(Fourth Generation Warfare)* 18
   b. Asimetrik Savaş, Terörizm ve 11 Eylül Saldırıları 22
      (1) Asimetrik Savaş *(Asymmetric Warfare)* 23
      (2) Terörizm *(Terrorism)* 27
      (3) 11 Eylül Saldırıları *(The September 11 Attacks)* 31
   c. "Siber" Ön Eki ve Türetilen Kavramlar 34
      (1) Siber Uzay *(Cyberspace)* 36
      (2) Siber Güvenlik *(Cybersecurity)* 39
      (3) Siber Savaş *(Cyberwarfare)* 43
      (4) Siber Terörizm *(Cyberterrorism)* 47
      (5) Siber Suçlar *(Cybercrimes)* 55
   ç. Elektronik Savaş ve Enformasyon Savaşı 60
      (1) Elektronik Savaş *(Electronic Warfare)* 61
      (2) Enformasyon Savaşı *(Information Warfare)* 64
2. KURAMSAL ÇERÇEVE 67

a. Güvenlikleştirme Teorisi *(Securitisation Theory)* 68
(1) Kopenhag Okulu 69
(2) Paris Okulu 72
b. Çerçeveleme Teorisi *(Framing Theory)* 74
c. Gündem Belirleme Teorisi *(Agenda-Setting Theory)* 76

İKİNCİ BÖLÜM
ABD'DEKİ İSTİHBARAT VE GÜVENLİK YAPILANMASININ ASİMETRİK TEHDİT VE SİBER GÜVENLİK BAĞLAMINDA GEÇİRDİĞİ DEĞİŞİM

1. İSTİHBARAT VE GÜVENLİK AYGITI 81
2. FEDERAL SORUŞTURMA BÜROSU *(FEDERAL BUREAU OF INVESTIGATION)* 91
3. İÇ GÜVENLİK BAKANLIĞI *(DEPARTMENT OF HOMELAND SECURITY)* 93
   a. Ulusal Siber Güvenlik Bölümü *(National Cyber Security Division)* 94
   b. ABD Bilgisayar Acil Durum Hazırlık Takımı *(United States Computer Emergency Readiness Team)* 95
   c. Ulusal Altyapı Koruma Merkezi *(National Infrastructure Protection Center)* 95
   ç. Ulusal Siber Güvenlik ve İletişim Entegrasyon Merkezi *(National Cybersecurity and Communication Integration Center)* 96
   d. Endüstriyel Kontrol Sistemleri Acil Durum Hazırlık Takımı *(Industrial Control Systems Computer Emergency Readiness Team)* 97
   e. ABD Gizli Servisi *(United States Secret Service)* 97
4. ULUSAL GÜVENLİK TEŞKİLATI *(NATIONAL SECURITY AGENCY)* 98
5. ULUSAL İSTİHBARAT DİREKTÖRÜ OFİSİ *(OFFICE OF DIRECTOR OF NATIONAL INTELLIGENCE)* 100
   a. Ulusal Terörle Mücadele Merkezi *(National Counterterrorism Center)* 101

ÜÇÜNCÜ BÖLÜM
ASİMETRİK TEHDİT BAĞLAMINDA SİBER GÜVENLİĞİN SAĞLANMASINA YÖNELİK YASAL DÜZENLEMELER

1. SİBER GÜVENLİK İLE İLİŞKİLİ YASAL DÜZENLEMELER 104
2. ABD VATANSEVERLİK YASASI (USA PATRIOT ACT) 107
   a. Birinci Bölüm: İç Güvenliğin Terörizme Karşı Geliştirilmesi 112
   b. İkinci Bölüm: Takip Prosedürlerinin Geliştirilmesi 113
   c. Üçüncü Bölüm: 2001 Tarihli Uluslararası Para Aklamanın Azaltılması ve Terörizme Karşı Finansman Yasası 118
   ç. Dördüncü Bölüm: Sınırın Korunması 119
   d. Beşinci Bölüm: Terörizm Soruşturmalarının Önündeki Engellerin Kaldırılması 120
   e. Altıncı Bölüm: Terörizm Kurbanlarına, Kamu Güvenliği Görevlilerine ve Ailelerine Sağlanan İmkânlar 121
   f. Yedinci Bölüm: Kritik Altyapı Koruması İçin Arttırılmış Bilgi Paylaşımı 122
   g. Sekizinci Bölüm: Terörizme Karşı Ceza Kanunlarının Güçlendirilmesi 122
   ğ. Dokuzuncu Bölüm: Geliştirilmiş İstihbarat 132
   h. Onuncu Bölüm: Münferit Düzenlemeler 133
3. İÇ GÜVENLİK YASASI (HOMELAND SECURITY ACT) 135
   a. İç Güvenlik Yasası Kapsamında Yer Alan Hükümler 136
      (1) Birinci Bölüm: İç Güvenlik Bakanlığı 136
      (2) İkinci Bölüm: Enformasyon Analizi ve Altyapı Koruma 138
      (3) Üçüncü Bölüm: İç Güvenliğin Desteklenmesinde Bilim ve Teknoloji 141
      (4) Sekizinci Bölüm: Federal Olmayan Kuruluşlar ile Koordinasyon, Genel Müfettiş, ABD Gizli Servisi, Sahil Güvenlik, Genel Hükümler 141
   b. Siber Güvenliğin Geliştirilmesi Yasası *(Cyber Security Enhancement Act)* 144
   c. Federal Enformasyon Güvenliği Yönetimi Yasası *(Federal Information Security Management Act)* 147

DÖRDÜNCÜ BÖLÜM
SİBER GÜVENLİĞİN SAĞLANMASINA YÖNELİK YÜRÜTME FAALİYETLERİ

1. FEDERAL HÜKÜMET POLİTİKALARI 152
2. FEDERAL KURUMLAR ARASINDA İŞBİRLİĞİ 159
3. KOLLUK KUVVETLERİNİN GÜÇLENDİRİLMESİ 162

BEŞİNCİ BÖLÜM
SONUÇ, DEĞERLENDİRME VE ÖNERİLER

KAYNAKÇA 174

KISALTMALAR LİSTESİ

ABD : Amerika Birleşik Devletleri

ARPANET : *Advanced Research Projects Agency Network* (İleri Araştırma Projeleri Kurumu Bilgisayar Ağı)

ATF : *Bureau of Alcohol, Tobacco, Firearms and Explosives* (Alkol, Tütün, Ateşli Silahlar ve Patlayıcılar Bürosu)

BM : Birleşmiş Milletler

CCRC : *Computer Crime Research Center* (Bilgisayar Suçları Araştırma Merkezi)

CIA : *Central Intelligence Agency* (Merkezî Haberalma Teşkilatı)

CIPA : *Critical Infrastructures Protection Act of 2001* (2001 Tarihli Kritik Altyapıların Korunması Yasası)

CNCI : *Comprehensive National Cybersecurity Initiative* (Kapsamlı Ulusal Siber Güvenlik Girişimi)

CNO : *Computer Network Operations* (Bilgisayar Ağı Operasyonları)

CS&C : *Office of Cybersecurity and Communications* (Siber Güvenlik ve İletişim Dairesi)

CSS : *Central Security Service* (Merkezi Güvenlik Servisi)

CSSP : *Control Systems Security Program* (Kontrol Sistemleri Güvenlik Programı)

CWEID : *Cyber Warfare, Exploitation & Information Dominance Lab* (Deniz Kuvvetleri Siber Savaş, İstismar ve Enformasyon Hakimiyeti Laboratuvarı)

CWIS : *Campus Wide Information System* (Yerleşke Çapında Enformasyon Sistemi)

DEA : *Drug Enforcement Agency* (Uyuşturucuyla Mücadele Teşkilatı)

DIA : *Defense Intelligence Agency* (Savunma İstihbarat Teşkilatı)

DCI : *Director of Central Intelligence* (Merkezi İstihbarat Direktörü)

DHS : *Department of Homeland Security* (İç Güvenlik Bakanlığı)

DNI : *Director of National Intelligence* (Ulusal İstihbarat Direktörü)

DRAG : *US Army Training and Doctrine Command Doctrinal Review and Approval Group* (ABD Kara Kuvvetleri Eğitim ve Doktrin Komutanlığı Doktrin İnceleme ve Onay Grubu)

ECTFs : *Electronic Crimes Task Forces* (Elektronik Suçlar Görev Kuvvetleri)

EMP : *Electromagnetic Pulse* (Elektromanyetik Darbe)

EO : *Executive Order* (Başkanlık İdari Emri)

EW : *Electronic Warfare* (Elektronik Savaş)

ERRI : *Emergency Response and Research Institute* (Acil Durum Müdahale ve Araştırma Enstitüsü)

FBI : *Federal Bureau of Investigation* (Federal Soruşturma Bürosu)

FISA : *Foreign Intelligence Surveillance Act of 1978* (1978 tarihli Yabancı İstihbarat Takip Yasası)

FISMA : *Federal Information Security Management Act of 2002* (2002 tarihli Federal Enformasyon Güvenliği Yönetimi Yasası)

GAO : *US Government Accountability Office* (ABD Hükümeti Hesapverilebilirlik Dairesi)

GSA : *US General Services Administration* (ABD Genel Hizmetler İdaresi)

GRC : *Governance, Risk Management, and Compliance* (Yönetişim, Risk Yönetimi ve Uyumluluk)

HSA : *Homeland Security Act of 2002* (2002 tarihli İç Güvenlik Yasası)

HSARPA : *Homeland Security Advenced Research Projects Agency* (İç Güvenlik İleri Araştırma Projeleri Kurumu)

HSC : *Homeland Security Council* (İç Güvenlik Konseyi)

HSPD : *Homeland Security Presidential Directive* (Başkanlık İç Güvenlik Direktifi)

IC : *Intelligence Community* (İstihbarat Topluluğu)

ICC : *Integrated Cyber Center* (Bütünleşik Siber Merkez)

ICS-CERT : *Industrial Control Systems Computer Emergency Readiness Team* (Endüstriyel Kontrol Sistemleri Acil Durum Hazırlık Takımı)

Internet : *International Network* (Uluslararası Ağ)

IO : *Information Operations* (Enformasyon Operasyonları)

IP : *Office of Infrastructure Protection* (Altyapı Koruma Dairesi)

IRTPA : *Intelligence Reform and Terrorism Prevention Act of 2004* (2004 tarihli İstihbarat Reformu ve Terörizmin Önlenmesi Yasası)

LAN : *Local Area Network* (Yerel Alan Ağı)

LII : *Cornell University Law School Legal Information Institute* (Cornell Üniversitesi Hukuk Fakültesi Yasal Mevzuat Bilgi Enstitüsü)

MAN : *Metropolitan Area Network* (Metropol Alan Ağı)

NATO : *North Atlantic Treaty Organization* (Kuzey Atlantik Antlaşması Örgütü)

NCCIC : *National Cybersecurity and Communications Integration Center* (Ulusal Siber Güvenlik ve İletişim Entegrasyon Merkezi)

NCIRP : *National Cyber Incident Response Plan* (Ulusal Siber Olaylara Müdahale Planı)

NCRCG : *National Cyber Response Coordination Group* (Ulusal Siber Müdahale Koordinasyon Grubu)

NCS : *National Communications System* (Ulusal İletişim Sistem Dairesi)

NCSD : *National Cyber Security Division* (Ulusal Siber Güvenlik Bölümü)

NCTC : *National Counterterrorism Center* (Ulusal Terörle Mücadele Merkezi)

NGA : *National Geospatial-Intelligence Agency* (Ulusal Coğrafi İstihbarat Teşkilatı)

NIMA : *National Imagery and Mapping Agency* (Ulusal Görüntüleme ve Haritalama Teşkilatı)

NIP : *National Implementation Plan for the War on Terror* (Teröre Karşı Savaş Ulusal Uygulama Planı)

NIPC : *National Infrastructure Protection Center* (Ulusal Altyapı Koruma Merkezi)

NIPP : *National Infrastructure Protection Plan* (Ulusal Altyapı Koruma Planı)

NISAC : *National Infrastructure Simulation and Analysis Center* (Ulusal Altyapı Simülasyon ve Analiz Merkezi)

NIST : *National Institute of Standards and Technology* (Ulusal Standartlar ve Teknoloji Enstitüsü)

NPPD : *National Protection and Programs Directorate* (Ulusal Koruma ve Programlar Müdürlüğü)

NRC : *Nuclear Regulatory Commission* (Nükleer Düzenleme Komisyonu)

NRO : *National Reconnaissance Office* (Ulusal Keşif Ofisi)

NSA : *National Security Agency* (Ulusal Güvenlik Teşkilatı)

NSC : *National Security Council* (Ulusal Güvenlik Konseyi)

NSCT : *National Strategy for Combating Terrorism* (Terörle Mücadele Ulusal Stratejisi)

NSF : *National Science Foundation* (Ulusal Bilim Vakfı)

NSPD : *National Security Presidential Directive* (Başkanlık Ulusal Güvenlik Direktifi)

NSS : *National Security Strategy* (Ulusal Güvenlik Stratejisi)

NTOC : *NSA/CSS Threat Operations Center* (NSA/CSS Tehdit Harekat Merkezi)

ODNI : *Office of Director of National Intelligence* (Ulusal İstihbarat Direktörü Ofisi)

OMB : *Office of Management and Budget* (Yönetim ve Bütçe Dairesi)

ONI : *Office of Navy Intelligence* (Donanma İstihbarat Ofisi)

OPSEC : *Operations Security* (Operasyon Güvenliği)

ÖOS : Öldürücü Olmayan Silahlar

PDD : *Presidential Decision Directive* (Başkanlık Karar Direktifi)

PSYOPS : *Psychological Operations* (Psikolojik Operasyonlar)

RAND : *Research and Development Corporation*

RICO : *Racketeer Influenced and Corrupt Organizations* (Haraç ve Suç Örgütleri)

SCADA : *Supervisory Control And Data Acquisition* (Yönetsel Kontrol ve Veri Edinimi)

SEM : *Security Event Management* (Güvenlik Olay Yönetimi)

SIEM : *Security Information and Event Management* (Güvenlik Bilgisi ve Olay Yönetimi)

SIGINT : *Signal Intelligence* (Sinyal İstihbaratı)

SIM : *Security Information Management* (Güvenlik Bilgisi Yönetimi)

SOPA : *Stop Online Piracy Act* (Çevrimiçi Korsanlığı Durdurma Yasası)

STO : *Special Technical Operations* (Özel Teknik Operasyonlar)

US/U.S. : *United States* (Amerika Birleşik Devletleri)

USC : *United States Code* (ABD Federal Kanunlar Külliyatı)

US-CERT : *United States Computer Emergency Readiness Team* (ABD Bilgisayar Acil Durum Hazırlık Takımı)

USCYBERCOM: *United States Cyber Command* (ABD Siber Komutanlığı)

USA PATRIOT ACT: *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001* (2001 tarihli Terörizmi Önlemek ve Engellemek için Gerekli Uygun Araçları Sağlamak Suretiyle Amerikayı Birleştirme ve Kuvvetlendirme Yasası)*

USS : *United States Ship* (ABD Gemisi)

---

* Çalışma metni içerisinde "ABD Vatanseverlik Yasası" olarak anılmıştır.

USSC : *United States Sentencing Commission* (ABD Ceza Komisyonu)

USSS : *United States Secret Service* (ABD Gizli Servisi)

USSTRATCOM: *United States Strategic Command* (ABD Stratejik Komutanlığı)

WAN : *Wide Area Network* (Geniş Alan Ağı)

ÖN SÖZ

Özellikle son 10 yıllık dönemde iletişim ve enformasyon teknolojilerinde şahit olunan hızlı gelişim ve bu gelişime bağlı olarak ortaya çıkan yeni gerçeklikler, toplumların sahip oldukları sosyo-kültürel değer ve yapılar üzerinde ciddi etkilere sahiptir. Benzeri bir biçimde; "küreselleşme", "postmodernite" ve "dördüncü nesil savaş" olgularının bir araya gelmesinden doğan sinerjik nitelikteki siyasal-sosyal-askeri yoğunlaşma da siyaset ve güvenlik alanlarında ciddi değişimler yaratmaktadır. Her ne kadar yaşanmakta olan sosyo-kültürel ve siyasal değişiklikler tümüyle bu olgulara ve teknolojik gelişmelere bağlanamaz ise de, söz konusu olgu ve gelişmelerin özellikle güvenlik alanında, soğuk savaş sonrasında dünyayı şekillendiren en etkili faktörler arasında yer aldıkları inkar edilemez.

Bu çerçevede 11 Eylül Saldırıları; hem bahse konu faktörlerin yarattıkları güvenlik tehditlerini oldukça net bir biçimde somutlaştırması, hem de bu somutlaşmaya verilen yine somut tepkilere sağlam bir zemin sağlamış olması ile, özellikle asimetrik tehdit bağlamındaki güvenlik politikaları için bir milat niteliği kazanmıştır. Bu somutlaşmalar paralelinde, gerek asimetrik tehdit bağlamındaki güvenlik kaygılarının artmasına ve gerekse de teknolojik gelişmelerin sağladığı ciddi ve sürekli artan gözetleme kapasitesine bağlı olarak, totaliter bir idareye zemin hazırlayabilecek bir gözetim toplumunun ortaya çıkabileceği kaygıları da sıklıkla ABD'de dile getirilmeye başlanmıştır. Bu kapsamda, 11 Eylül Saldırılarına ilişkin olarak akıldan çıkartılmaması gereken en önemli nokta; saldırılardan önceki dönemi hiçbir asimetrik tehdit tartışmasının yapılmadığı ve güvenlik yaklaşımının geliştirilmediği "karanlık bir çağ" olarak görmenin, saldırılardan sonraki dönemi ise alınan tedbirlerin kapsam genişliği ve sağladığı yapısal dönüşüm üzerinden idealize etmenin ve ortaya çıkan tüm bu değişimlerin bir anda gerçekleştiklerini varsaymanın, pek çok sosyal ve siyasal olgu ile bu

olguların içerisinde etkileştikleri süreçleri fazlasıyla basite indirgemek olacağı hususudur.

Yukarıda kısaca ortaya konulmaya çalışılan yaklaşım ışığında bu çalışmanın ana kaygısı, asimetrik tehdit bağlamında ve 11 Eylül 2001 sonrası dönemi kapsayacak şekilde ABD örneği üzerinden, siber güvenlik olgusunun kapsamına ilişkin bir durum tespiti yapmak ve objektif bir çerçeve çizmek olup; siber güvenlik ile ilişkili olduğu değerlendirilen kavramların ve kuramların daha derinlemesine incelenmesi ya da 11 Eylül Saldırıları sonrasında alınan tedbirlerin gerekliliklerinin ve verimliliklerinin değerlendirilmesi veya sorgulanması, elbette ki ileride yapılabilecek daha eleştirel akademik çalışmaların konusunu oluşturabilecektir. Nesnelliği ön planda tutma gayreti içerisinde yürütülen bu çalışma, kapsamına aldığı olgu ve kavramlara ilişkin olarak; hem ileride yapılabilecek daha derinlemesine çalışmalar için objektif bir kavramsal ve kuramsal çerçeve örneği sunmak, hem de bahse konu olgu ve kavramlar arasındaki ilişkilere dikkati çekmiş olmak ile görevini yerine getirmiş olacaktır.

GİRİŞ

Günümüzün güvenlik yönetimi jargonunda oldukça önemli yerleri işgal eden "enformasyon operasyonları", "asimetrik tehdit", "siber savaş" veya "kritik altyapı" gibi "sihirli kelimeler", güvenlik karar alıcıları tarafından geliştirilen politikaların meşrulaştırılmasında oldukça kritik ve merkezi roller oynamaktadırlar. İster asimetrik tehditlerle dolu, enformasyon teknolojileri odaklı, küreselleşen postmodern bir dünyada olsun, isterse de doğadan gelen tehditlerle dolu, taş aletlerin kullanıldığı tarih öncesi devirlerde olsun; bireylerin varlık ve huzurları üzerinde olumsuz etkilere sahip olgular -tehditler- mevcut oldukları sürece, onların var olmadığı bir ortamı yaratma -güvenlik- ihtiyacı ve gayreti de kaçınılmaz olarak mevcut olacaktır.

Bu çerçevede, ABD'li Psikolog A.H. Maslow tarafından geliştirilmiş olan "İhtiyaçlar Hiyerarşisi Teorisi *(Hierarchy of Needs)*"nde de ifade edildiği üzere, kişinin "emniyet ve güvenliğini sağlama" ihtiyacı, en temel insani ihtiyaçlarını oluşturan fizyolojik ihtiyaçların hemen ardından ikinci sırada yer almaktadır (Boeree [web], 2006).

Dolayısı ile yukarıda dikkat çekilen, kelimeler üzerinden somutlaştırılan ve bireylerin karşı koymakta zorlandıkları söz konusu sihirli etkinin, Maslow tarafından da vurgulandığı gibi güvenliğin temel insan ihtiyaçları arasında yer almasından kaynaklanıyor olduğunu ileri sürmek de mümkündür.

Elbette ki, toplumlar tarafından yaşanılmış olan her bir eşsiz tecrübe de, o toplumun güvenliğe ilişkin algı, anlayış ve yaklaşımlarını temelden etkilemektedir. Özellikle bireysel, toplumsal ve tarihsel temelleri ile ön plana çıkan "güvenlik" olgusu ve onunla ilişkili algılar; insanlar ve toplumlar var oldukları sürece, en göze çarpan yerde ve kaçınılmaz bir biçimde var olmaya devam edeceklerdir.

Örneğin, Avrupa'dakiler başta olmak üzere, dünyanın geri kalanındaki yoğun rekabet ve savaşlardan iki büyük okyanus sayesinde tarihsel olarak uzak kalmayı başarmış olan ABD toplumu için; yabancı bir güç tarafından kendi topraklarında vurulma -ve güvenlik içinde olma

durumundan uzaklaşma- duygusunu yaşatan 07 Aralık 1941 tarihli Pearl Harbor Saldırısı ve 11 Eylül 2001 tarihli terör saldırıları travmatik birer tecrübe olmuşlardır.

Bu kapsamda, asimetrik tehdidin oldukça net bir biçimde somutlaştığı 11 Eylül Saldırılarına dayanan, son dönem ABD tecrübesinin önemi; geliştirilen tepkinin siyasi, hukuki ve askeri yansımalarının oldukça büyük olması ve neredeyse "kutsal" kabul edilen ABD Anayasasında yer alan bazı temel hak ve özgürlükleri dahi tehdit edebilecek bir ortamı yaratmasındadır.

ABD'nin yaşadığı travmatik güvenlik tecrübeleri arasında oldukça önemli bir yere sahip olan 11 Eylül Saldırılarının, siber güvenlik olgusu üzerindeki etkilerini ortaya koymayı amaçlayan bu akademik çalışma ise, yapısal olarak beş ana bölümden meydana gelmektedir.

Kavramsal ve kuramsal çerçeveye ayrılmış olan, çalışmanın birinci bölümünde; gerek araştırmanın ileriki safhalarında karşılaşılacak kavramlar için ön bilgilendirme yapılması, gerekse de söz konusu kavramların birbirleri ile sahip oldukları ilişkilerin ortaya konulması temel amaçtır. Bu çerçevede, birbirleri ile yakın ilişkide oldukları değerlendirilen kavramlar gruplandırılarak birlikte ele alınmışlardır. Her ne kadar bu noktada, bahse konu kavramların ayrı ayrı ve çok daha ayrıntılı olarak ele alınmaları da mümkün olmakla birlikte: çalışmanın kapsamını çizen "asimetrik tehdit" ve "siber güvenlik" bağlamlarına sadık kalmak kaygısı ile, kavramlar arasındaki ilişkilerin ortaya konulmasına odaklanılmak suretiyle literatür içerisinde seçici davranılmıştır. Söz konusu seçici davranış süreci içerisinde temel yaklaşım; belirli bir düşünceyi desteklemek ya da eleştirmek yerine, ilgili kavramların mümkün olduğunca fazla ve farklı boyutlarının ortaya konulması olmuştur.

Durum ve olgu tespitine odaklanmış olan bu çalışma, herhangi bir hipotez geliştirme kaygısı taşımamaktadır. Bu nedenle, çalışmada yer verilen kuramsal çerçeve ile; olgu ve kavramlara çalışma içerisinde biçilen rollerin açıklanmasından ve desteklenmesinden ziyade, güvenlik politikalarının oluşturulması sırasında bahse konu olgu ve kavramların içerisinden geçtikleri süreçlerin olabildiğince geniş okunabilmesini

sağlamak amaçlanmıştır. Yine bu çerçevede, ABD'li karar alıcıların güvenlik algılarına ilişkin olarak, tasarımcılarının sınırlı ve sübjektif olabilecek bakış açılarına dayalı kimi eleştirel kalıplara ya da spekülatif yorumlara yer vermek yerine; güvenlikleştirme süreçlerine ilişkin "temel" bilgiler verilmek suretiyle, tehdit ve güvenlik algısının ortaya çıkışının nesnel bir biçimde kavranmasını sağlamak amaçlanmıştır. Dolayısı ile, eksik olduğu değerlendirilen olgu ve kavramların eklenmesi veya ilgili güvenlikleştirme kuramlarının üzerine daha fazla eğilmek suretiyle, bu çalışma kapsamında ulaşılmış olan sonuçlardan daha farklı ve derinlemesine sonuçlara ulaşılabilmesi de mümkündür.

Çalışmanın ikinci bölümü, kendisinden sonra gelen bölümlerde ayrıntılı bir biçimde ele alınmış olan, siber güvenlik alanında hayata geçirilen hukuki ve idari tedbirlere ilişkin bir ön hazırlık sağlaması ve güvenlik politikalarını ortaya çıkartan "yapı" hakkında temel bilgilendirmeyi sağlaması maksadıyla; ABD'deki ulusal güvenlik yapılanmasına ve 11 Eylül Saldırıları sonrasında geçirdiği değişime ayrılmıştır.

Çalışmanın, 11 Eylül Saldırıları sonrasında asimetrik tehditler bağlamında, siber güvenlik ve ilişkili diğer alanlarda federal seviyede hayata geçirilen yasal tedbirlere ayrılmış olan üçüncü bölümünde; 2001 tarihli ABD Vatanseverlik Yasası ve 2002 tarihli İç Güvenlik Yasası gibi, 11 Eylül Saldırılarını takip eden süreçte kabul edilmiş ve önemli etkilere sahip olan kanunlar incelenmiştir. Elbette ki bahse konu kanunlar haricinde, siber güvenlik ile ilişkili içeriğe sahip olan pek çok başka kanun da söz konusu süreçte ya da sonrasında kabul edilmiş ise de, yukarıda belirtilen kanunların etkileri, gerek kronolojik öncelikleri, gerekse de kapsam ve içerikleri nedeniyle belirleyici seviyede olmuştur.

11 Eylül Saldırıları sonrası dönemde siber güvenliğe yönelik federal hükümet faaliyetlerini içeren, çalışmanın dördüncü bölümü ise; gerek geliştirilen politikalara ilişkin pek çok bilgi ve belgenin "gizli" gizlilik derecesine sahip olması, gerekse de çoğu zaman için stratejik bir perspektif ortaya koymaktan ziyade teşkilatlanmaya odaklanmış olmaları nedeniyle, kaçınılmaz olarak sınırlı kalmıştır.

Sonuç ve değerlendirmeye ayrılmış olan, çalışmanın beşinci bölümünde; çalışmanın önceki bölümleri bir bütün olarak ele alınarak, tehdit algısına ve güvenlik politikalarının karakterine ilişkin tespit ve değerlendirmelerde bulunulmuştur.

Bu kapsamda, çalışmanın kavramsal ve kuramsal çerçevesi ayrıntılı bir şekilde ortaya konulmadan önce; konu, amaç, kapsam ve sınırlılıklar gibi noktalar üzerinden, yapılan araştırmanın nitel profilinin ortaya konulması faydalı olacaktır.

Çalışma kapsamında yürtülen araştırma faaliyetinin konusu; 11 Eylül 2001 tarihinde ABD hedeflerine yönelik girişilmiş olan terör saldırıları sonrasındaki dönemde, bahse konu saldırılara bağlı olarak özellikle güvenlik yönetimi alanında hızla önem kazanmış olan "asimetrik tehdit" olgusu ile, ABD'nin siber güvenliğini sağlamaya yönelik çabaları arasındaki ilişki ve bu ilişkiden doğmuş olan sonuçlardır. Bu çerçevede, 11 Eylül Saldırıları ile birlikte ulusal ve uluslararası güvenlik politikalarını yoğun ve derinden etkileyen bir nitelik kazanmış olan "asimetrik tehdit" kavramı temelinde; siber tehditlerin nasıl algılandıkları, bu algıya dayanılarak geliştirilmiş olan yasal düzenlemeler ve güvenlik politikaları öncelikli olarak ele alınmışlardır.

Araştırma faaliyetleri süresince göz önünde bulundurulan temel amaç ise; ABD'deki siber güvenlik yaklaşımlarına hâkim olan, *"Bir mouse'un, en az bir kurşun veya bomba kadar tehlikeli olabileceği"*[1] inancının temelinde yatan "asimetrik tehdit" kavramı üzerinden 11 Eylül Saldırıları sonrası dönemdeki siber güvenlik politikalarının karakteristik özelliklerinin ortaya konulması olmuştur.

Bilişim sistemlerinin öneminin her geçen gün daha da arttığı ve siber kimliklerin ortaya çıktığı günümüz dünyasında, siber tehdit olarak değerlendirilen olguların kapsamları ve tanımları üzerinde halen bir fikir birliği sağlanabilmiş değildir. Söz konusu durum, siber güvenlik alanında

[1] ABD Temsilciler Meclisinin Teksas Eyalet Temsilcisi ve Cumhuriyetçi Parti üyesi olan Lamar Smith'e ait olan bu ifade, 11 Eylül Saldırılarından kısa bir süre sonra kullanılmış olup; orijinal hali, *"A mouse can be just as dangerous as a bullet or a bomb"* şeklindedir (CCRC [web], 2002). Halen aynı görevi sürdürmekte olan Lamar Smith, dikkat çekici bir şekilde; internet üzerinden yapılan telif hakkı ihlallerinin önlenmesine yönelik olarak 2011 yılı sonunda hazırlanan ve kolluk kuvvetlerinin bu alandaki yetkilerinin arttırılmasını öngören, ancak neden olduğu ciddi tepkiler sonrasında askıya alınmak zorunda kalınan SOPA Yasa Tasarısının da sahibidir.

görev almakta olan gerek teknik, gerekse de karar alıcı personelin, görevleri kapsamında yürüttükleri tehdit değerlendirmesi ve risk analizi süreçleri için gerekli farkındalığı tam olarak geliştirmelerini önleyebilmektedir. Bu çerçevede, çalışma kapsamında siber tehditlere asimetrik tehdit bağlamında ve ABD örneği üzerinden yaklaşılmak suretiyle; özellikle siber güvenlik alanında görev alan veya alabilecek karar alıcılarda, siber tehditlere ve siber güvenliğe ilişkin güncel tartışmalar ve çağdaş eğilimler hakkında farkındalık yaratılması da hedeflenmektedir. Çalışmadan beklenilen bir diğer sonuç ise; gerek siber güvenlik alanında ileride yapılabilecek benzeri yüksek lisans çalışmaları için objektif bir kavramsal ve kuramsal çerçeve örneğinin oluşturulabilmesi, gerekse de özellikle "Siber Güvenlik Doktrinleri" üzerine ileride yapılabilecek doktora seviyesindeki çalışmalar için gerekli altyapının tesis edilmesidir.

Yukarıda sayılan amaçlara ulaşılması maksadıyla yürütülen bu çalışma kapsamında; siber güvenlik ile ilişkilendirilerek ele alınan aktörler, kanunlar ve uygulamalar üzerinden de dolaylı olarak, ABD'deki siber güvenlik arenasında hakim konumda bulunan aktörlere dair mümkün olduğunca güncel ve ayrıntılı bilgilerin sağlanmasına da çaba gösterilmiştir.

Diğer güvenlik tehditlerinde olduğu gibi, siber güvenlik tehditlerinin yarattıkları riskleri ortadan kaldırmak ya da en azından kabul edilebilir bir seviyeye indirmek için de yapılması gereken; onların doğalarını doğru anlamak, karşı karşıya bulunulan biçimlerini doğru tespit etmek ve etkili sonuçlar verecek doğru karşı-tedbirleri almak suretiyle tekrar ortaya çıkmalarına engel olmaktır. Ancak böylelikle, gerek siber, gerekse de konvansiyonel güvenlik tehditleri ulusal güvenlik ve modern toplumsal hayat için birer risk ve huzursuzluk kaynağı olmaktan çıkarılabileceklerdir.

Bu nedenle, bilimselliği ve ona ulaşma kaygısından kaynaklanan nesnelliği içeren akademik çalışmaların, gerek siber güvenlik, gerekse de daha kapsamlı bir analiz düzeyi olarak güvenlik yönetimi alanlarında artan sayıda yapılmaları kritik önemdedir. Siber güvenlik politikaları ve stratejilerine geliştirilmeleri aşamasında katkıda bulunmak, oluşturulabilecek yol haritaları için fikir vermek ve tamamlanma tarihleri

itibariyle kapsamlı birer bibliyografik kaynakçayı bir araya getirmiş olmak gibi özellikler, bu tip çalışmaların hem pratik hem de akademik önemlerini ciddi bir biçimde arttıracaktır.

Bu çerçevede, yapılmış olan bu çalışmanın da; özellikle iç tehdit ve siber tehdit algılamaları arasındaki kesişmeye ilişkin bir farkındalığın yaratılması, asimetrik tehditler bağlamında kritik altyapı güvenliğinin siber boyutuna dikkat çekilmesi ve 11 Eylül 2001 sonrası dönemde terörizmle mücadele etmek maksadıyla yürürlüğe konulan kanunların sahip oldukları kişi hak ve hürriyetlerini tehdit edici potansiyelin ABD örneği üzerinden ortaya konulması açısından önemli olduğu değerlendirilmektedir.

Bu çalışmanın yürütülmesi kapsamında, gerekli sürekliliği sağlayan temel unsurlar; araştırma faaliyetinin gerekliliğine ve yürütülüş biçimine ilişkin olarak yapılan bazı kritik tespitlerin yanı sıra araştırma faaliyetinin itici gücünü sağlayan araştırma soruları olmuştur. Bu çerçevede, araştırma faaliyetinin gerekliliğine ve yürütülüş biçimine ilişkin olarak yapılmış olan tespitler şöyle sıralanabilirler:

- Siber güvenlik ile ilişkili oldukları değerlendirilen pek çok kavramın ve olgunun, yaygın ve açık tanımları bulunmamaktadır.

- Küreselleşme, postmodernite, dördüncü nesil savaş ve asimetrik savaş gibi kavramlar; dengesizlik ve düzensizlik durumlarını da en az denge ve düzen durumları kadar doğal kabul eden, mevcut olanın sorgulanması ve eşit olmayanlar arası ilişkileri ön plana çıkartan yaklaşım ve anlayışları teşvik etmektedirler.

- 11 Eylül Saldırıları sonrası dönemde hayata geçirilen ilgili yasal düzenlemeler, asimetrik tehdidin somutlaşmış hali olan terörizm ile mücadeleye odaklanmış olmaları nedeniyle, "ulusal güvenlik" ve "iç güvenlik" kaygıları üzerinden temel kişi hak ve hürriyetlerini sınırlandırıcı bir potansiyele sahip bulunmaktadırlar.

Yapılmış olan bu tespitler ışığında, çalışma kapsamında cevapları aranılmış olan araştırma soruları ise şöyle sıralanabilirler:

- Asimetrik tehdit bağlamında, "siber güvenlik" olgusu ile doğrudan veya dolaylı olarak ilişkili olan kavramlar nelerdir ve birbirleri ile nasıl bir ilişki içerisindedirler?

- ABD'de 11 Eylül Saldırıları sonrasında, asimetrik tehdit bağlamında nasıl bir siber tehdit algısı ortaya çıkmıştır?

- ABD'de 11 Eylül Saldırıları sonrasında geliştirilen siber güvenlik politikalarının genel karakteristikleri ve yarattıkları sonuçlar nelerdir?

- Siber tehdit algısına ve güvenlik politikalarına hakim olan anlayışın somut sonuçlarını yansıtan bir düzlem olarak, 11 Eylül Saldırıları sonrasında ABD'de yürürlüğe konulan yasal düzenlemeler nelerdir ve ne gibi tedbirleri öngörmektedirler?

- ABD'de 11 Eylül Saldırıları sonrasında geliştirilen siber güvenlik politikalarının hayata geçirilmesi hususunda, uygulamaya ilişkin olarak yapılan tespitler nelerdir?

Zaman, mekan ve bağlam açısından oldukça net sınırlara sahip olan ve esas itibariyle siber güvenlik olgusunun ele alındığı bu çalışma; mekan açısından ABD ile, zaman açısından 11 Eylül 2011 tarihinden sonraki dönem ile ve bağlam açısından ise asimetrik tehdit kavramı ile sınırlandırılmıştır.

Bahse konu iradi sınırlandırmaların yanı sıra içerik itibari ile de siber güvenlik olgusunun *"sui generis"* karakterinden kaynaklanan bir biçimde; siber güvenliğin teknik boyutu, kaçınılmaz bir şekilde hukuksal ve siyasal boyutundan ayrışarak, çalışma kapsamının dışında kalmıştır. Çalışma kapsamında ele alınan hukuksal ve siyasal tedbirler ise, gerek ABD'nin federal bir yönetim yapısına sahip olması ve gerekse de bahse konu tedbirlerin federal hükümeti ön plana çıkartan karakteristikleri nedeniyle, federal seviyedeki düzenlemeler ve uygulamalar ile sınırlı tutulmuşlardır. Başka bir ifade ile çalışma perspektifi; ABD'nin federal seviyede sahip olduğu siber tehdit algılarını ve geliştirmiş olduğu siber

güvenlik politikalarının sosyal ve siyasal boyutlarını kapsayan bir niteliktedir.

Siber tehditlerin, "siber suç", "siber terörizm" ve "siber savaş" üzerinden somutlaşan sosyal, siyasal ve askeri boyutları ile, siber güvenliğe ilişkin "yasal düzenlemeler" ve "güvenlik doktrinleri" üzerinden somutlaşan karşı-tedbirlerin, ABD'li uzmanlar ve güvenlik karar alıcıları tarafından oldukça uzun zamandır ve fazlasıyla içselleştirilmiş olması; çalışma konusu olarak ABD'nin ve onun güvenlik uygulamalarının tercih edilmesinde temel etken olmuştur. Bunun yanı sıra siber uzayın ana omurgasını oluşturan internetin kontrolünü münhasıran elinde bulundurması ve asimetrik tehdidin en net biçimde somutlaştığı 11 Eylül Saldırılarının hedefinde yer almış olması nedeniyle de; ABD, asimetrik tehdit bağlamında ortaya çıkan siber tehdit algısı ve güvenlik tedbirleri hususlarında yapılacak bir araştırma için, ideal bir inceleme nesnesi özelliği kazanmıştır.

Çalışma kapsamında karşılaşılan en önemli sınırlılık; ulusal güvenliğin bir alt dalı olarak görülen siber güvenlik alanında, özellikle savunma ve istihbarat merkezli gerçek tehdit değerlendirmelerine ve alınması öngörülen karşı tedbirlere ilişkin bilgilere, "Gizli" gizlilik derecesine sahip olmaları nedeniyle açık kaynaklardan ulaşılamaması olmuştur. Bu nedenle çalışma kapsamında, resmi nitelikteki ABD açık kaynaklarında yer alan veri, doküman ve bilgilere mümkün olabildiğince öncelik verilmiş, ikincil kaynaklara ise bilgilendirme ve kontrol amacıyla yönelinmiştir. Dolayısı ile çalışmada yer alan bilgilerin ve yapılan tespitlerin derinliği, ABD'nin ulusal güvenlik ve siber güvenlik politikaları çerçevesinde bilinmesine izin verdiği seviye ile sınırlı kalmıştır. Her ne kadar söz konusu kısıtlayıcı durum çalışmanın niteliği ve önemi üzerinde fazla bir etki yaratmamış ise de; savunma ve istihbarat alanlarına ilişkin bilgilendirme kapasitesini sınırlarken, hukuk ve iç güvenlik alanlarının çalışma içerisindeki ağırlığının göreceli olarak artmasına neden olmuştur.

Konu ve kapsamına bağlı olarak, çalışmanın ağırlıklı olarak ve doğrudan yabancı kaynaklardan faydalanılmak suretiyle hazırlanmış olması da; gerek çalışmanın kavramsal ve kuramsal çerçevesinin

oluşturulmasının, gerekse de kaynak tarama, alıntılama, çeviri ve kontrol faaliyetlerinin diğer çalışmalarda beklenilenden çok daha fazla zaman almasına yol açmıştır. Bu çerçevede çalışma kapsamında yürütülen çeviri faaliyetlerinde, İngilizce terim ve ifadelerin dilimizdeki karşılıklarının tam ve doğru olarak tespit edilmesi hususunda özel hassasiyet gösterilmiş ise de; gerek tam anlamın karşılanamaması, gerekse de ülkemizde aynı olgu için farklı terim ve ifadelerin kullanılabiliyor olması nedeniyle, -"enformasyon" örneğinde olduğu gibi- bazı İngilizce kelimelerin Türkçe karşılıklarının kullanılmasından bilinçli olarak kaçınılmıştır.

Yine çeviri faaliyetleri kapsamında, çalışma içerisinde kritik öneme sahip olan bazı yasal düzenleme isimlerinin Türkçe karşılıklarının belirlenmesi hususunda da kaçınılmaz olarak bazı öznel tercihlerde bulunulmak zorunda kalmıştır. Bu çerçevede;

- Gerek açık isminin Türkçe karşılığının çalışma metni içerisinde sıklıkla yer verilemeyecek kadar uzun olmasına, gerekse de kısaltılmış isminin içerdiği politik anlamın korunması kaygısına bağlı olarak *"USA PATRIOT Act"* isimli yasal düzenlemenin Türkçe karşılığı "ABD Vatanseverlik Yasası" olarak tespit edilmiş,

- *"Homeland Security Act"* isimli yasal düzenlemenin Türkçe karşılığı "İç Güvenlik Yasası" olarak tespit edilmiş,

- Hali hazırda aynı isimle yapılmış başka yasal düzenlemelerin bulunmaması nedeniyle, ABD Vatanseverlik Yasasının ve İç Güvenlik Yasasının orijinal isimlerinde yer alan -sırasıyla- "2001 tarihli" ve "2002 tarihli" ibarelerine çalışma metni içerisindeki yaygın kullanım kapsamında yer verilmemiştir.

Çalışmanın doğrudan yabancı kaynaklara dayalı olarak yürütülmüş olması -benzeri bir biçimde- şekli özellikleri üzerinde de biçimlendirici bir etki göstermiştir. Literatür araştırması niteliği ön plana çıkan bu çalışma kapsamında yapılan çevirilerde, atıfta bulunulan kaynağın görüşleri mümkün olabildiğince değiştirilmeden ve anlam kayıplarına yol açmadan verilmeye çalışılmıştır. Bu çerçevede yapılan her bir alıntı, gerek diğer alıntılar, gerekse de tez çalışması kapsamında

yapılan tespit ve yorumlar ile karışmaması maksadıyla ayrı birer paragraf halinde çalışmaya dahil edilmiştir. Çalışmanın esas itibariyle bir literatür taraması faaliyetine dayalı olmasının yanı sıra herhangi bir "bilimsel aşırma" durumunun ortaya çıkmasından da kaçınmak kaygısından kaynaklanan bu yaklaşım çerçevesinde; atıf içeren paragraflarda yer alan tüm ifadelerin ilgili kaynak lehine yorumlanmak suretiyle, o kaynağa ait veya o kaynaktan esinlenilmiş olarak kabul edilmesi uygun olacaktır.

Bilimsel araştırma yöntemi olarak "tanımlayıcı-betimleyici" yöntemin benimsenmiş olduğu bu çalışma; yaşanılan bir olaydan doğan etkilere karşılık, belirli bir bağlamda belirli bir durumu sağlamak maksadıyla, belirli bir zaman diliminde ve belirli bir yapı içerisinde ortaya çıkmış olan belirli tepkilerin biçim ve niteliklerinin tespit edilmesi çabasının bir eseridir. Bu çerçevede söz konusu çabanın akademik ve somut boyutunu oluşturan tez çalışması, üç safhada yürütülmüştür.

Birinci safhada, araştırma konusu ile ilgili olan temel kavramlardan hareketle, kapsamlı bir literatür taraması yapılmıştır. Bu aşamada yürütülen çalışmalar kapsamında; gerek kavramsal çerçeve oluşturulmuş, gerekse de çalışmanın ikinci aşamasında ele alınmış olan hukuksal ve idari düzenlemeler tespit edilmiştir. Bunun yanı sıra, ABD'li uzmanların ve güvenlik karar alıcılarının asimetrik ve siber tehditlere ilişkin yaklaşımlarını eleştirel bir bakış açısı ile ele alan kaynaklar özel olarak incelenerek, sonraki aşamalarda yürütülecek olan analiz ve sentez süreçleri için temel tartışma noktaları tespit edilmiştir.

İkinci safhada, 11 Eylül 2001 tarihinden sonra siber güvenlik alanında ABD'de hayata geçirilmiş olan hukuksal düzenlemeler ile istihbarat, ulusal savunma, ulusal güvenlik ve iç güvenlik alanlarında geliştirilen politikalara ilişkin belgeler, asimetrik tehdit bağlamında kapsamlı bir inceleme ve değerlendirmeye tabi tutulmuşlardır. Bu çerçevede "siber" kavramı, sadece internet veya kişisel bilgisayarları içerecek biçimde ele alınmayarak; savunma, güvenlik ve istihbarat alanlarında yoğun bir biçimde kullanılan elektronik sistemleri de içerecek biçimde, "iletişim" ve "enformasyon" olgularına da yer veren çok daha geniş bir perspektiften yorumlanmıştır.

Üçüncü safhada ise, önceki aşamalarda ulaşılmış olan bilgiler ve yapılmış olan tespitler nitel analiz yöntemleri kullanılmak suretiyle analiz edilmiştir. Söz konusu analiz süreci neticesinde ulaşılan sonuçlar ise, nesnel bir yaklaşımla ele alınarak, çalışmanın gerek ilgili kısımlarında, gerekse de sonuç kısmında paylaşılmıştır.

Çalışmanın asli veri kaynağı; literatürde yer alan kitap ve akademik çalışmalar ile resmi rapor ve dokümanlardır. Daha önceden de ifade edildiği üzere, araştırmanın yabancı bir ülke ve onun ulusal güvenlik algısı ile bağlantılı bir konu üzerine yapılıyor olması, "Gizli" gizlilik dereceli olanlar başta olmak bazı veri ve kaynaklara ulaşılmasını engellemektedir. Bu açıdan, ilgili tüm veri, kaynak veya olguların çalışma kapsamında tespit edilebildiğini ileri sürmek mümkün değilse de; çalışmanın konu ve kapsamı içerisinde yer alan kavramlar arasındaki ilişkileri genel ve açık olarak ortaya koyabilmek, bahse konu ilişkilerden ortaya çıkan somut sonuçları tespit edebilmek ve gelecekteki çalışmalar için bir vizyon ve çerçeve sağlayabilmek için yeterli veri ve kaynağa fazlasıyla ulaşılabilmiştir. Bu çerçevede literatür taraması faaliyeti olabildiğince geniş kapsamlı yürütülmek suretiyle; çalışmanın konu ve kapsamına ilişkin olarak "güvenlik" kaynaklı ortaya çıkan bahse konu sınırlılığın etkisi asgariye indirilmeye çalışılmıştır.

Araştırma konusunun karakteristik özellikleri nedeniyle, çalışma kapsamında ulaşılan bilgilerin ve yapılan tespitlerin betimlenmesinde, analizinde ve yorumlanmasında nitel analiz teknikleri kullanılmıştır. Temel veri toplama tekniği olarak "literatür taraması yöntemi"nin benimsenmiş olduğu bu çalışma kapsamında, "doküman incelemesi yöntemi"nden de faydalanılmıştır.

Çalışmanın sonuç kısmında, araştırma sorularına verilen açık ve net yanıtlara yer verilmiştir. Bahse konu yanıtların yanı sıra çalışma kapsamında önceden yapılmış olan tespitlerin de bir araya getirilerek genel bir değerlendirmeye tabi tutulmuş oldukları bu kısım, aynı zamanda çalışmanın en spekülatif ve öznel bölümünü oluşturmaktadır.

BİRİNCİ BÖLÜM

KAVRAMSAL VE KURAMSAL ÇERÇEVE

Çalışma kapsamında öncelikli olarak kavramsal çerçevenin oluşturulması suretiyle; hem önemli kavramlara ilişkin temel bilgilerin verilmesi, hem de bahse konu kavramların çalışmanın ilerleyen kısımlarında nasıl ve hangi kapsamda ele alınacaklarına ilişkin bir çerçeve yapının oluşturulması amaçlanmıştır. Araştırma konusu ile ilişkili kavramların tanımlanması -ve dolayısı ile de sınırlandırılması- sonucunda ortaya çıkan kavramsal çerçeve, aynı zamanda çalışmanın niçin belirli kavramlara odaklanmış olduğuna, söz konusu kavramların birbirleriyle olan ilişkilerine ve genel perspektif içerisindeki -kritik- konumlarına ilişkin bir ön fikir verme işlevini de yerine getirmektedir. Bu nedenle, kavramsal çerçeve içerisinde yer verilen kavramlar, genel olarak "ulusal güvenlik" özel olarak ise "siber güvenlik" olgusu üzerinde yarattıkları benzer etkiler ve sonuçlar üzerinden gruplandırılarak ele alınmışlardır.

Olguların ve aralarındaki ilişkilerin ortaya konulmasına odaklanan, herhangi bir teoriye dayanmayan ve herhangi bir hipotez geliştirme kaygısı taşımayan bu çalışmanın kuramsal çerçeve kısmında ise; özellikle güvenlik tehditlerinin algılanmaları ile ilişkili süreçlerin açıklanmasında faydalı olabilecekleri değerlendirilen bazı teorik yaklaşımlara kısaca yer verilmiştir. Söz konusu yaklaşımlara kuramsal çerçeve kısmında yer verilmek suretiyle ulaşılmak istenilen amaç; hem her türlü güvenlik politikasının analiz edilmesinde kullanılma kapasitesine sahip olan bu teorilerine ilişkin belirli bir farkındalık yaratmak, hem de çalışmada ortaya konulan olguların ve yapılan tespitlerin içerisinde değerlendirilebilecekleri örnek -bilimsel- düşünce çerçeveleri sunmaktır.

1. KAVRAMSAL ÇERÇEVE

a. Küreselleşme, Postmodernite ve Dördüncü Nesil Savaş

Küreselleşme, postmodernite ve dördüncü nesil savaş olgularının bir arada ele alınmalarının temel nedeni; küreselleşme ile birlikte güvenlik tehditlerinin ciddi bir biçimde artmasına ve bu tehditlere ilişkin algıların hızla değişmesine paralel olarak, gerek postmodernitenin yarattığı sosyal gerçekliğin, gerekse de dördüncü nesil savaş konseptinin öngördüğü savunma yaklaşımının, "belirsizlik" ve "asimetri" kavramlarını -ulusal- güvenlik gündeminin üst sıralarına taşımış olmasıdır. Küreselleşme ve postmodernite olgularının siyasal ve sosyal hayattaki köklü ve dönüştürücü etkileri göz önüne alındığında, güvenlik gündemindeki bu değişimin de kaçınılmaz olduğununu ileri sürmek mümkündür.

(1) Küreselleşme *(Globalization)*

Soğuk Savaş sonrası dönemde dünyanın içerisine girmiş olduğu küreselleşme süreci ile birlikte; devlet dışı aktörlerin yükselişi ve egemen ulus devletlerin güçlerinin erozyona uğraması, siyasal ve ekonomik sınırların ve sınırlamaların büyük oranda zayıflaması, iletişim ve bilişim alanları başta olmak üzere teknolojinin giderek artan önemi ve yarattığı bağımlılık, terörizm ile somutlaşan ve ulusal güvenlik kaygılarının merkezinde yer alan asimetrik tehditlerin hem nitel olarak çeşitlenmesi hem de nicel olarak artması gibi, güvenlik gündemi ve politikaları üzerinde derin etkilere sahip birçok yeni durum ortaya çıkmıştır.

Siyaset ve güvenlik alanındaki etkilerinin yanı sıra, küresel ekonomi ve ticaret, küresel mali krizler ve küresel bağımlılık gibi, ekonomi ağırlıklı kavramlar da küreselleşmenin birer ürünü olarak gündelik

hayatımıza dahil olmuşlardır. Nitekim, küreselleşmeyi özellikle ekonomik ilişkiler ve "küresel bağımlılık" üzerinden ele alan Puşcaş'a göre (2010: 9); literatürdeki pek çok ismin de üzerinde mutabık olduğu üzere, küreselleşmenin sonucu olarak ortaya çıkan bağımlılığı yönetmek, küresel dengesizlik (asimetri) ile yüzleşmek ve denge (simetri) oluşturmak anlamına gelmektedir.

Teeple ise, küreselleşmenin özellikle ulus devletler üzerindeki etkilerini, neyi yarattığı üzerinden değil de, neyi yok ettiği üzerinden, şöyle ifade etmektedir (2009: 49):

> "Devlet ve sivil toplum ulusal olarak kaldığı, işsizlik sınırlandığı ve maddi imkanlarda bir iyileşme umudu olduğu sürece, ulusal hükümetlerin meşruiyeti korunabilirdi."

Teeple'nin küreselleşmeye ilişkin eleştirel bakış açısı, siyasetin, toplumun, umutların ve ekonominin küreselleştiği bir dünyada güvenliğin ne kadar ulusal kalabileceği sorusunu da akla getirmektedir. Bu kapsamda, konvansiyonel ve nükleer savaşların rasyonel bir seçenek olmaktan oldukça uzaklaştığı ve daha fazla aktörün asimetrik tehdit yaratma potansiyeline sahip olduğu küreselleşen bir dünyada terörizm; hem devletleri birbirleri ile işbirliği yapmaya zorlamakta hem de ulusal güvenliği sürekli ön planda tutmak suretiyle ulusal hükümetleri güvenlik boyutunda kuvvetlendirmektedir.

Özellikle ekonomik açıdan dışa kapalı ve kendi kendine yeten ulus-devlet anlayışını çağdışı bırakmakla birlikte, ulus devletlerin iki kutuplu dünyasının yaratıcı performansını da sergilemekten oldukça uzak olan küreselleşmiş dünyanın "yeni" düzeni; ne kollektif güvenlik, ne de uluslararası politika alanlarında, -NATO veya BM benzeri- kendi damgasını taşıyan ve ideolojisini yansıtan yapılar üret(e)memiştir. Esas itibari ile Soğuk Savaştan miras kalan bir yapı içerisinde işleyen küreselleşme süreci çerçevesinde; ulus devletler, ekonomi alanındakiler başta olmak üzere pek çok yapının "ulusal olma" niteliğini yitirmesine rıza gösterirlerken, kendi ulusal güvenlik yaklaşım ve yapılarını azami derecede muhafaza etmeye gayret göstermektedirler. Bu eğilim içerisinde, özellikle ciddi terör eylemlerine muhatap olunması sonrasında, -11 Eylül

Saldırıları sonrası ABD örneğinde olduğu gibi- ulusal güvenlik ve istihbarat yapılarının daha da güçlendirilmesinin bir sonucu olarak; temel hak ve hürriyetlerde ciddi bir geriye gidiş olduğu eleştirileri de yaygın bir biçimde dile getirilmektedir.

Küreselleşme ile terörizm arasında teşvik edici bir ilişki olduğunu ileri süren ve bu ilişkiyi psikolojik temelde ele alan Moghaddam'ın da dikkati çektiği gibi (Moghaddam, 2008: 6); küreselleşmenin pek çok farklı yüzü bulunmakta ve dolayısı ile de dünyanın farklı yerlerinde oldukça farklı biçimlerde görülmekte ve anlaşılmaktadır.

İster Henry Kissinger tarafından yapıldığı gibi, ABD'nin en önemli rolü oynayacağı kaçınılmaz bir süreç olan "Yeni Dünya Düzeni" olarak isimlendirilsin (Wikipedia [web], 2012b), isterse de Lyndon LaRouche Jr. tarafından yapıldığı gibi, "Yeni Emperyalizm" olarak isimlendirilsin (2005: 6); pek çok farklı isimlendirme ve tanımlamaya sahip olan "küreselleşme" ile birlikte dünyamızın Soğuk Savaş dönemindekinden oldukça farklı sosyal, politik ve ekonomik iklimleri yaşamaya başladığı açıktır.

Nitekim İngiliz siyaset bilimcileri David Held ve Anthony G. McGrew küreselleşmeyi, tarihsel süreç içerisinde kazanmış olduğu, şu dört ana karakteristik özellik üzerinden tanımlamaktadır (2007: 2-3):

- Siyasal sınırları aşan sosyal, siyasal ve ekonomik faaliyetlerden doğan bir gerilimi içermesi,

- Sosyal gerçekliğin neredeyse her alanının(ekonomi, ekoloji, sağlık, güvenlik vb.) birbirleri ile olan bağlantılarının giderek artan büyüklüğü veya yoğunluğu,

- Fikirlerin, malların, enformasyonun, sermayenin ve teknolojinin dünya üzerinde hareketlerini hızlandıran yeni ulaştırma ve iletişim sistemlerinin gelişmesi ile birlikte, sınıraşan etkileşim ve süreçlerin daha da hızlı ilerlemesi,

- Yerel olan ve küresel olan arasındaki derinleşen "yapışma" ile bağlantılı olarak, küresel etkileşimlerin artan yaygınlığı, şiddeti ve hızı.

Bu kapsamda, tam olarak ne zaman tamamlanacağı "belirsiz" olan küreselleşme sürecinden doğan "derin ve sürekli değişim" olgusunun, güvenlik alanında da pek çok algı ve yaklaşımı değiştirmesi bir anlamda kaçınılmazdır.

(2) Postmodernite *(Postmodernity)*

Günlük hayatta, akademik kaygılardan uzak bir şekilde, postmodernite ile postmodernizm kavramlarının birbirleri yerine ve aslında "modern" ya da "çağdaş" anlamına gelecek şekilde kullanıldığı sıklıkla görülebilmektedir.

Oxford Sosyoloji Sözlüğü'nde yer alan tanımına göre (2009: 585); ortaya çıktığı dış görünüm ne olursa olsun postmodernite, modern sembolik düzenlerin dağılmasını içermesinin ve tüm "evrenseller"in varlığını inkar etmesinin yanı sıra hayal gücünün, yaratıcılığın, uyuşmazlığın, çelişkilerin araştırılmasının ve ölçülemeze karşı hoşgörülü olunmasının kültürüne de yer vermektedir.

Postmodernizm akımının -ve teriminin- ise, 1960'lı yıllarda sol eğilimli politikaların yükselişinin ardından inşa edilen, sosyal eleştiri *(social criticism)* dalgası ile sosyoloji alanına giriş yaptığını belirten Macionis; postmodern düşüncenin birçok değişik biçimi olmasına rağmen şu beş noktayı paylaştıklarına dikkati çekmektedir (1997: 652-653):

"* Önemli noktalarda, Modernizm başarısız olmuştur.

* 'İlerleme'nin parlak ışığı sönmektedir.

* Bilim gerekli cevapları artık sağlayamamaktadır.

* Kültürel tartışmalar yoğunlaşmaktadır.

* Sosyal kurumlar değişime uğramaktadır."

Postmodernitenin somutlaştığı toplumlara ilişkin günümüzdeki tartışmaların endüstri sonrası toplum tartışmalarının ötesine geçtiğini ifade

eden Schaefer; postmodern toplumu -Brannigan'a atfen-, *"tüketici ürünleri ve medya imajları ile meşgul olan, teknolojik açıdan gelişmiş bir toplum"* olarak tanımlamaktadır. Schaefer'in dikkat çektiği üzere böyle toplumlar, malları ve enformasyonu kitlesel ölçeklerde tüketmektedirler (Schaefer, 2005: 119).

Postmoderniteyi somut toplumsal sonuçları açısından ele alan Lawson ise (1993: 301); kültürel gücün, postmodern dünyada politik etkilere sahip olan ve "gerçekliği" yaratmak ile itham edilen medyada imajların manipüle edilmesi olarak, gücün postmodern toplumdaki en önemli hali biçiminde görüldüğünü belirtmektedir. Bir topluluğun dayandığı sosyal temelin ne olduğu noktasında, postmodern toplumda medyanın rolüne dikkat çeken Lawson; ayırt edici bir gençlik altkültürü fikrinin şekillenmesinde medyanın oynadığı merkezi rolün farkına varan bazı sosyologların, postmodern vatandaşların bir aidiyet duygusu tanımlayabilecekleri ve taşıyabilecekleri "hayali topluluklar"ın inşa edilmesinde de medyanın kullanıldığını ileri sürdüklerini ifade etmektedir (1993: 248). Bu kapsamda postmodernitenin -özellikle medya üzerinden yaygınlık kazanan- toplumsal ve kültürel etkileri, gerek siber uzayın gerçekliğinin ve doğasının açıklanması noktasında, gerekse de tehdit ve güvenlik algılarının şekillendirilmeleri noktasında bu çalışma açısından da büyük anlam kazanmaktadır.

Güvenlik perspektifinden bakıldığında ise, küreselleşen postmodern bir dünyada özellikle "düzen" olgusunda yaşanılan erozyona ve çoğulculuğun teşvik edilmesine paralel ortaya çıkan istikrarsızlık ve belirsizlik durumları hem tehdit kaynak ve biçimlerini nicel olarak arttırmakta, hem de;

- Tehdidin varlığının,
- Tehdidin -gerçek- kaynağının,
- Tehdidin yarattığı risk seviyesinin,
- Tehdidin somutlaşma biçiminin,
- Tehdidin somutlaşacağı yer ve zamanın

önceden tahmin edilebilirliğini azaltmak suretiyle etkili güvenlik tedbirlerinin alınmasını da zorlaştırmaktadır. Dolayısı ile, özellikle -çoğunlukla sınırlı olan- mali kaynakların etkin kullanılamadığı, analiz kabiliyetinin sınırlı kaldığı ve alınan güvenlik tedbirlerinin tehdidin karakteri ile örtüşmediği durumlarda, güvenliğin sağlıklı bir biçimde sağlanması da beklenilmemelidir.

(3) Dördüncü Nesil Savaş *(Fourth Generation Warfare)*

Bu çalışma kapsamında dördüncü nesil savaşın, küreselleşme ve postmodernite ile birlikte ele alınarak açıklanmasının nedeni; özünde yer alan belirsizliğin, bulanıklığın ve istikrarsızlığın soğuk savaş sonrasının postmodern dünyasındaki politik iklim ile gösterdiği uyumdur. Nitekim gerek teknoloji kullanımına ve taraflar arasındaki asimetriye yapmakta olduğu vurgu, gerekse de var olanı sorgulayan ve mevcut olanı değiştirmeye odaklanmış yaklaşımı üzerinden, dördüncü nesil savaşın diğer iki olguya rahatlıkla eklemlenebilmesi de mümkündür. Hatta daha da ileri gidilerek; dördüncü nesil savaşın, küreselleşmiş ve postmoderniteye kaymış "çağdaş" dünyanın savaş biçimi olduğu ileri sürülebilir.

Echevarria'nın ifade ettiği üzere (2005: vı); özellikle bilginin ve teknolojinin yaygınlaşmasında ve yayılmasında küreselleşmeye bağlı olarak ortaya çıkan artış, başta terörist gruplar olmak üzere devletdışı aktörlere daha büyük bir hareketlilik ve küresel etki sağlamaktadır.

Bu çerçevede dördüncü nesil savaşın, Treglia'nın da Manwaring'den aktardığı gibi, ulus devlete yönelik olarak yarattığı tehditler ve tarafları üzerinden tanımlanabilmesi mümkündür (Manwaring, 2003'den aktaran Treglia, 2010: 1);

> "Dördüncü nesil savaş; savaş, suç ve barışın, devlet dışı aktörler (çeteler, teröristler, milisler, karteller, klanlar, korsanlar ve diğer suç oluşumları),

> sivil toplum organizasyonları ve süreçleri tarafından ulus devletlerin istikrarına yönelik tehditler olarak, kendilerini bulanık bir şekilde ortaya koydukları belirsiz bir alana ait olan bir olgudur."

Görülebileceği üzere yukarıdaki tanım, belirsizlik ve soğuk savaş sonrası uluslararası ilişkilerin yükselen yıldızları olan devlet dışı aktörler üzerine inşa edilmiştir.

Echevarria'ya göre (2005: v); dördüncü nesil savaş teorisi, özellikle 11 Eylül 2001 tarihinden sonra yeniden keşfedilmiştir.

Treglia'nın da ifade ettiği üzere; her ne kadar ABD tarafından Irak ve Afganistan'da yürütülen "Teröre Karşı Savaş" dördüncü nesil savaşın bir örneği olarak kabul edilmekte ise de, belirsizliğe vurgu yapan dördüncü nesil savaş kavramının kendisi de ironik bir biçimde, belirsizdir. Tıpkı terörizm ve onunla bağlantılı kavramlarla ilgili olarak sıkça dile getirildiği gibi, dördüncü nesil savaş olgusunun da genel kabul görmüş bir tanımı bulunmamaktadır. Bu kapsamda Treglia; 20 yıldan fazla bir süreden beri tartışılmakta olmasına rağmen, akademik çalışmasının tamamlandığı 2010 yılının Eylül ayı itibari ile, dördüncü nesil savaşın ABD Ordusu tarafından herhangi bir doktrinel yayında tanımlanmamış olmasına dikkati çekmektedir (Treglia, 2010: 13).

Doktrinel olarak açık bir biçimde ortaya konulmamış olması nedeniyle; bahse konu teoriye ilişkin eleştirel tartışmalar, resmi tanımlar veya uygulamalardan ziyade onu savunan kişilerin literatürdeki çalışmaları üzerinden ilerlemektedir.

Bu çerçevede Hoffman, dördüncü nesil savaş üzerine yapılan tartışmaların taraflarını beş ana gruba ayırmaktadır (2007b). Hoffman'a göre, birinci grup tümüyle yeni bir olgu ile karşı karşıya olunduğunu savunmakta iken; ikinci grup, dördüncü nesil savaş üzerine yapılan tartışmaları suni ve savunulamaz bulmaktadır. Üçüncü grup, dördüncü nesil savaş teorisinde tarihin seçici olarak kullanıldığını ve teorik açıdan zayıf kalındığını ifade ederken; savaşın önceki şekillerinden açıkça farklı ve görülebilir yeni bir savaş formu ile karşı karşıya olunduğu iddiası ile de dördüncü grup ortaya çıkmaktadır. Yine Hoffman'a göre, beşinci grupta

yer alanlar; savaşın evrim süreci içerisinde, yeni teknolojiler ve daha da önemlisi yeni veya yeniden ortaya çıkan çevresel veya sosyo-politik şartlara dayalı bir kışkırtmadan ziyade, savaşın seviyesindeki bir kayma ile karşı karşıya olunduğunu ileri sürmektedirler.

Dördüncü nesil savaş savunucularını *"oldukça dar odaklı ve onarılamayacak kadar kusurlu bir mantığa sahip olmakla"* ve *"tekerleği yeniden icat etmekle"* itham eden Echevarria; *"hiçbir şart altında, asla dönmeyecek bir tekerlek"* olduğunu ileri sürdüğü dördüncü nesil savaş olgusuna, "teorik olarak" da olsa kayıtsız kalamamaktadır (2005: 16-17).

Nitekim savaş olgusunun tarihsel süreç içerisinde geçirdiği değişimlere dikkati çeken Echevarria'nın da ifade ettiği üzere (2005: v); teoride, savaşın dört nesil şeklinde evrildiği kabul edilmekte ve bunlardan ilk üçünün karakteristik özellikleri, kitlesel insan gücünün kullanımı, ateş gücü ve manevra olarak sıralanmaktadır. Echevarria'ya göre dördüncü nesil savaşın karakteristiği ise (2005: v); *"bir rakibin karar alıcılarını stratejik hedeflerinin ulaşılamaz veya oldukça maliyetli olduklarına ikna etmek için mümkün olan tüm -siyasal, ekonomik, sosyal, askeri- ağların kullanıldığı, evrilmiş bir "ayaklanma" biçimi*"nin hakim olmasıdır.

21.nci Yüzyılda yaşanılacak olan çatışmaları "Melez Savaşlar *(Hybrid Wars)"* olarak nitelendiren Frank G. Hoffman, 2007 yılında yayımlanmış olan "Melez Savaşların Yükselişi" isimli çalışmasında; dördüncü nesil savaş tartışmalarını da içeren bir şekilde, askeri çatışmaların içerisinde bulunduğu evrimsel süreci, özellikle örgütlenme ve asimetri gibi karakteristik bazı özellikleri üzerinden ele almaktadır.

Treglia, Meksika'daki uyuşturucu bağlantılı organize suç örgütlerinin ABD için yaratabileceği tehdidi dördüncü nesil savaş perspektifinden ele aldığı çalışması kapsamında, Hoffman'ın dördüncü nesil savaş yaklaşımını özellikle devlet dışı aktörler bakımından ayrıntılı bir biçimde incelemektedir. Dördüncü nesil savaş kapsamında devlet dışı aktörler tarafından şiddete başvurulduğu durumları tanımlamak için, "Melez Tehdit" tabirini kullanan Hoffman (Hoffman, 2007'den aktaran Treglia, 2010: 16); yeni bir savaş biçiminin ortaya çıkmaya devam etmekte

olduğunu ve kurumların bu duruma uyum sağlamakta yavaş kaldıklarını ileri sürmektedir. Düzenli savaş, düzensiz savaş, terörizm ve yıkıcı faaliyetler arasındaki ayrımları bulanıklaştıran, savaş biçimlerinin kaynaştığı bir durum ile karşı karşıya bulunulduğunu savunan Hoffman'ın şiddetin sürekliliğine özellikle dikkati çektiğini belirten Treglia'ya göre (Treglia, 2010: 16-17);

> "Ayrımlar arasındaki bu bulanıklaşma, savaş benzeri şiddet ile suç davranışları arasındaki "gri" alanda faaliyet göstermekte olan devlet dışı aktörlerin şiddet eylemlerinde ortaya çıkmaktadır."

Nitekim Hoffman tarafından yapılan ve yukarıda özetlenmiş olan yaklaşımını yansıtan tanımına göre, hem devletler hem de devlet dışı aktörler tarafından yürütülmeleri mümkün olan "melez savaşlar" (Hoffman, 2007a: 29);

> "...geleneksel kabiliyetleri de içeren bir dizi savaş biçimini, düzensiz formasyon ve taktikleri, gelişigüzel şiddet ve zorlamayı içeren terörist eylemleri ve suç olaylarına dayalı karışıklıkları bünyelerinde biraraya getirmektedirler."

Melez savaş olgusunu, organize suç eylemleri ile dördüncü nesil savaşın iç içe geçtiği noktada ve ulaşılmak istenilen amaçlar açısından ele alan Treglia, dördüncü nesil savaşın amacını Meksika örneği üzerinden şöyle ifade etmektedir (2010: 1);

> "Dördüncü nesil savaş, hükümetin veya ülkenin siyasal sınırlarının kontrolünü ele geçirmek için değil, Meksika içerisinde kanunların uygulanamayacakları alanların, arazilerin ve ticaret rotalarının kontrolünü sağlamak için yürütülen bir mücadeledir."

Geniş bir perspektiften ve melez savaş konsepti gözönünde bulundurulmak suretiyle değerlendirildiği zaman dördüncü nesil savaş olgusu, asimetriye yaptığı vurgu ve içerdiği muğlaklık üzerinden düzensiz savaş -ve türevleri-, terörizm ve organize suç gibi oldukça hayati ulusal güvenlik tehditlerinin tek bir çatı altında biraraya getirilebilmesi için gerekli olan mantıksal ve kavramsal temeli de sağlamaktadır. Günümüzde "Asimetrik Tehditler" olarak isimlendirilen bu "çatı" altında yer alan her bir

olgu ve kavram, içeriğindeki asimetri ortak paydası üzerinden değerlendirilmekte ve güvenlikleştirilmektedirler.

Kendisine yönelik olarak sahip olunan farklı bakış açılarına göre değişik güvenlik değerlendirmelerinin yapılmasına müsait bir yapıda olan "asimetrik tehdit" olgusu, silahlı kuvvetler ile kolluk kuvvetleri arasında görev alanları üzerinden yapılan keskin ayrımları da bir anlamda yumuşatmaktadır.

Bu yaklaşım çerçevesinde düzensiz savaş olgusundan -ve türevlerinden- uzaklaşılarak suç eylemlerinin ön plana çıktıkları melez savaş olgusuna yaklaşıldıkça, güvenliğin sağlanması sorumluluğunun da doğal olarak silahlı kuvvetlerden kolluk kuvvetlerine doğru kaymasının beklenilmesi mümkündür. Bununla birlikte düzensiz savaş -ve türevleri-, terörizm, organize suç, çıkar amaçlı suç ve kaçakçılık gibi olgular ile ilişkili tanımların ve bunlarla ilintili örgüt tipolojilerinin net bir biçimde ortaya konul(a)madığı, bu duruma bağlı olarak da kesin yetki ve sorumluluk dağılımının yapıl(a)madığı bir güvenlik ortamında; silahlı kuvvetlerin ve kolluk kuvvetlerinin yetki ve sorumluluk alanları arasında ortaya çıkabilecek boşluklarda, devlet dışı aktörler yaşama ve eylemde bulunma imkanını rahatlıkla bulabileceklerdir.

b. Asimetrik Savaş, Terörizm ve 11 Eylül Saldırıları

İster soğuk savaş döneminde olduğu gibi nicel ve nitel esaslı karşılaştırmalara dayalı olsun, isterse de küreselleşmenin devlet dışı aktörlere ve terörizme sağladığı avantajlara vurgu yapsın, asimetrik savaş terimi daima taraflar arası bir eşitsizlik durumunu ifade etmektedir. Nitekim asimetrik savaş ve tehditlere ilişkin kaynaklar ayrıntılı bir şekilde incelendiğinde; asimetrik savaş konseptinin çoğu zaman için, sayı, örgütlenme ve teknoloji açısından zayıf olan taraf lehine örtülü bir avantajı öngördüğü farkedilecektir.

Gerek ABD'deki, gerekse de dünyanın geri kalan kısmındaki güvenlik karar alıcıları için "asimetrik tehdit"in oldukça açık ve net bir şekilde somutlaştığı 11 Eylül 2001 tarihi, dünyayı asimetrik tehditler bağlamında algılayan ve değerlendiren güvenlik anlayışı için gerçek bir milat niteliğindedir.

(1) Asimetrik Savaş *(Asymmetric Warfare)*

Soğuk Savaş döneminde, "gayri nizami harp" veya "gerilla savaşı"[2] gibi geleneksel olmayan savaş konseptlerinin genel karakterlerini ifade etmek üzere kullanılan "asimetrik savaş" ve "asimetrik tehdit" terimleri; Soğuk Savaşın sona ermesinin ardından, özellikle terörizm ile bağlantılı olarak ortaya çıkan yeni güvenlik tehditlerinin ifade edilmesi için kullanılmaya başlanmıştır.

"Asimetri" olgusunun Soğuk Savaş dönemindeki ABD askeri stratejik düşüncesi içerisinde, her zaman bu isimle anılmasa da, oldukça önemli bir yeri olduğunu ifade eden Dunn Cavelty (2008: 68); bu durumun, özellikle SSCB'nin Avrupa'daki nicel üstünlüğünün ancak ABD ve NATO'nun nitel üstünlüğü ile karşılanabileceği algısından kaynaklandığı düşüncesindedir.

Bu kritik tespite rağmen, "asimetri" olgusunun 1997 yılı Eylül ayında yayımlanmış olan "Harekat Talimnamesi"nde yer almadığını ifade eden, ABD Kara Kuvvetlerinden Binbaşı Stephen D. Pomper; aynı talimnamenin 2003 yılında yayımlanan ve dolaşımda olmayan DRAG

[2] "ABD Kara Kuvvetleri Gerilla Savaşı El Kitabı" isimli kaynaktaki tanımına göre (Department of the Army, 2009: 8); gerilla savaşı, ağırlıklı olarak yerel güçlerden oluşan kuvvetler tarafından, düşmanın muharebe etkinliğini, endüstriyel kapasitesini ve moralini azaltmak üzere, düşman kontrolünde bulunan bölgede yürütülen muharebe operasyonlarını içerir. Gerilla operasyonları, saldırgan taktikleri benimsemiş olan göreceli olarak küçük gruplar tarafından yürütülürler ve diğer askeri operasyonları da destekleyebilirler. Yine aynı kaynağa göre; gerilla savaşı saldırgan hareket ile karakterize edilmekte ve gerillalar, "hareketlilik *(mobility)*", "kaçamaklık *(elusiveness)*" ve "şaşırtma *(surprise)*" esaslarına dayanmaktadırlar. Bu özelliklerinin yanı sıra, mutlaka belirtilmesi gereken diğer karakteristikleri ise; sivil destek *(civilian support)*, dış destek *(outside sponsorship)*, siyasal yönler *(political aspects)*, hukuki yönler *(legal aspects)*, taktikler *(tactics)* ve gelişme -zaman ve uzay- cepheleri *(development aspects)*'dir (2009: 8-11).

versiyonunda[3] ise, *"örgütlenme, teçhizat, doktrin, yetenekler ve değerler açısından ABD Kuvvetleri ile (düzenli olsun veya olmasın) diğer silahlı kuvvetler arasındaki farklılıklar"* olarak, söz konusu olgunun tanımlanmış olduğuna dikkati çekmektedir (2004: 17). Bu kapsamda, bahse konu talimnameye göre;

> "Eğer kuvvetler, teknolojiler ve silahlar benzer iseler çatışmalar simetriktirler; eğer kuvvetler, teknolojiler ve silahlar farklı iseler yada terörizme başvuruluyor ve daha geleneksel angajman kuralları kabul edilmiyorsa çatışmalar asimetriktirler."

Savaştaki asimetrileri, karşı karşıya gelen güçler arasındaki dengesizlikler olarak tanımlayan ve bu farklılıkların askerlerin sayısı, teçhizat, ateş gücü, moral, taktikler, değerler veya diğer faktörler noktasında ortaya çıkabileceklerini ifade eden Kushner ise (2003: 54); hafif silahlarla donanmış partizanlar ile konvansiyonel bir ordu arasında meydana gelebilecek olan bir gerilla savaşını, asimetrik savaşa örnek olarak vermektedir. Kushner'e göre; uçak kaçırma veya intihar saldırıları gibi terörist taktikler, hem daha küçük ve zayıf olanı daha kuvvetli olana karşı saldırıya sevk etme eğilimleri, hem de sivillere yönelik saldırıların tek taraflı bir savaşa göre tanımlanması nedeniyle asimetrik olarak kabul edilirler.

Nitekim Kushner'in de yukarıda değinmiş olduğu nedenler ile, asimetrik tehdit terimi; dar anlamı ile, teröristlerin özellikle konvansiyonel askeri hedeflere yönelik olarak asimetrik savaş taktik ve tekniklerini kullandıkları durumları ifade etmek için, geniş anlamı ile ise, terör örgütlerince sivil asker ayrımı gözetmeksizin yapılan her türlü saldırıyı kapsayacak biçimde kullanılmaktadır. Yine bu kapsamda, gerek Kushner'in çalışmasında ve gerekse de diğer birçok kaynakta, "dördüncü nesil savaş", "gerilla savaşı", "konvansiyonel olmayan savaş", "düşük yoğunluklu savaş" veya "Terörizm" terimleri için de "asimetrik savaş" terimine atıfta veya göndermede bulunulmaktadır.[4]

---

[3] FM 1-03, Operations—DRAG

[4] Bu kapsamda bahse konu kavramlar arasında mutlak bir çakışma olmayıp; konvansiyonel savaş konseptinden uzaklaşmış olmalarının yanı sıra benzeri taktik ve stratejileri benimsemeleri noktasında da ortaya çıkmış olan bir yakınlaşmadan söz edilebilmesi mümkündür. Bahse konu yakınlaşma çerçevesinde dikkat çekici nitelikte olan bir nokta ise; gerilla savaşı taktiklerinin ve

Bu kapsamda, Henry Kissinger tarafından Vietnam Savaşı üzerinden gerilla savaşı olgusuna ilişkin olarak yapılmış olduğu tespitler -dolaylı olarak da olsa- asimetrik savaş olgusunun doğasının ve asimetrik tehditlerin karakterlerinin ortaya konulması açısından oldukça önemlidir (Kissinger, 1994: 629):

> "Konvansiyonel bir savaşta, muharebedeki yüzde 75'lik bir başarı oranı zaferi garantiler. Gerilla savaşında ise, vaktinizin sadece yüzde 75'inde nüfusu korumak yenilgi getirir. Ülkenin yüzde 75'inde sağlanan yüzde 100 güvenlik, ülkenin yüzde 100'ünde sağlanan yüzde 75 güvenlikten çok daha iyidir. Eğer savunan kuvvetler -en azından önemli kabul ettikleri bir bölgede- nüfus için neredeyse mükemmel bir güvenlik sağlayamazlarsa; gerillalar er ya da geç savaşı kazanır.
>
> Gerilla savaşının temel denklemi, hayata geçirmesinin zor olduğu kadar da basittir: gerilla ordusu, kaybetmekten uzak kalabildiği sürece kazanır; konvansiyonel ordu, kesin bir biçimde kazanmadıkça kaybetmeye mahkumdur. Bir kilitlenme durumu, neredeyse asla meydana gelmez. Kendisini bir gerilla savaşına sokan her ülke uzun bir mücadele için hazır olmalıdır. Gerilla ordusu, büyük oranda azalmış kuvvetlerle bile, vur-kaç taktiklerini uzun bir süre devam ettirebilir. Açık seçik bir zafer oldukça seyrektir; başarılı gerilla savaşları, uzun bir zaman sürecine yayılarak tipik bir biçimde tavsarlar."

Denver Üniversitesi'nden Tom J. Farer'in aşağıdaki görüşleri ise, asimetrik tehditlerin küreselleşen dünyadaki yerlerini ve ABD başta olmak üzere pek çok ülkenin güvenlik gündemlerindeki önemini ortaya koyan kısa bir özet mahiyetindedir (Farer, 2004: 44):

> "Savaş bizim kaderimizdir. Konvansiyonel bir savaş, bizimki gibi bir askeri güce sahip olan bir ülke için, küçük bir mesele olurdu. Ancak küreselleşme çağında, asimetrik savaşa karşı mücadele etmek zorundayız. Açık toplumun düşmanları, ordularımıza karşı duramadıkları andan itibaren, siviller ve onları destekleyen altyapılar gibi yumuşak hedeflere yönelmişlerdir...

---

stratejilerinin ortak paydayı oluşturmalarıdır. Bu çerçevede, yol gösterici bir mahiyette kullanılmak üzere; Wikipedia İnternet Sitesi <http://en.wikipedia.org/wiki/Asymmetric_warfare> adresinde yer almakta olan *"Asymmetric Warfare"* maddesinin yanı sıra yine aynı internet sitesinde yer almakta olan *"4th Generation Warfare"*, *"Guerilla Warfare"*, *"Unconventional Warfare"*, *"Low Intensity Conflict"* ve *"Terrorism"* maddelerinden faydalanılabilmesi de mümkündür. Basılı literatür kapsamında ise; H.W. Kushner, K.L. Lerner ve B.W. Lerner, S.K. Anderson ve S. Sloan ya da R.J. Samuels gibi yazarların bu çalışmanın kaynakçasında da yer almakta olan eserlerine başvurulmasının uygun olabileceği değerlendirilmektedir.

...Dünya Ticaret Merkezinin yıkımı, kitle imha silahlarından yararlanılmaksızın yürütüldüğü zaman dahi, asimetrik savaşın sahip olduğu ölümcül potansiyelini resmetmiştir. Alışılmadık silahların karışımı ile birlikte ise, tarifsiz felaket görüntüleri akıllara gelmektedir."

Asimetrik savaşı, asimetrik aktörlerin stratejik amaçlarına ulaşabilmek amacıyla karşı gücün iradesini kırmak üzere, onun güvenlik açıklarına taktik ve operasyonel kuvvet uygulamak suretiyle orantısız bir güç elde etme çabası olarak tanımlayan McKenzie'ye göre ise (McKenzie, 2000'den aktaran Rodin, 2006: 154), böyle bir savaşta kullanılabilecek asimetrik silah ve taktiklerin şu altı ana başlık altında ele alınabilmesi mümkündür:

- Kimyasal Silahlar
- Biyolojik Silahlar
- Nükleer Silahlar
- Enformasyon Savaşı
- Terörizm
- Alternatif Operasyonel Konseptler (gerilla taktikleri, devlet dışı aktörlerin muharebelere müdahil olmaları, askeri kuvvetler ve tesisler ile sivil topluluklar ve altyapının birbirleri içine sokulmaları, sivillerin canlı kalkan olarak kullanılmaları, çarpışma sahalarının ileri teknoloji silahların etkilerini azaltacak olan karmaşık şehir ortamlarına kaydırılması, ilkel silah ve teknolojilerin şaşırtıcı biçimlerde kullanılmaları).

Tek başlarına olduğu kadar bir arada kullanılabilmeleri de mümkün olan yukarıdaki asimetrik silah ve savaş taktiklerine ilişkin olarak Samuels ise, bu çalışmanın konusu ile de doğrudan ilişkili olan terörizm ve enformasyon savaşı olgularını birbirlerine yaklaştıran bir anlayışa örnek olarak; ERRI tarafından 1998 yılında yayınlanmış olan "Asimetrik Savaş, Terörizmin Evrimi ve Devredilmesi: Acil Durum ve Ulusal Güvenlik Kuvvetleri için Yaklaşan Meydan Okuma" başlıklı rapora atıfta bulunmaktadır (Samuels, 2006: 50). Samuels tarafından ifade edildiği üzere; ABD'nin yakın geleceğinde yüzleşmek zorunda kalacağı

çatışmaların asimetrik karakterde olacaklarının ileri sürüldüğü söz konusu rapor çerçevesinde, ABD'nin bilgisayar altyapısına karşı girişilebilecek muhtemel siber saldırılara ise özellikle dikkat çekilmektedir.

(2) Terörizm *(Terrorism)*

1790'lı yılların Devrim Fransa'sında iktidarda bulunan Robespierre'in jakoben -Halk- hükümetinin, "Terör Dönemi *(Reign of Terror)*" olarak da anılan iktidarı süresince bu dönemin sembolü ve aracı olan giyotin ile 17.000 idam gerçekleştirdiğini ifade eden Barker; bu uygulamayı eleştiren dönemin muhafazakâr İngiliz siyasetçilerinden Edmund Burke'nin, "terörizm" ve "terörist" terimlerini ilk kullanan yazarlardan biri olduğunu ileri sürmektedir (Barker, 2003: 10).

Terörizm olgusuna, devlet dışı yapılar tarafından politik amaçlarla girişilen şiddet eylemleri perspektifinden yaklaşıldığı zaman ise, Hasan Sabbah'ın kontrolü altında faaliyet göstermiş olan Haşhaşi Tarikatının eylemlerinin de terörizmin ilk örnekleri arasında sayılabilmesi mümkündür.

Nitekim terörizm tarihinin şiddetin politikayı etkilemek maksadıyla kullanılmasına yönelik insan iradesi kadar eski olduğunu ifade eden Amy Zalman'a göre([web] 2012); milattan önce 1.nci Yüzyılda etkin olan Musevi kökenli *"Sicarii"* grubunun ya da milattan sonra 11.nci ve 13.ncü Yüzyıllar arasında etkin olan Haşhaşi tarikatının eylemleri, terörizmin tarihsel örnekleri arasındadır.

Dünya genelinde kabul görmüş ortak bir terörizm -ve dolayısı ile de terörist- tanımlamasının olmaması ve üzerine pek çok akademik çalışma yapılmış olmasına rağmen insanlığın halen bir güvenlik tehdidi olarak terörizm olgusu ile birlikte yaşamak zorunda olması, onu tam anlamıyla bir fenomen haline getirmektedir.

Birleşmiş Milletler Üniversitesinde görevli E. Newman'a göre, "terörizm"i tanımlamak analitik olduğu kadar politik de bir meydana

okumayı da içermektedir (2007: 119). W. Laqueur'un terörizme ilişkin genellemelerin "neredeyse her zaman yanıltıcı" olduğuna, J.I. Rose'un ise terörizme ilişkin akademik çalışmaların "tanımlama açısından zengin ancak analitik olarak çorak" olduğuna dair tespitlerine dikkati çeken Newman; çok geniş bir dizi fenomeni tarif etmek için tek bir terimin – terörizm- kullanılmasının metodolojik açıdan oldukça sorunlu olduğunu ifade etmektedir (Newman, 2007: 119).

Dünya ülkelerinin siyasal çıkarlarının çatışması nedeniyle müşterek bir terörizm tanımı yapılamadığına dikkati çeken Teeple (2009: 37); terörizmi, devletin ve toplumun varlığına kasteden bir tehditten ziyade, bir araç –uygulama, taktik veya strateji- olarak kabul etmek suretiyle yapılacak olan tanımlamaların olumlu sonuçlar vereceğini savunmaktadır. Bu çerçevede, terörizmin "amaç değil araç olma" niteliğine sıklıkla vurgu yapan Teeple'nin kendisine çıkış noktası olarak aldığı ve şiddete vurgu yaptığı tanıma göre; "Terörizm", insanları belirli bir istikamete doğru zorlamak üzere –şiddet kullanmak veya kullanma tehdidinde bulunmak suretiyle- fiili sindirme uygulanmasıdır.

Bu yaklaşıma göre; terörizmin ve kendisinde somutlaştığı şiddet eylemlerinin amacı, muhatap ülkeyi siyasal olarak fiilen parçalamak veya o ülke vatandaşlarını öldürmek değil, stratejik hedeflere ulaşma yolunda o ülke insanlarını ve güvenlik karar alıcılarını yönlendirebilecek bir etki yaratmaktır. Bu tanımı ile, politik açıdan zayıf olanın başvuracağı asimetrik bir araç niteliğine bürünen terörizm; asimetrik tehdit olgusunun özünde var olan istikrarsızlık yaratma kapasitesini de açık bir biçimde ortaya koymaktadır. Bu çerçevede, sayıca az ve kuvvetçe zayıf olanın görüşleri kabul edilmedikçe veya hedef toplumun iradesi kırılmadıkça şiddet eylemlerinin devam etmesi ve böylelikle de toplumun, ödeyeceği bedeller üzerinden sindirilmeye çalışılması muhtemeldir. Bu sürecin, bugüne kadar ki pek çok örnekte de görüldüğü gibi, uzun ve yıpratıcı olacağı açıktır.

Terörizmin kesin bir biçimde şiddet içerdiğini ve bunun aynı zamanda politik bir şiddet olduğunu ifade eden Held ise, geleneksel terörizm tanımlarının içerisinde barınan bir tanım sorununa da dikkati çekmektedir (Held, 2008: 17):

> "Sivillerin hedef alınmasının mutlaka terörizm tanımı içerisinde yer alması gerekliliği ve böyle bir hedef almanın diğer siyasal şiddet türlerini de terörizm haline getirip getirmediği iki önemli tanımsal meseledir."

Yaygın yaklaşımda, var olan bir siyasal güç mücadelesinin şiddete dayalı bir aracı olarak görülen terörizm; sahip olduğu siyasal ve sosyal boyutlardan soyutlanarak, tümüyle teknik açıdan ele alındığı noktada ise asimetrik savaş olgusu ile örtüşmektedir.

Terörizmi asimetrik savaşın bir biçimi olarak kabul eden ve yine asimetrik savaşın diğer bir biçimi olan gerilla savaşı ile arasındaki temel farka dikkati çeken Mirabello'ya göre (2009: 270); teknolojik açıdan ilerlemiş, zengin ve gelişmiş bir altyapıya sahip olan devletlerde, geleneksel gerilla savaşından ziyade terörizm ile karşılaşılması daha muhtemeldir. Mirabello bu durumun gerekçesini, dikkat çekici bir biçimde, şöyle ortaya koymaktadır:

> "Zengin devletlerin lüks ve refah ile yumuşamış vatandaşları, geleneksel bir ayaklanmanın yokluk, fedakarlık ve zahmetlerine dayanamadıklarından dolayı, kırsal kesimde bir gerilla harekatı yürütmekten acizdirler. Onlar sadece şehirlerdeki terörizm için uygundurlar."

Bu çalışmanın konusu göz önünde bulundurulduğunda, ele alınan ve tanımlanmaya çalışılan hemen hemen her olgunun bugün için karşı karşıya olunan biçimleri ile, çok daha önceden tanımlanmış olan geleneksel biçimleri arasında; ister küreselleşmeye, ister postmoderniteye, isterse de hızla ve sürekli olarak gelişen teknolojinin etkilerine dayandırılsın, bariz farklar olduğu açıktır. Nitekim bu genel yönelim içerisinde, herhangi bir ayrıcalığı olmayan terörizm olgusunun da değişime uğramakta olması son derece doğaldır.

Ian O. Lesser ve çalışma arkadaşları, 1999 yılında RAND için yapmış oldukları bir çalışmada; örgütlenme, doktrin, strateji ve teknoloji boyutlarında yaşanan değişimlerin tümü birlikte ele alındığında ortaya çıkan olguyu, "Yeni Terörizm *(New Terrorism)*" olarak nitelendirmişlerdir. Yaşanılan değişimin üç ana boyutunun olduğunu ve terörizmin, "Ağ Savaşı

(Netwar)" olarak isimlendirdikleri, yeni bir yönde evrildiğini savunan bahse konu yazarlara göre (Lesser ve diğerleri, 1999: 40-41);

- Örgütlenme alanında; liderlik esaslı hiyerarşik tasarımlar enformasyon çağının ağa dayalı ve merkezi olmayan tasarımları lehine güç kaybedecek ve internete bağlı ulusaşan grup dizileri oluşturma çabalarında artış görülecektir.

- Doktrin ve Strateji alanında; teröristler yeni yetenekler kazanırken, enformasyon operasyonlarının geleneksel eylem biçimleri kadar kullanışlı bulunmaları durumunda, "sistemik bozulmalar *(systemic disruption)*" yaratmak, hedeflerin yok edilmesi kadar önemli birer amaç haline gelebilecektir.

- Teknoloji alanında; gelişmiş enformasyon teknolojileri, örgütsel yapıların desteklenmesi için olduğu kadar, saldırı ve savunma maksatlı olarak da artan bir şekilde kullanılabileceklerdir.

Örgütlenme, doktrin, strateji ve teknolojilerin enformasyon çağına uydurulmuş biçimlerinin kullanıldığı "ağ savaşı"nı, gelişmekte olan bir çatışma ve suç biçimi olarak tanımlayan Lesser ve çalışma arkadaşları (1999: 47-48); birçoğunun devlet dışı nitelikte olduğu ağ savaşı aktörleri arasında "Siber Sabotajcı *(Cyboteur)*"lara da yer vermektedirler.

Enformasyon teknolojilerine vurgu yapan "yeni terörizm" yaklaşımının ortaya atılmasından kısa bir süre sonra gerçekleştirilen 11 Eylül Saldırıları, geleneksel terörizm biçimlerine ve eylemlerine ilişkin mevcut güvenlik kaygılarını pekiştirirken, ABD topraklarının terörizm karşısındaki dokunulmazlığını da ciddi biçimde sorgulanır hale getirmiştir. Bu çerçevede 11 Eylül Saldırıları öncesi dönemde, ABD'nin terörizme ilişkin sahip olduğu tehdit algısının; denizaşırı ve ağırlıklı olarak da Ortadoğu'daki askeri varlığına yönelik geleneksel terör eylemlerine dayandığını ileri sürmek yanlış olmayacaktır.

Nitekim bomba yüklü araçlar ile; 1983 yılında, Beyrut'taki ABD Deniz Piyadeleri Kışlasına yapılan ve 241 ABD askerinin hayatını

kaybettiği intihar saldırısı[5] ile 1996 yılında, Suudi Arabistan'ın El Khobar şehrindeki ABD askeri hedeflerine yapılan ve 19 Amerikan vatandaşının hayatını kaybedip 372'sinin de yaralandığı intihar saldırıları[6], 11 Eylül 2001 öncesi dönemde ABD hedeflerine yönelik girişilmiş olan ve ABD'deki tehdit algısını şekillendiren önemli geleneksel eylem örneklerini oluşturmaktadır.

Bunun yanı sıra Samuels'in de dikkat çektiği üzere (2006: 17-18); El Kaide lideri Osama Bin Laden'in, İran bağlantılı olarak patlayıcı maddelerin elde edilmesine yardım etmek suretiyle, El Khobar Saldırılarını gerçekleştiren saldırganlara destek sağlamış olabileceği hususu da ABD Kongresi bünyesinde oluşturulan 11 Eylül Saldırılarını Araştırma Komisyonu tarafından 2004 yılında ifade edilmiştir.

Dolayısı ile siber tehditlerin, "yeni terörizm" ya da "ağ savaşı" adı altında güvenlik gündeminde yer edinmelerine ilişkin ilk işaretlerin ortaya çıkmakta olduğu bir dönemde; en geniş zararı vermek için -bomba yüklü olmamakla birlikte- yolcu uçaklarının kullanıldığı ve islami kimliğe sahip teröristlerin ABD'nin ekonomik ve askeri güç sembollerine yönelik giriştikleri 11 Eylül Saldırıları, geçmiş dönemdeki tecrübelerden çok da farklı bir özellik göstermemişlerdir. Böylelikle 11 Eylül Saldırıları sonrasında; ABD'nin terörizme ilişkin sahip olduğu tehdit algısı, tehdidin denizaşırı karakteri haricinde pek çok yönden pekişirken, ABD topraklarındaki muhtemel terör eylemlerine ilişkin olarak yeni bir asimetrik -iç- tehdit algısı da net bir biçimde ortaya çıkmıştır.

(3) 11 Eylül Saldırıları *(the September 11 Attacks)*

"9/11 Saldırıları *(9/11 Attacks)*" olarak da anılan ve ABD hedeflerine yönelik olarak 11 Eylül 2001 tarihinde gerçekleştirilen terör saldırıları, Turner tarafından kısaca şöyle özetlenmektedir (Turner, 2006: 202):

[5] Veriler (Samuels, 2006: 446)'dan alınmıştır.
[6] Veriler (Samuels, 2006: 17)'den alınmıştır.

"...New York'da bulunan Dünya Ticaret Merkezi kulelerine ve Washington D.C.'nin banliyösünde yer alan Pentagon'a yapılmış bir dizi koordineli intihar saldırısıdır. Saldırılar üç yolcu uçağının kaçırılması ve hedef binalara çarptırılması biçiminde gerçekleşmiştir. Kaçırılmış olan dördüncü bir yolcu uçağı ise, Pennsylvania'nın kırsal kesiminde bir alana düşmüştür. ABD hükümetinin El Kaide'nin sorumlu olduğunu düşündüğü saldırılarda yaklaşık 3000 kişi hayatını kaybetmiştir."

11 Eylül Saldırıları öncesindeki dönemde ABD'nin terörizme ilişkin temel deneyiminin, 1998 yılında Kenya ve Tanzanya'daki ABD Büyükelçiliklerinin bombalanmasında veya 2000 yılında ABD savaş gemisi USS Cole'a yönelik yapılan saldırıda olduğu gibi, denizaşırı askeri ve diplomatik tesislerini hedef alan saldırılardan ibaret olduğunu ifade eden Sheppard (2009: 120); ABD topraklarında terörist saldırılar düzenlemek için 11 Eylül 2001 öncesi dönemde de değişik girişimlerde bulunulduğuna dikkati çekmektedir. Bu kapsamda, 1993 yılı Şubat ayında El Kaide Örgütü tarafından Dünya Ticaret Merkezi'ne yönelik yapılan -ilk- bombalama girişimini örnek olarak veren Sheppard'a göre; Timothy McVeigh tarafından, ABD hükümetinin 1993 yılında Waco'daki müdahalesine tepki olarak, 1995 yılında gerçekleştirilen ve 168 kişinin öldüğü Oklahoma Saldırısı ise, 1993 yılındaki El Kaide Saldırısının ardından gerçekleştirilmiş olan en önemli terör eylemidir (2009: 120-121). Bu noktada Shephard, Dünya Ticaret Merkezine yönelik olarak 1993 yılında düzenlenen saldırının aksine, Oklahoma Saldırısını düzenleyen kişinin ülke içinden beyaz bir Amerikalı olmasına da dikkati çekmektedir.

Çoğunluğu sivil olmak üzere 80'den fazla kişinin hayatını kaybettiği ve Oklahoma Saldırısının da gerekçesini oluşturan "Waco Kuşatması"; federal bir kolluk kuvveti olan ATF tarafından, 1993 yılı başında Teksas'ın Waco kentinde bulunan Protestan Davidian tarikatına ait bir çiftliğe düzenlenen operasyon ile başlamış ve FBI'nın sonradan müdahil olması ile birlikte 50 günden fazla sürmüştür (Wikipedia [web], 2011c).

11 Eylül Saldırılarını önceki örneklerinden ayıran belki de en önemli özellik ise, küresel çapta yürütülecek ve "savaş" olarak

nitelendirilecek olan bir terörle mücadele politikasının hayata geçirilmesine yol açması olmuştur.

Janczewski ve Colarik'in de ifade ettiği üzere (2005: 36); 11 Eylül Saldırıları sonrasında "Teröre Karşı Savaş *(War on Terror)*" ilan eden ABD Başkanı G.W. Bush, bu savaşın uzun ve acılı olacağını da vurgulamıştır. Ancak, Newman'ın da belirttiği üzere (2007: 133); ABD'nin teröre karşı savaşı son derece tartışmalı olup, askeri bir yaklaşımı ön plana çıkaran bu girişim birçok gözlemci tarafından adil olmamakla ve ikiyüzlü olmakla itham edilmektedir.

Bu kapsamda 11 Eylül Saldırılarının yarattığı etkilere ve sonuçlara ilişkin bir dizi tespitte bulunan Newman'ın, şu iki tespiti özellikle dikkat çekicidir (2007: 122);

- 11 Eylül Saldırıları sonrasındaki dönemde terörizme verilen devlet desteği ve terör örgütlerine yataklık edilmesi, soğuk savaş dönemindekinden çok daha az hoş görülür bir hale gelmiştir.

- ABD, Avustralya, Rusya ve İsrail'inde aralarında bulunduğu bazı devletler, diğer devletlerin egemenlik alanlarından eylemlerde bulunan teröristleri, ilgili devletin onayı olmaksızın askeri güç kullanmayı da içerecek biçimde, tek taraflı olarak izleme hakları olduğunu ilan etmişlerdir.

Daha önce de ifade edildiği üzere, 11 Eylül Saldırıları ile birlikte terörizme ilişkin olarak ABD kamuoyunda önceden var olan risk algısı birçok açıdan pekişirken; tehdidin sadece denizaşırı ABD hedeflerine yönelik olduğuna ilişkin anlayışın yerini, ABD topraklarının ve varlıklarının tümüyle terörizm tehdidi ile karşı karşıya olduğuna ilişkin anlayış almıştır. Nitekim 11 Eylül Saldırıları sonrasında hayata geçirilen ve pek çok kişiye göre ABD Anayasasındaki temel hak ve özgürlükleri ihlal eden güvenlik politikalarının ve terörle mücadele tedbirlerinin özünde de bu yeni "iç tehdit" algısı yer almaktadır. Bu çerçevede genel bir değerlendirme yapmak gerekirse; Oklahoma Saldırısı ve 11 Eylül Saldırıları, ABD'nin yaşamış olduğu -ülke içi- terörizm tecrübeleri olarak özellikle ön plana çıkmaktadırlar.

c. "Siber" Ön Eki ve Türetilen Kavramlar

Bilgisayarların ve internetin günlük hayatımızdaki rollerinin yadsınamayacak bir şekilde artması ile birlikte, feminizmden diplomasiye kadar, neredeyse her olgunun siber uzayda var olan ya da teknolojiden faydalanma esasına dayanan bir türevinin üretilmesi mümkün hale gelmiştir. İlişkilendirildiği kavram ve olguların günümüzün teknoloji odaklı dünyasındaki değerini arttırma kaygısını da içeren bu "siberleştirme" eğilimden, geleneksel biçimleri de kamuoyu için oldukça dikkat çekici olan "suç", "savaş", "terörizm" ve "güvenlik" gibi kavramlar da etkilenmiş ve hızla siber türevleri üretilmiştir.

Bu çerçevede, yeni doğmuş bir olguyu nitelendirmesi nedeniyle, "siber" kavramının kapsamına ilişkin olarak da açık ve net bir tanımlama bulunmamaktadır. Kimilerine göre sadece kişisel bilgisayarlar veya internet ile kurulan ilişkileri niteleyen bu kavram, kimleri için ise tümüyle fiziksel dünyanın ötesindeki bir sanal gerçekliği temsil etmektedir. Söz konusu farklı yaklaşımların yanı sıra, kişisel bilgisayarların ve internetin yoğun olarak kullanıldıkları iletişim, hizmetler ve finans gibi pek çok alandaki isimlendirmeler de; "e-posta" veya "e-devlet" örneğinde olduğu gibi, "siber" olmalarına değil, "elektronik" tabanlı olmalarına vurgu yapmaktadırlar.

"Siborg *(cyborg)*" ve "sibernetik *(cybernetics)*" gibi kavramların tanımları ile birlikte değerlendirildiğinde ise; "siber *(cyber)*" ön eki, makine ile biyolojik varlık ya da makine ile insan arasındaki sistemsel bir bütünleşmeye vurgu yapan bir karakter kazanmaktadır.

Genel bir değerlendirme yapıldığında ise; siber olgusunun en başarılı eşleşmesinin suç olgusu ile olduğunu ileri sürmek yanlış olmayacaktır. Nitekim bu eşleşmeden doğan "siber suç" olgusu; siber güvenliği bir anlamda, siber suçlar ve geriye kalanlar olmak üzere ikiye bölmektedir. Esas itibariyle, siber suçların siber güvenlik alanındaki bu belirleyici konumunun; gerek kronolojik olarak diğer tehditlerden çok daha önce ortaya çıkmış olmaları, gerekse de kapsamlı hukuksal

düzenlemelerin ve güvenlik yapılarının ortaya çıkmasına yol açmaları ile açıklanması mümkündür.

Bu kapsamda, ister siber savaş veya siber terörizm, isterse de siber sabotaj ya da siber casusluk olarak nitelendirilsin, bir bilgisayara veya sisteme yetkisiz erişim sağlama eylemi, çıkar amaçlı olarak işlenmiş bir -siber- suç ile aynı hukuki usul ve esaslara göre ele alınarak aynı cezai müeyyide ile karşılandığı sürece; ortada, "bilişim sistemine yetkisiz erişim sağlama" suçundan çok daha kompleks bir eylemin somut olarak var olduğunu ileri sürmek de oldukça zorlaşmaktadır. Dolayısı ile, var olan çatışma biçimlerinin veya güvenlik tehditlerinin başına siber ön eki getirmeyi esas alan bir isimlendirme çabası; hukuki ve bilimsel sonuçlar yerine, siber uzayda var olduğu iddia edilen güvenlik tehditlerine ilişkin kamuoyunda kısmi bir farkındalık ve korkudan başka somut bir sonuç üretmeyecektir.

Nitekim siber uzaydan farklı olarak, içerisinde bulunduğumuz fiziksel dünyada; savaş, terörizm, casusluk gibi olguların, hukuken kendilerine özgü olağanüstü usul ve esaslara -bir anlamda kendi hukuklarına- tabi olmaları nedeniyle, kavramsal olarak nasıl tanımlandıkları ve terimsel olarak nasıl nitelendirildikleri oldukça büyük bir önem kazanmaktadır.

Bu aşamada, genel olarak siber uzaya, özel olarak ise siber güvenliğe ilişkin olarak yapılabilecek birçok tanımın ve tespitin içeriğini etkileyebilecek olan şu iki kritik noktanın da açıklığa kavuşturulması gerekmektedir:

- Siber uzay ile fiziksel dünya arasında hiyerarşik bir ilişki bulunup bulunmadığı; eğer böyle bir ilişki var ise, söz konusu ilişkinin niteliği.

- Siber uzayın sadece internet veya kişisel bilgisayarları mı, yoksa her türlü elektronik sistemi mi içerdiği.

Her ne kadar günümüz itibariyle siber ön eki eklenmek suretiyle kastedilenler, genel olarak kişisel bilgisayarlar ve özellikle de internet ile

bağlantılı olgular olsalar da, bu çalışmada benimsenmiş olan yaklaşım; özellikle "siber güvenlik" söz konusu olduğu zaman, çok daha büyük elektronik sistemlerin ve enformasyon sistemlerinin de siber güvenliğin kapsamına kaçınılmaz olarak girdikleri yönündedir. Ancak ister geniş kapsamlı, isterse de dar kapsamlı bir biçimde yorumlansın; siber olgusunun varlığı ve onun güvenliği, enformasyon ve iletişim sistemlerinin varlığına ve güvenliğine sıkı sıkıya bağlıdır.

Gerek siber olgusunun kapsamına, gerekse de ondan türetilen -özellikle güvenlik ile ilişkili- kavramlara yönelik benimsenecek temel yaklaşım; yapılacak tanımlar ve bu tanımların kabul edilmesine bağlı olarak ortaya çıkacak sonuçlar üzerinde belirleyici olan en önemli etkendir. Siber olgusunun başlı başına bağımsız bir gerçeklik olarak kabul edilmesi bizi yepyeni bir dünya ve hatta evren kabulüne götürürken; onu gerçek dünyadaki teknolojik gelişmelerin basit bir sonucu olarak görmek ise, bizi sadece sanal araç ve uygulamaların tanımlanması sorunu ile karşı karşıya bırakacaktır.

Bu çerçevede, ister günlük hayatın akışı içerisinde özensizce, isterse de uzmanlar tarafından büyük bir dikkatle kullanılmış olsunlar; "siber" ön ekini taşıyan kavramlara veya olgulara bu niteliği gerçek anlamda kazandıran şey, çeşitli teknolojiler ve ağlar üzerinden "siber uzay" ile kurmuş oldukları ilişkidir. Dolayısı ile siber uzay, bu çerçevede öncelikli olarak açıklanması ve netleştirilmesi gereken bir kavram olarak karşımıza çıkmaktadır.

(1) Siber Uzay *(Cyberspace)*

Sosyal bir gerçeklik olarak "siber uzay"; insanların fiziksel olarak yer almamalarına rağmen içerisinde "yaşayabildikleri", ancak "gerçek" –fiziksel- dünyada her hangi bir varlığa sahip olmayan sanal ve dolayısı ile de yapay bir mekandır. Dolayısı ile özellikle gerçekliği noktasında siber uzay olgusu, tartışmaya açık bir konumda bulunmaktadır.

Bu çerçevede, siber uzayın yarattığı sosyal etkileri "Ağ Toplumu *(Network Society)*" kavramı üzerinden ele alan Manuel Castell'e göre (2010: 387) ise; sanal dünyada oluşturulan toplulukların gerçek birer topluluk *(community)* olup olmadıklarına ilişkin sorulacak bir soruya, hem olumlu, hem de olumsuz yanıt vermek mümkündür. Fiziksel olmayan birer topluluk olarak, fiziksel topluluklar ile aynı iletişim ve etkileşim kalıplarını izlemeyen sanal topluluklar; "gerçekdışı" da olmayıp, farklı bir gerçeklik seviyesinde işlemektedirler. Bu topluluklar, zayıf bağlara dayanan ancak oldukça da çeşitlenmiş ve özelleşmiş olan, kişiler arası sosyal ağlardır.

Askeri bakış açısından ise, saldırmak ya da savunmak için siber uzayın yeterli fiziksel gerçekliğe sahip olduğunun değerlendirildiğini ifade eden Fahrenkrug'a göre ([web], 2007); ABD Savunma Bakanlığı, bir savaş alanı olarak kabul ettiği siber uzaya ilişkin anlayışına, "Siber Uzay Operasyonları için Ulusal Askeri Strateji"nin yayınlanması ile resmiyet kazandırmıştır. Fahrenkrug'un aktardığı üzere, söz konusu belge ile "siber uzay"; ağ sistemleri ve ilişkili fiziksel altyapılar vasıtası ile verilerin saklanması, değiştirilmesi ve el değiştirmesinde elektronik cihazların ve elektromanyetik spektrumun kullanılması ile karakterize edilen bir alan olarak tanımlanmaktadır. Siber uzayın askeri tanımına ilişkin olarak, Fahrenkrug'un da dikkat çektiği üzere ([web], 2007):

> "Bu tanıma göre siber uzay, elektromanyetik enerji kullanan elektronik cihazları ve ağ sistemlerini kapsayan oldukça gerçek, bir fiziksel alandır. Siber uzay; hava, kara, deniz ve uzay alanları boyunca var olur ve bu fiziksel alanları saklanmış, değiştirilmiş veya el değiştirmiş verileri kullanan bilişsel süreçler ile birbirlerine bağlar."

Siber uzayın sıralanabilecek pek çok özelliği içerisinde, siber güvenlik yönetimi açısından belki de en önemli olanı, mesafe kavramını ortadan kaldırmasıdır. Bu durumu Kovachic ve Halibozek şöyle ifade etmektedirler (2003: 19);

> "Fiziksel sınırların olduğu kadar coğrafi mesafeler de, siber uzayda neredeyse anlamsızdırlar; uzak mesafede bulunan bir hedef, yerel bir hedef kadar kolay saldırılabilirdir. Bu güvenlik profesyonelleri için anlamaları gereken önemli bir konsepttir."

Siber uzayın, siber terörizmi teşvik edici olarak değerlendirilebilmesi de mümkün olan, bir diğer özelliği ise; kendisi üzerinden etkileşime giren kişiler arasındaki ilişki biçimlerini alışılmadık bir biçimde değiştirmesidir. Siber uzayda sergilenen davranışlar veya yapılan eylemler, kurbanlar üzerinde çeşitli olumsuz sonuçlara sahip olabilseler de; özellikle eylemciler üzerinde gerçek fiziksel riskler veya etkiler yaratmamaktadırlar. Söz konusu durumu Mirabello şöyle ifade etmektedir (2009: 270):

> "Bugün, teröristler interneti bir silah olarak kullanabilirler. Gezegen üzerindeki herhangi bir yerden -neredeyse hiçbir maliyeti olmaksızın- bir siber terörist, elektronik olarak bir bilgisayar sistemine girebilir ve hasara neden olabilir. Tüm bu saldırı süresince, bahse konu siber teröristin kimliği belirsiz olarak kalabilir ve yakalanmaktan, yaralanmaktan veya ölümden korunabilir."

Bu noktada, hem siber uzayı genişleten, hem de siber uzaydaki en büyük güvenlik sorunlarını yaratan "Ağ *(Network)*" olgusunun kapsamına da kısaca değinmek faydalı olacaktır. "Ağ" terimi, genel olarak siber tehditler, özel olarak ise siber savaş bağlamında kullanıldığında; küresel ya da kurumsal olarak oluşturulabilecek, birden fazla bilgisayarın birbirlerine bağlı olduğu her türlü duruma ve bu durumun oluşmasını sağlayan altyapıya karşılık gelmektedir. Özellikle siber suçlar bağlamında kullanıldığında ise "Ağ" terimi; çoğunlukla gündelik hayattaki kullanımına yaklaşmak suretiyle, geçmişi 1969 yılında hayata geçirilimiş bir bilgisayar ağı olan ARPANET[7]'e dayanan, İnternete karşılık gelmektedir.

Bu çerçevede, hem bilimsel, hem de felsefi boyuta sahip olan yaklaşımı ile Floridi; *"(LAN, CWIS, MAN, WAN gibi bölgesel ya da ulusal) yüzlerce ağın topaklaşmasından doğan uluslararası bir dijital iletişim ağı"* olarak tanımladığı "İnternet"i, teknik açıdan ise, şu üç farklı alanın bir araya gelerek oluşturduğu bir bütün olarak ele almaktadır (1999: 61):

---

[7] ARPANET *(Advanced Research Projects Agency Network)*; ABD Savunma Bakanlığının desteği ile ARPA *(Advenced Research Projects Agency)* tarafından geliştirilmiş olup, internet de dahil olmak üzere, bilgisayar ağlarının ilk çıkış noktası olarak kabul edilmektedir (Bidgoli, 2004:49). Morley ve Parker'a göre (2010: 322), ARPANET'in ortaya çıkış amaçları; farklı yerlerde bulunan araştırmacıların birbirleri ile iletişimlerine imkan tanıyacak bir bilgisayar ağı yaratmak ve bir nükleer saldırı veya doğal afet durumunda bir kısmı yok olsa dahi, ağ iletişiminin devam edebilmesini sağlayacak çeşitli yollar üzerinden veri gönderme ve alma kabiliyetine sahip bir bilgisayar ağı kurmaktır.

"* Altyapı (Fiziksel Boyut)

* Hafıza Düzlemi (Dijital Boyut)

* Semantik Uzay (Siber Uzay Boyutu)."

Siber uzayın insanoğlunun daha önceden benzeri ile karşılaşmadığı bir olgu olduğu açıktır ve belki de gelecekte, genel olarak siber uzayın ve özel olarak ise internetin ortaya çıkışı, ateşin bulunması veya tekerleğin icadı gibi insanoğlunun büyük başarıları arasında sayılacaktır. Siber uzayın insan olmanın kültürel ve sosyal boyutları üzerinde ne gibi etkilerinin olduğu, bu etkilerin nasıl ortaya çıktıkları, hangi süreçler üzerinden işledikleri ve bu etkilerin ne kadar kritik olduklarına ilişkin tartışmalar ise, elbette ki antropolojinin ve sosyolojinin ilgi alanlarına girmektedirler.

Bununla birlikte siber uzayın insanlar üzerindeki etkilerine -bu çalışmanın konu ve kapsamı ile de ilişkilendirilebilecek bir biçimde- dikkati çeken Dreyfus'a göre (2009: 6-7); kişiler, siber uzaya girdiklerinde ve duygusal, sezgisel, konumlanmış, yaralanabilir, cismani benliklerini arkalarında bıraktıklarında, daha önceden insanoğlu için asla mevcut olmayan kayda değer yeni bir özgürlük kazanmaktadırlar. Ancak bu kazanımla da eş zamanlı olarak, bazı çok önemli kapasitelerini zorunlu olarak kaybetmektedirler. Bu kapasitelerin kaybedilmesinden ise; fiziksel dünyada var olan eşyalara ilişkin his ve duygular, başarı ve başarısızlığın ciddiyetine ilişkin duygular ve insan hayatına anlam kazandıran gerçek bağlılık duygusu etkilenmektedir.

(2) Siber Güvenlik *(Cybersecurtiy)*

"Güvenlik" terimi günlük hayattaki kullanımında, emniyet içerisinde bulunma veya korku içerisinde olmama gibi durumları ifade etmektedir.

"Güvenlik nedir?" sorusuna, terimin günlük kullanımının dışında, özellikle ulusal güvenlik ve tehdit merkezli olarak verilebilecek geleneksel cevabı ise; güvenlik ve güvenlikleştirme *(Securitisation)* üzerine önemli çalışmalar yapmış olan Barry Buzan, yakın çalışma arkadaşı Ole Waever'in görüşlerine atfen, şöyle ifade etmektedir (Buzan ve diğerleri, 1998: 21);

> "Geleneksel olarak, "Güvenlik" kelimesinin kullanılması; acil durum şartlarının ifade edildiği, böylelikle de bir tehdidin gelişimini engellemek üzere gerekli olan her türlü tedbirin kullanılmasına dair bir hak iddiasında bulunulduğu bir durumdur."

Bu kapsamda, -alışıldık biçimi ile- bir fiziksel varlığa sahip olmayan siber uzayın güvenliğinin nasıl sağlanabileceğine ilişkin soruya verilecek yanıt; siber güvenliğin tam ve doğru tanımına ulaşmak için atılmış en önemli adım olacaktır. Bu çerçevede, çalışma kapsamında yürütülen literatür taraması faaliyeti sırasında özellikle dikkati çeken, siber güvenliğe ilişkin kaygı, algı, tedbir ve tespitlerin yoğunlaştığı noktaları şöyle sıralayabilmek mümkündür:

- Kişilerin art niyetli, bilinçli veya bilinçsiz olarak fiziksel dünyaya veya siber uzaya yönelik tehlike yaratan davranışlarının engellenmesi,

- Siber uzayda sınırlı veya genel olarak kullanıma sunulmuş olan verilerin korunması ve yönetilmesi,

- Genel olarak yazılımlardaki, kısmi olarak ise donanımlardaki tasarım ve üretim hatalarının giderilmesi,

- Siber uzaya, gerek -sanal- bir gerçeklik olarak hayat veren, gerekse de onun fiziksel gerçekliğini oluşturan iletişim ve enformasyon altyapısının, enerji altyapısı ile birlikte güvenli bir şekilde ayakta tutulması.

Bu aşamada gerek yapılan tespitlerin anlaşılabilirliğinin arttırılması, gerekse de siber tehditlerin doğalarının ortaya konulabilmesi maksadıyla, özellikle emniyet ve kaza önleme kapsamında yaygın bir bilinirliğe sahip olan "Ateş Üçgeni *(Fire Triangle)*" olgusu ile siber tehditler

arasında bir benzerlik kurulması uygun olacaktır. Bu çerçevede, bir yangının çıkması için mutlaka bir araya gelmesi gereken ısı, yanıcı madde ve oksijen unsurlarından oluşan "ateş üçgeni" örneğinde olduğu gibi, bir siber güvenlik tehdidinin ortaya çıkabilmesi için de; veri haline getirilerek siber uzayda yerini almış olan bir enformasyonun, bu veri ile ilişkili bir enformasyon sisteminin ve bahse konu veriye ya da sisteme doğrudan veya bir yazılım vasıtası ile dolaylı olarak yönelmiş olan beşeri bir iradenin biraraya gelmiş olması gerekmektedir. Dolayısı ile "Veri", "Makine" ve "İrade" üçlüsünden herhangi birinin denklemden çıkartıldığı noktada, tehdit de ortadan kalkmaktadır. Ancak, ağların günlük hayatın merkezinde vazgeçilmez bir şekilde yer aldıkları ve siber uzayda fiziki dünyaya göre çok daha hızlı ve sınırsız hareket edilebildiği gerçekleri gözönünde bulundurulduğunda; bu üç unsurun salt güvenlik kaygıları ile birbirlerinden ayrılmaları muhtemel görünmemektedir.

1984-1990 yılları arasında Avustralya Savunma Bakanlığı da yapmış olan, Batı Avustralya Üniversitesinden Sosyal ve Politik Teori Profesörü Kim C. Beazley; teknolojik gelişme ile -özellikle ulusal- güvenlik arasında var olan ve kaçınılmaz bir gerçeklik olarak siber güvenliği yaratan ilişkiyi şöyle ortaya koymaktadır (Waters ve diğerleri, 2008: xx):

> "Uzun vadeli bekamız, bize karşı kullanılabilecek kabiliyetlerin net bir şekilde anlaşılmasına ve bunları karşılamada teknolojik avantajı korumanın küçük bir ulus için açık bir ihtiyaç olmasına dayanmaktadır."

Chatham House için Paul Cornish ve arkadaşları tarafından hazırlanan ve 2010 yılı Kasım ayında yayımlanan "Siber Savaş Üzerine" isimli rapora göre ise; siber uzaydaki tehditler aşağıda yer alan dört ana başlık altında gruplandırılabilmektedirler (Cornish ve diğeleri, 2010: 5):

- Devlet Destekli Siber Saldırılar
- İdeolojik ve Siyasal Aşırılıkçılık
- Ciddi Örgütlü Suçlar
- Düşük Seviye/Bireysel Suçlar

Bu kapsamda McCrie ise, siber tehditlerin sürekli olarak genişleme eğiliminde olan doğasına dikkati çekmektedir (McCrie, 2001: 326):

> "Veri sistemlerinin korunması oldukça önemli ve karmaşık bir konudur. Siber tehditlerin doğası, ağlar günlük operasyonlarda daha büyük bir rol oynadığı sürece genişlemeye devam etmekte, internet ve e-ticaretten yeni güvenlik açıkları ortaya çıkmaktadır."

Siber güvenlik olgusunun kapsamına ilişkin olarak ise; ulusal güvenliğin bir boyutu olarak siber güvenliğe odaklanmış, politik ve sosyal kimlikleri ön plana çıkan güvenlik ve strateji uzmanları ile, siber saldırılara karşı güvenliği sağlamayı amaçlayan, teknik kimlikleri ön plana çıkan siber güvenlik uzmanları arasında bir ayrışmanın olduğunu ileri sürmek mümkündür. Bu ayrışma, aynı gerçekliğe yönelik farklı bakış açılarından ziyade; enformasyon teknolojilerine ilişkin ihtiyaç duyulan teknik bilginin karmaşıklığı ve ciddi bir uzmanlığı gerektirmesi gerçeğinden doğmaktadır. Dolayısı ile siber uzayın ve onun güvenliğinin teknik boyutu, sosyal, politik ve hukuki boyutlarından ayrışmaktadır.

Söz konusu ayrımın yanı sıra, siber terörizm başlığı altında bu çalışmanın ilerleyen kısımlarında da değinileceği üzere; gerek sanal olarak, gerekse de fiziksel olarak siber uzaya varlık kazandıran iletişim ve enformasyon altyapısı tesislerinin fiziki güvenliklerinin sağlanması ihtiyacı üzerinden, siber güvenlik bir fiziksel güvenlik boyutu da kazanmaktadır. Zira kritik altyapı tesisleri, gerek siber dünya için gerekli olan enerji ve kapasiteyi sağlamaları, gerekse de kullandıkları bilgisayar sistemleri üzerinden siber dünyanın bir parçası olmaları nedeniyle, kaçınılmaz bir şekilde siber güvenliğin tam da merkezinde yer almaktadırlar. Bu durum ise, kritik altyapı tesislerinin günümüzün en önemli siber güvenlik nesneleri olmasının asli nedenini oluşturmaktadır.

11 Eylül Saldırılarının hemen ardından yayımlanan ve geleneksel siber tehdit senaryoları ile bunların dayandığı risk analizi süreçlerini eleştirel bir biçimde ele aldığı çalışmasında, James A. Lewis'e tarafından da ifade edildiği üzere (2002: 1-2); -verimli siber güvenlik çalışmaları yürütülebilmesi için- siber tehditlere ilişkin olarak yapılacak bir yeniden değerlendirme süreci, aşağıdaki esasları bünyesinde barındırmalıdır:

- Siber savaş ve siber terörizm olguları, altyapı tesislerine yönelik -konvansiyonel- saldırıların tarihsel bağlamı içerisinde ele alınmalıdır.

- Siber saldırılar, -kriz yönetimi kapsamında yer alan- rutin altyapı/tesisat arızaları ile karşılaştırmalı olarak ele alınmalıdır.

- Altyapı tesislerinin bilgisayar ağlarına olan bağımlılığı ölçülmelidir.

- Siber terörizm söz konusu olduğunda, siber silahların teröristlerin politik hedefleri ve amaçları bağlamında kullanımları mutlaka dikkate alınmalıdır.

Bu kapsamda özellikle, Lewis'in de çalışmasında sıklıkla dikkat çekmekte olduğu, kritik altyapı tesislerinde yaşanılan "rutin arızalar" olgusu, siber tehditlerin kritik altyapı tesislerine yönelik olarak yarattığı iddia edilen tehlikelerin gerçekliğinin ve ciddiyetinin sorgulanması noktasında oldukça kritik bir rol oynamaktadır.

(3) Siber Savaş *(Cyberwarfare)*

Günümüz itibariyle, "siber savaş"ın konvansiyonel savaş ile aynı türde veya eşit değerde bir olgu olduğunu ileri sürmek oldukça zordur. Nitekim böyle bir iddianın geçerli olabilmesi öncelikli olarak; bu tip bir savaşta kullanılacak siber silahların, bunları kullanacak siber askerlerin, bu savaşın kapsamı içerisinde yürütüleceği siber savaş hukukunun ve bahse konu askerlerin görevlerini yerine getirirken işleyecekleri siber savaş suçlarının belirlenmesini ve tanımlanmasını gerektirmektedir.

Nitekim bu kapsamda Clarke ve Knake de, sormakta oldukları *"Hangi uluslararası yasalar siber savaşı kapsıyor?"* sorusu üzerinden siber savaşın hukuki boyutuna dikkati çekmektedirler (2010: 110).

Günümüz dünyasında siber savaşın; diğerlerinden ayrışmış ve kendi başına bağımsız bir biçim almış olan konvansiyonel savaş, nükleer savaş veya gerilla savaşı örneklerinin aksine, bir ülkenin silahlı kuvvetlerinin personel, kaynak, imkan ve kabiliyetlerinin başka bir ülkeninkilere karşı kullanıldığı, siber uzayda cereyan eden -resmi- bir çatışma biçimi olma özelliği gösterdiğini ileri sürmek mümkündür. Başka bir ifadeyle, söz konusu -siber- çatışmanın "savaş" olarak isimlendirilmesine yol açan; sahip olduğu askeri, stratejik ya da felsefi özelliklerden ziyade, tıpkı İkinci Dünya Savaşı içerisindeki "çöl savaşı" veya "denizaltı savaşı" örneklerinde olduğu gibi, çatışmaya yön veren unsurlardır. Nitekim siber savaş kapsamında da söz konusu yönlendirici unsurlar; sırası ile, siber uzay ve bilişim sistemleridir.

Clarke ve Knake, siber savaşı; *"bir devletin başka bir devletin bilgisayar sistemlerine ve ağlarına sızarak hasar veya kesinti yaratmak üzere hareket etmesi"* olarak tanımlamaktadırlar (2010: 8).

Cornish ve çalışma arkadaşlarına göre ise (Cornish ve diğerleri, 2010: 3):

> "Siber Savaş, politik, ekonomik veya toprak kazanma amaçları ile askeri ve endüstriyel hedeflere yönelik olarak kesin ve orantılı bir kuvvetin kullanıldığı devletlerarası bir çatışmadır."

ABD Savunma Bakanlığı tarafından yayınlanmış olan "Siber Uzay Operasyonları için Ulusal Askeri Strateji'" belgesini değerlendiren Fahrenkrug'a göre ([web], 2007); fiziksel bir varlığa da sahip olan siber uzayda yürütülen ve elektronik savaş kabiliyetlerini gerektiren siber savaş konseptinin özünde, "karşı siber operasyonlar *(countercyber operations)*", "birden fazla savaş alanına yayılan operasyonlar *(cross domain operations)*" ve sivil otoriteler ile savunma sanayinin desteklenmesi yer almaktadır.

ABD'li gazeteci Tim Weiner ise, CIA tarihine ilişkin çalışmasında siber savaşı, diğer örtülü ve özel operasyon biçimleri ile birlikte bir "silah" ve dolayısı ile de bir "araç" olarak ele almaktadır. Weiner, soğuk savaş

döneminde KGB'ye yönelik yapılmış olan bir operasyona ilişkin olarak aşağıdaki tespitlerde bulunmaktadır (2007: 387):

> "Operasyonda CIA'nın komutası altındaki neredeyse her silah -psikolojik savaş, sabotaj, ekonomik savaş, stratejik aldatma, karşı istihbarat, siber savaş- tümüyle Ulusal Güvenlik Konseyi, Pentagon ve FBI ile işbirliği içerisinde kullanıldı. Bu operasyonla, güçlü bir Sovyet casusluk ekibi yok edildi, Sovyet ekonomisine zarar verildi ve Sovyet devletinin dengeleri bozuldu. Bu etkileyici bir başarıydı. Diğer tarafın bakış açısından ise, bu bir terör eylemi olarak görülebilirdi."

"Örtülü operasyonlar *(covert operations)*"a ilişkin yaptığı tanımlamada, Weiner ile benzeri bir yaklaşımı paylaşan Prados'a göre de (2002: 387); politik eylem, paramiliter faaliyet, psikolojik savaş ve ekonomik savaş gibi çok sayıda farklı faaliyeti içerebilen örtülü operasyon konseptinin kapsamına, "siber eylem *(cyberaction)*" veya "bilgisayar savaşı *(computer warfare)*" gibi oldukça geniş kategorilerin de eklenebilmesi mümkündür.

Siber savaşın başlı başına bir silah ve dolayısı ile de bir araç olarak görüldüğü noktada, siber silah olgusunun var olup olmadığı ve eğer varsa da, nasıl tanımlanması gerektiği sorunu ile karşı karşıya kalınmaktadır. Ancak burada hemen ifade etmek gerekir ki; yukarıda kullanıldığı biçimiyle "araç" terimi, Clausewitz'in ifade ettiği gibi savaşın politikanın stratejik bir aracı olduğu süreç ya da eylemlerdeki anlamından ziyade, savaşma eylemi içerisinde düşmana zarar vermek için kullanılan taktik veya operasyonel bir "alet" olma durumunu karşılamaktadır.

Silahların düşmana saldırmak veya savunma yapmak için kullanılabilecekleri düşünüldüğünde; siber uzayda söz konusu işlevlere sahip olan araçların da, birer -siber- silah olarak nitelendirilebilmeleri mümkün gözükmektedir. Nitekim bazı kaynaklarda, "bilgisayar virüsleri *(computer viruses)*" açık bir şekilde "siber silah *(cyberweapons)*" olarak nitelendirilmektedirler. Bu çerçevede siber silahları, ateşli veya nükleer silahlardan ayıran belki de en önemli niteliklerinin; insanlara yönelik doğrudan şiddet uygulama ve fiziksel zarar verme kapasitesine sahip olmamaları olduğunu kabul etmek de yanlış olmayacaktır.

Siber silahların "Öldürücü Olmayan Silahlar (ÖOS)" kategorisindeki kullanımı kapsamında siber uzaydaki ilk saldırının, Kosova Olayları sırasında Sırbistan'a karşı ABD güçleri tarafından gerçekleştirildiği ifade edilmektedir (Özkaya, 2002: 286 ve 337'den aktaran Aktürk, 2006: 20). Bu çerçevede söz konusu saldırı; internet üzerinden, Sırp bilgi işlem sistemlerine yönelik olarak NSA tarafından düzenlenmiştir.

Nitekim Lerner'in de dikkat çektiği üzere (2004a: 264); NSA'ya göre, terörist grupların yanı sıra 100'den fazla hükümet de siber silah geliştirme çabası içerisinde bulunmaktadır.

Ancak nükleer savaş örneğinde olduğu gibi, bugüne kadar herhangi bir -resmi- siber savaş tecrübesinin yaşanmamış olması, bu konu ile alakalı pek çok tanım ve değerlendirmenin afaki ve spekülatif kalmasına yol açmaktadır. 2007 yılında Estonya'ya ve 2008 yılında Gürcistan'a yönelik yürütülen ve Rusya Federasyonu kaynaklı olduğu tespit edilen siber saldırılar, her ne kadar sıklıkla birer siber savaş örneği olarak sunulsalar da; kaynak ülke olan Rusya Federasyonu tarafından aynı biçimde nitelendirilmemekte ve resmen kabul edilmemektedirler.

Böyle bir belirsizlik ortamında, New York Times Gazetesinde 31 Mayıs 2011 tarihinde yer alan bir habere göre ise ([web], 2011); ABD'ye yönelik siber saldırıları caydırmak maksadıyla ABD Savunma Bakanlığı tarafından, yabancı ülkelerden gelecek bilgisayar saldırılarının -askeri karşılık verilmesini de içerecek bir biçimde- savaş nedeni olarak kabul edilmesini öngören yeni ve resmi bir stratejinin geliştirilmesine yönelik çalışmalar yürütülmektedir.

Siber uzaydaki kapasiteler üzerinden sürdürülen sanal çatışmanın, bağımsız bir savaş biçimi mi, yoksa gerçek dünyadaki politik ve askeri çatışmaların teknoloji yoğun bir aracı mı olduğuna dair verilecek karar; siber savaş kavramının kapsam ve niteliğinin yanı sıra onunla bağlantılı pek çok kavramın tanım ve kapsamını da derinden etkileyecektir. Bununla birlikte, her ne şekilde nitelendirilirse nitelendirilsin, ortada bir "siber" çatışma ya da mücadelenin bulunduğu da aşikardır. Bu kapsamda, söz konusu mücedelenin resmi boyutunun şimdiye kadar örtülü operasyonlar

konsepti içerisinde yürütüldüğünü ve bundan sonra da benzeri bir çerçevede yürütülmeye devam edileceğini ileri sürmek yanlış olmayacaktır.

(4) Siber Terörizm *(Cyberterrorism)*

Dolnik'in ifade ettiği üzere (Mickolus, 2002: 96'dan aktaran Dolnik, 2007: 35); veri yokedici bir virüsün 1988 yılında Kudüs Yahudi Üniversitesindeki yayılımı siber terörizmin ilk örneklerinden bir tanesini oluşturmaktadır. Tamil Kaplanları Örgütünün bir kolu olan İnternet Kara Kaplanları tarafından 1997 yılında Sri Lanka'nın dış temsilciliklerine ait e-posta hesaplarına yönelik yapılan saldırılar ve Belgrad merkezli hackerlar tarafından 1999 yılında NATO'nun resmi internet sitesine yönelik girişilen saldırı da, yine Dolnik'e göre kayda değer siber terörizm vakaları arasında yer almaktadır (2007: 35).

H.W. Kushner, terörizm üzerine yaptığı ansiklopedik çalışmasında siber terörizmi; *"terörizm ve siber uzayın yakınsaması, enformasyon sistemlerinin siyasal güdümlü sabotajı"* olarak tanımlamaktadır. 1990'lı yıllardan bu yana "Hackleme *(Hacking)*" olaylarının, siber suçların ve son derece yıkıcı bilgisayar virüslerinin yaygınlaştığına dikkati çeken Kushner; bu gelişmelere rağmen siber terörizmin çoğu kişi tarafından bir gerçeklikten ziyade muhtemel bir yakın tehlike olarak kabul edildiğini ifade etmektedir (2003: 103).

Dolnik'e göre ise siberterörizm; tıpkı mekanik sabotaj veya kaynakların ve ürünlerin kirletilmesi eylemlerinde olduğu gibi sabotaj başlığı altında değerlendirilebilecek bir eylem biçimidir. Birçok terörist grubun üyelerinin iletişim ve operasyonel planlama maksadıyla bilgi teknolojilerini kullandıklarının bilindiğini ifade eden Dolnik (2007: 35); muhtemelen dolaylı birer saldırı yöntemi olmalarına bağlı olarak tatmin düzeylerinin düşük olması nedeniyle, geleneksel terör örgütleri tarafından

girişilen siber sabotaj eylemlerinin ender sayıda olmasına dikkat çekmektedir.

Genel bir değerlendirme yapıldığında, sabotaj kavramını ön plana çıkaran yukarıdaki yaklaşım, özellikle kritik altyapının korunması noktasında güncel siber güvenlik tartışmaları ile de uyum içerisinde görünmektedir.

Siber terör olgusunu enformasyon teknolojileri ve muhtemel terörist faaliyetler arasındaki etkileşim üzerinden somutlaştıran Janczewski ve Colarik ise; söz konusu muhtemel terörist faaliyetleri şöyle sıralamakta ve açıklamaktadırlar (2005: 41-42):

- Enformasyon teknolojileri tesislerine yapılacak doğrudan -siber- saldırılar. Bu gibi saldırıların muhtemel sonuçları, sağlanılan hizmetlerin geçici olarak kesintiye uğraması olacaktır. Bununla birlikte özellikle hava trafik kontrol sistemleri veya hastaneler gibi doğrudan insan hayatı ile ilişki içerisinde olan sistemlerde, ölümcül sonuçların ortaya çıkabilmesi de mümkündür.

- Diğer hedeflere karşı girişilen terörist saldırılardan kaynaklanan enformasyon teknolojilerine yönelik ikincil zararlar. Bu çerçevede, geleneksel saldırı biçimlerinden bir tanesi olan bombalama eylemleri sonucunda, enformasyon teknolojileri altyapısı ve tesislerinde ikincil zararların ortaya çıkabilmesi mümkündür.

- Terör örgütlerinin amaçları için enformasyon teknolojileri tesislerinin kullanılması. Bu kapsamda, terör eylemlerinin planlanması ve icrasında intrenetin veya benzeri enformasyon altyapılarının kullanılması mümkündür.

Siber terörizme ilişkin olarak literatürde yer alan tehdit algı ve değerlendirmeleri genel olarak ele alındıklarında ise; söz konusu algı ve değerlendirmelerin, eylemlerin hedeflerine ve biçimlerine göre aşağıdaki iki ana başlık altında gruplandırılabilmeleri mümkün gözükmektedir:

- İletişim altyapısı ve enerji tesisleri başta olmak üzere "Kritik Altyapı Tesisleri"ni hedef alan "Siber Sabotajlar",

- Gerçek dünyadaki terörist saldırıların etkilerini arttırmak üzere, bir "Kuvvet Çarpanı" olarak girişilebilecek olan "Siber Saldırılar".

Bu kapsamda, NSC'nin kritik altyapının korunmasından sorumlu eski bir üst düzey yöneticisi olan Jeffrey A. Hunker'e göre (Kushner, 2003: 104); siber saldırılara, gerek panik yaratmak üzere internet üzerinden yanlış bilgilerin gönderilmesi, gerekse de finansal ağların, acil müdahale veya iletişim ağlarının sabote edilmesi suretiyle gerçek dünyadaki bir bombalama veya saldırı için "kuvvet çarpanı" oluşturmak maksadıyla başvurulabilmesi mümkündür.

Dönemin CIA Başkanı John Deutch'un 1996 yılında yapmış olduğu, "elektronik bir Pearl Harbor Saldırısının yaklaştığına" dair iddialı açıklamasının halen fazlaca desteklenmemiş olduğuna dikkati çeken Kushner; siber terörizmin sahip olduğu "terör" yaratma potansiyeline ilişkin görüşleri, iki ana grup altında toplamaktadır. Çoğunluğun, "Hackleme" eyleminin geleneksel terörist saldırılar ile birlikte bir "Kitlesel Karışıklık Silahı *(Weapon of Mass Disruption)*" olarak kullanılabileceğine inandığını ifade eden Kushner; azınlıkta kalan grubu ise "Şüpheciler" olarak isimlendirmektedir. Kushner'e göre "Şüpheciler"; içeriğindeki dram eksikliğine bağlı olarak, intihar saldırıları gibi oldukça etkili geleneksel terör araçlarına sahip geleneksel teröristler için siber terörizmin fazlaca bir vaatte bulunmadığı kanısındadırlar (Kushner, 2003: 104).

Yapılan siber terörizm tanımlamalarını var olan olguyu analiz etmek için aşırı genel bulan ve terörizm olgusunun doğasında yatan şiddet kullanımına dikkati çeken Anderson ve Sloan'a göre ise (2009: lxii-lxiii); her hangi bir bankacılık sistemine veya veri tabanına yönelik olarak girişilen yıkıcı bir siber saldırı, doğurduğu sonuçlar kişilere yönelik fiziksel bir şiddeti içermedikçe veya buna yol açmadıkça terörizm kapsamında değerlendirilmemelidir. Bir siber saldırıdan doğan karışıklık durumunun, o saldırının bir terör eylemi olarak nitelendirilebilmesi için kendi başına yeterli olmadığına dikkati çeken Anderson ve Sloan; ancak söz konusu eylemin sonucunda -örneğin kişilerin ölüm ya da yaralanmalarına neden olunması gibi- ortaya çıkan ikincil etkilerin "şiddet" gerekliliğini karşılaması durumunda yapılacak olan "terörizm" nitelendirmesinin haklılık kazanacağı

görüşündedir. Bu çerçevede siber terörizmi enformasyon savaşı başlığı altında ele almayı tercih eden Anderson ve Sloan; "siber karışıklık *(cyberdisruption)*" ile "siber terörizm *(cyberterrorism)*" arasında var olduğunu ileri sürdükleri bu ayrımın kabul edilmesinde yaşanılacak başarısızlığın, mevcut tehdidin kapsamının belirlenmesinde de ciddi bir sorun yaratacağını ileri sürmektedirler (2009: lxiii).

Siber terörizmin tehdit ve etki kapasitesinin çok daha somut bir biçimde ortaya konulabileceği siber sabotajlar hususunda ise; özellikle kritik altyapının korunması kaygısı ve SCADA Sistemleri, güncel siber güvenlik tartışmalarının merkezinde yer almaktadırlar.

Kritik altyapının korunmasının 11 Eylül 2001 tarihinden sonra özellikle ABD'de büyük önem kazandığına dikkati çeken Lerner'e göre (2004a: 282);

> "Kritik Altyapı (Critical Infrastructure)", hükümet ve ekonominin işlevlerini yerine getirebilmeleri için gerekli olan fiziksel ve bilgisayar tabanlı sistemler için kullanılan genel bir terimdir. Telekomünikasyon, enerji, bankacılık ve finans, ulaştırma, su sistemleri ve acil durum hizmetleri söz konusu sistemler arasında yer almaktadırlar."

ABD'de kritik altyapının korunmasına ilişkin hükümet girişimlerinin 1982 yılına kadar geri götürülebileceğini ifade eden Gopalakrishnan ve Peeta ise (2010: 81-82); o günden bu yana hükümetin geleneksel güvenlik politikasının "koruma" odaklı olduğuna, 11 Eylül Saldırıları sonrasında ise "tesislerin fiziksel güvenliği"nin daha da önplana çıktığına dikkat çekmektedir. Yine aynı yazarlara göre; kritik altyapı tesislerinin 18 ayrı kategori altında sınıflandırıldığı günümüzdeki mevcut yaklaşım, esneklikten uzak olduğu kadar yönetim açısından da oldukça zor ve pahalıdır.

Bu kapsamda, ABD tarafından 2009 yılında yayımlanmış olan "Ulusal Altyapı Koruma Planı (NIPP)"nda yer alan kritik altyapı sektörlerini ve bunların korunmasından sorumlu olan kurumları şöyle sıralamak mümkündür (DHS, 2009: 3):

- Tarım ve Gıda (Tarım Bakanlığı, Sağlık ve İnsani Hizmetler Bakanlığı)
- Savunma Sanayi (Savunma Bakanlığı)
- Enerji (Enerji Bakanlığı)
- Kamu Sağlığı ve Sağlık (Sağlık ve İnsani Hizmetler Bakanlığı)
- Ulusal Anıtlar ve Simgeler (İçişleri Bakanlığı)
- Bankacılık ve Finans (Hazine Bakanlığı)
- İçme Suyu ve Su Arıtma (Çevre Koruma Kurumu)
- Kimyasal Tesisler (İç Güvenlik Bakanlığı)
- Ticari Tesisler (İç Güvenlik Bakanlığı)
- Kritik İmalat (İç Güvenlik Bakanlığı)
- Barajlar (İç Güvenlik Bakanlığı)
- Acil Durum Hizmetleri (İç Güvenlik Bakanlığı)
- Nükleer Reaktörler, Malzemeler ve Atık (İç Güvenlik Bakanlığı)
- Enformasyon Teknolojisi (İç Güvenlik Bakanlığı)
- İletişim (İçişleri Bakanlığı)
- Posta ve Kargo (İç Güvenlik Bakanlığı)
- Ulaştırma Sistemleri (İç Güvenlik Bakanlığı)
- Hükümet Tesisleri (İç Güvenlik Bakanlığı)

Yukarıdaki sınıflandırma ve kurumlararası görev dağılımı, ABD'de "kritik altyapı" terimi ile neyin kastedildiğini ve ne kadar geniş kapsamlı bir

tehdit algısına sahip olunduğunu ortaya koyması bakımından da son derece önemlidir.

11 Eylül Saldırıları, temelleri çok daha önce atılmış olan "kritik altyapının korunmasının gerekliliği" perspektifinden yeniden ele alındığı zaman görülmektedir ki; söz konusu saldırıların hedefinde yer alan Dünya Ticaret Merkezi ve Pentagon, simgesel birer ticari ve askeri hedef olmalarının ötesinde, Amerikan Ulusunun bekasını sağlayan birer kritik altyapı tesisidirler. Dolayısı ile, bu tesisler üzerinden Amerikan Ulusunun varlığına yönelik yapılmış olan böyle bir -terörist- saldırıya -teröre karşı- savaş ilanı ile cevap verilmesi de oldukça anlaşılır ve meşru bir durum halini almaktadır.

Mirabello'nun ifade ettiği üzere (2009: 270); nükleer silahların ve hassas askeri sistemlerin yanı sıra CIA ve FBI gibi kurumların bilgisayar sistemlerinin güvenliği "Hava Boşluğu *(Air Gap)*" olarak adlandırılan bir sistem ile sağlanmaktadır. Bu kapsamda söz konusu bilgisayar sistemleri doğrudan internete bağlanmamakta ve böylelikle de -kurum dışı- "hackerlar" için tümüyle erişilemez bir konumda bulunmaktadırlar. Gelişmiş ekonomilerin özellikle finans ve hizmet sektörlerindeki kritik altyapılarının, bilgisayarlar üzerinden ağa bağlı bir nitelikte olmalarının yarattığı güvenlik açığına vurgu yapan Mirabello (2009; 270); 14 Ağustos 2003 tarihinde gerçekleşen, ABD ve Kanada'da 50 milyondan fazla kişiyi etkileyen ve "Büyük Kesinti *(Great Blackout)*" olarak isimlendirilen genel elektrik kesintisini ise islami siber terörizme örnek olarak göstermektedir. Mirabello'nun aktardığı bilgilere göre; bahse konu kesinti sırasında 16 nükleer enerji santrali kendiliğinden kapanmış ve eylemin sorumluluğu, El Kaide Örgütü ile bağlantılı olduğu iddia edilen, Ebu Hafs El Masri Tugayları tarafından üstlenilmiştir.

Özellikle son dönemdeki siber güvenlik tartışmalarının merkezinde yer alan SCADA Sistemleri, kurulu oldukları tesisin temel üretim, dağıtım ve/veya tüketim süreçlerini kontrol etmektedirler. Kritik altyapı tesislerinde yoğun olarak kullanılmakta olan bu sistemler, siber sabotaj eylemlerinin de öncelikli hedefi konumundadırlar.

İlk defa ABD tarafından Sibirya'daki bir Sovyet boru hattı tesisine yönelilk olarak 1982 yılında yapılmış olan, SCADA Sistemlerini hedef alan siber saldırıların son örnekleri ise; İran'ın Buşehr Nükleer Reaktörü ve Natanz Uranyum Zenginleştirme Tesisine yönelik yapılan ve "Stuxnet" isimli bilgisayar virüsünün kullanıldığı siber saldırılardır. Cornish ve arkadaşlarına göre; Stuxnet'in kullanıldığı ve oldukça karmaşık olan son SCADA saldırıları, gelecekteki siber saldırıların ve siber savaşların potansiyelini göstermeleri açısından oldukça önemlidirler (Cornish ve diğerleri, 2010: 7).

Nitekim 28 Mayıs 2012 tarihinde Kaspersky Lab tarafından kamuoyuna duyurulduğu üzere (Kaspersky [web], 2012); Asya kıtasının batı bölgelerinde bulaşmış olduğu bilgisayarlardaki verileri silen kötü amaçlı bir yazılıma yönelik olarak yürütülen çalışmalar sırasında, 2010 yılının Mart ayından bu yana aktif olduğu ve karmaşık yapısı nedeniyle şimdiye kadar tespit edilemediği değerlendirilen "Flame" isimli yeni bir virüs tespit edilmiştir. Kaspersky Lab uzmanlarının yaptığı ilk tespitlere göre birincil amacının siber casusluk olduğu tahmin edilen söz konusu yeni virüsün, Stuxnet'ten 20 kat daha güçlü olduğu değerlendirilmektedir.

Washington Post Gazetesinin haberine göre ([web], 2012); "Flame" virüsünden ulusal çapta etkilendiklerini ifade eden İranlı yetkililer, söz konusu kötü amaçlı yazılım ve iki yıl kadar önce nükleer tesislerine zarar vermiş olan başka bir virüs -Stuxnet- arasında bağlantı olduğu ileri sürmüşlerdir.

Bu gelişmelerin hemen ardından, New York Times Gazetesinde çıkan bir habere göre ise ([web], 2012); ABD Başkanı Barrack Obama göreve başlamasından kısa bir süre sonra, İran'ın nükleer tesislerine yönelik hali hazırda yürütülmekte olan siber saldırıların arttırılması emrini vermiştir. Söz konusu siber saldırıların Başkan Bush döneminde "Olimpiyat Oyunları *(Olympic Games)*" kod adı ile başlatılmış bir siber sabotaj programının parçası olduğunun ve "Stuxnet" virüsünün de bu program kapsamında ABD ve İsrail tarafından ortak olarak geliştirildiğinin belirtildiği bahse konu habere göre; yapılan siber saldırılar neticesinde

İran'ın nükleer silah geliştirme programının yaklaşık iki yıl geriye götürüldüğü tahmin edilmektedir.

Waters'ın dikkat çektiği üzere (Waters ve diğerleri, 2008: 95-96); başlangıçta kurumsal ağ bağlantıları olmayan SCADA Sistemleri, küreselleşmenin ve enformasyon çağının dayattığı daha yüksek verimlilik, daha fazla şeffaflık ve daha fazla erişim sağlama kaygılarının sonucunda kurumsal ağlara bağlı hale getirilmişler ve bu durumun bir sonucu olarak da, kurumsal ağlara sızmış olan hackerların SCADA Sistemlerine erişebilmeleri mümkün bir hal almıştır.

Kritik altyapı tesislerine yönelik muhtemel tehditleri fiziksel ve siber tehditler arasında bir ayrıma gitmeksizin bir bütün olarak ele alan Devost'a göre (1997: 78'den aktaran Dunn Cavelty, 2008: 22-23); gerçek dünyada veya siber uzayda, tümüyle fiziksel ya da tümüyle sanal varlığa yönelebilecek olan muhtemel saldırıların aşağıdaki biçimlerde gerçekleştirilebilmeleri mümkündür:

- İletişim kablolarının kesilmesi veya koparılması örneğinde olduğu gibi, fiziki varlığına yönelik fiziksel saldırılar,

- SCADA Sisteminin hacklenmesi örneğinde olduğu gibi, fiziksel varlığına yönelik siber saldırılar,

- EMP[8] veya radyo frekansı tabanlı diğer Elektronik Savaş silahlarının kullanılması suretiyle, siber varlığına yönelik fiziksel saldırılar,

- Bağlı olunan bilgisayar ağının hacklenmesi örneğinde olduğu gibi, siber varlığına yönelik siber saldırılar.

[8] *Electomagnetic Pulse* (Elektromanyetik Darbe); yüksek irtifada gerçekleşen nükleer bir patlamanın, oldukça kısa -birkaç yüz nanosaniye- sürmesine rağmen yoğun ve yaygın nitelik gösteren bir elektromanyetik radyasyon fırtınasına bağlı olarak ortaya çıkan bir etkisidir (Kamienski, 2008: 136). Bahse konu etkinin, Gamma ışınlarının patlama merkezinin görüş alanı içerisinde kalan herşeyi kapsayacak biçimde bir radyo frekans dalgası üretmek üzere atmosfer ile etkileşime girmesinden kaynaklandığını ifade eden Kamienski'ye göre (2008: 136); söz konusu patlamanın yarattığı elektrik ve manyetik alanların mevcut elektrik ve elektronik sistemleri ile bir araya gelmesi ciddi zararlar yaratabilecek olan akım ve voltaj dalgalanmalarına sebebiyet vermektedir. Yine Kamienski'nin dikkat çektiği üzere (2008: 136); bu çerçevede karada, denizde ve havada yeralan söz konusu sistemler paralize olabileceği ve geri döndürülemeyecek biçimde zarar görebileceği gibi radyo trafiğinin ve radar sinyallerinin de ciddi iletişim sorunlarına neden olacak bir biçimde kesintiye uğrayabilmeleri mümkündür.

Algılanmakta olan "siber terörizm tehdidi"nin -ABD açısından- ne oranda somutlaştığı noktasında ise, Dolnik'e göre (2007: 35); son yıllarda siber saldırılara ilişkin değerlendirmelerin medyada çok daha fazla yer almasına rağmen, gerçek hayatta karşılaşılan siber terörizm vakaları marjinal seviyede kalmaktadır.

Siber tehditlerin ABD'de, 1995 yılında yaşanılan Oklahoma Saldırısı sonrasında kritik altyapının korunması ve terörizm ile ilişkilendirilmeye başlandığını ifade eden ve 11 Eylül 2001 tarihinden sonra kritik altyapının korunmasının iç güvenlik olgusunun merkezine yerleştiğine dikkati çeken Dunn Cavelty (2008: 91-92); bu yeni dönemdeki siber tehdit algısının, özellikle siber araç ve yöntemlerin terörizmin fiziksel biçimleri ile entegre edilmesi üzerine odaklandığını belirtmektedir.

ABD'de kritik altyapının korunmasının, 11 Eylül Saldırıları sonrası dönemde her zamankinden çok daha önemli bir sorun haline geldiğini belirten Lerner ise (2004a: 282); alınan bazı tedbirlerin sivil haklar savunucularının öfkesini çektiğini belirterek, gelecekte kritik altyapı sistemleri üzerinde çok daha sıkı bir korumanın görülmesinin de muhtemel olduğunu ifade etmektedir.

Bu kapsamda "ABD Vatanseverlik Yasası (USA PATRIOT Act)"nı eleştirel bir yaklaşımla ele alan ve 2003 yılı itibariyle aktif olduğu ispat edilmiş herhangi bir siber terörist bulunmadığına dikkati çeken Skibell ise (2003: 920); siber kıyamet senaryoları ve siber teröristler üzerinden, güvenlik tehditlerinin abartıldığı kanaatindedir.

(5) Siber Suçlar *(Cybercrimes)*

"Siber Suç" teriminin İlk kez enformasyon güvenliği uzmanı Donn B. Parker tarafından kullanılmış olduğunu ifade eden McCrie'ye göre (2001: 397); bahse konu terim, enformasyon teknolojileri ile ilişkili bir dizi kanun ihlalini kapsamaktadır.

Waters ve çalışma arkadaşlarının dikkat çektiği üzere ise (2008: 57), ABD Hükümetine bağlı olarak faaliyet gösteren GAO'nun konu ile ilişkili raporlarında kullandığı biçimi ile siber suç terimi; zarar vermek veya sızmak maksadıyla belirli bir bilgisayarı veya ağı hedef alan suç eylemlerinin yanı sıra suç eylemleri gerçekleştirmek üzere bilgisayarların birer araç olarak kullanıldığı durumları da içermektedir.

İngiliz suç bilimcisi David Wall tarafından yapılmış olan bir tasnifine göre ise, siber suçlar şu dört ana başlık altında toplanabilmektedirler (Wall, 1999'dan aktaran Marsh, 2004: 125-126):

- Yetkisiz Erişim *(Cyber-Trespass)*
- Siber Hırsızlık *(Cyber-Thefts)*
- Siber Müstehcenlik *(Cyber-Obscenities)*
- Siber Şiddet *(Cyber-Violence)*

David Wall'ın siber suçlara ilişkin olarak yapmış olduğu, siber güvenliğin diğer boyutları ile siber suç boyutu arasındaki kritik ilişkiyi ortaya koyan oldukça önemli bir tespit de, suçun mağdurlarına ilişkindir. Wall'a göre; "kimlik gizleme *(cyberstalking)*" veya "siberpara hırsızlığı *(theft of cybercash)*" gibi olaylarda mağduriyet çoğunlukla doğrudan bir şahsa yönelik iken, "siber korsanlık *(cyberpiracy)*" veya "siber casusluk/terörizm *(cyberspying/terrorism)*" gibi olaylarda ise mağduriyet çok daha dolaylı bir biçimde ortaya çıkmaktadır (Wall, 1999'dan aktaran Marsh, 2004: 126).

Siber suç olgusu siber güvenlik kapsamındaki asıl önemini ise özellikle yetkisiz erişim noktasında göstermektedir. Zira ister siber savaş, ister siber casusluk, isterse de siber terörizm olarak nitelendirilsin; siber uzaydaki güvenlik ihlallerinin veya art niyetli eylemlerin tamamının amacı ve -eğer başarılı olunabilirse- sonucu, bir sisteme veya veriye yetkisiz erişim sağlanmasıdır. Bu çerçevede siber saldırıların ve tehditlerin, ne kadar farklı ve dikkat çekici şekilde isimlendirilirlerse isimlendirilsinler, hukuk sistemleri tarafından "adi birer siber suç" olarak nitelendirilerek yetkisiz erişim kapsamında değerlendirilebilmeleri mümkündür. Böylelikle hem bu gibi suçların devlet aleyhine ya da başka bir devlet, grup veya

kurum adına işlenmesi durumunda ilave düzenlemelere ve değerlendirmelere ihtiyaç duyulmaksızın mevcut ceza kanunu veya terörle mücadele mevzuatı kapsamında daha ağır cezaların verilmesi mümkün olmakta, hem de suçun niteliğine ve gelişimine ilişkin kararın verilmesinde yargı mekanizmaları fazla teknik bilgiye ihtiyaç duymamaktadır. Esnekliğin ön planda olduğu bu tarz bir yaklaşımın; kanunların yapılmalarına ilişkin yasama süreçleri içerisinde de teknik bilgiye duyulan ihtiyacı önemli oranda azaltırken, yasama tarafından öngörülen düzenleme ve tedbirlerin mevcut adli yapı tarafından daha kolay anlaşılmasını ve benimsenmesini sağlayacağını da ileri sürmek mümkündür.

Siber suçlar ile diğer siber güvenlik tehditleri arasında ortaya çıkan bu hiyerarşik durumun bir benzeri, siber suçlar ile diğer suçlar arasında da ortaya çıkmaktadır. Nitekim "siber" ön ekini taşıyan pek çok olgunun da kendi evrenleri içerisinde karşı karşıya kaldıkları gibi; varoldukları hukuk sistemi içerisinde siber suçların bağımsız bir suç kategorisini oluşturması gerektiğine ilişkin yaklaşım ile siber suçların aslında teknolojik gelişmelere bağlı olarak işleniş biçimleri değişmiş geleneksel suçlar olduklarına ve mevcut suç kategorileri kapsamında değerlendirilmeleri gerektiğine ilişkin yaklaşım arasında yapılan tercih, siber suçların tanım, kapsam ve niteliklerini kritik bir biçimde şekillendirmektedir.

Her tanımlamanın aynı zamanda bir sınırlama da olduğu ve kapsamına aldıkları kadar kapsamı dışında bıraktıklarının da bulunduğu gerçeği göz önüne alındığında; siber suçların tanım ve kapsamlarına ilişkin olarak -belki de yukarıda dikkat çekilmeye çalışılan esnekliği yitirme kaygısından kaynaklanan nedenlerle- genel kabul görmüş bir tanımlama ve sınıflandırma yapılamamış olması çok da şaşırtıcı gelmemektedir. Bununla birlikte söz konusu suçlara ilişkin genel kabul; bilgisayarların veya ağların yasadışı olarak hedef alındıkları ve bu yasadışı eylemlerde de genellikle diğer bir bilgisayarın kullanıldığı suçlar oldukları yönündedir.

Kavramsal açıdan bakıldığında, siber suçların yanı sıra bu suçlar ile yakından ilişkili olan "bilişim sistemi" ve "veri" kavramlarının da bir belirsizlik içerisinde oldukları görülmektedir. Söz konusu kavramların içerisinde bulundukları muğlaklık ve buna bağlı olarak oldukça geniş

yorumlanabilmeleri; saniyede trilyonlarca işlem yapan süper bilgisayarlar ile elektronik daktiloların ya da ulusal güvenlik açısından oldukça kritik şifrelenmiş enformasyon ile yaygın biçimde kullanılan basit müzik dosyalarının aynı kategoride değerlendirilebilmelerini mümkün hale getirmektedir.

Nitekim ABD yasama mekanizması söz konusu tanım sorununu - sadece siber suçlara özgü olmayan, genel nitelikli bir uygulama kapsamında-; Federal Kanunlar Külliyatı (USC) içerisinde, belirli ana bölüm başlıkları altında o bölümde yer alan önemli kavramları terimsel olarak açıklamak ve gerek görülmesi halinde ilgili kanun maddeleri ile paralel olarak bu açıklamaları da revize etmek suretiyle, etkin bir biçimde çözüme kavuşturmuştur.

Siber güvenlik tehditleri içerisindeki en somut olguyu oluşturan siber suçlar, doğal olarak siber güvenlik çabalarının da büyük bir kısmını kendi üzerlerine çekmektedirler. ABD merkezli Ponemon Enstitüsü tarafından siber suçların ABD firmaları üzerindeki özellikle mali etkilerine ilişkin olarak gerçekleştirilen, çeşitli sektörlerden büyük ölçekli 45 örgütü kapsayan ve 2010 yılında yayımlanmış olan "Siber Suçların Yıllık Maliyetine İlişkin Çalışma"nın, 50 örgütü kapsayan ve 2011 yılında yayımlanan ikincisinde yer alan tespitler, gerek siber suçların güncel niteliklerini, gerekse de kısa zaman içerisinde geçirebildikleri değişimi göstermesi açısından oldukça önemlidir (Ponemon Enstitüsü, 2011: 2-3):

- Bir önceki yıla göre, siber suçların ortalama maliyeti % 56 oranında, başarılı siber saldırıların sayısı ise % 44 oranında artış göstermiştir.

- Siber suçların maliyeti ile örgütsel boyut arasında pozitif bir ilişki olmakla birlikte, söz konusu suçların küçük örgütler üzerindeki etkileri daha ağır olmaktadır.

- "Zararlı Yazılımlar *(Malicious Codes)*", "Hizmetin Reddi Saldırıları *(Denial of Service)*", Çalınan veya Kaçırılan Cihazlar ve "Kurumiçi Kötü Niyetli Kişiler *(Malicious Insiders)*" maliyet açısından

kurumlara en büyük zararı vermekte ve toplam maliyetin % 90'ından fazlasına neden olmaktadır.

- Kısa sürede çözülemedikleri takdirde siber saldırıların maliyetleri daha da artmaktadır. Bir siber saldırının çözülmesi için geçen ortalama zaman, önceki yıla göre 4 gün artarak 18 güne çıkmış ve bu süre zarfında saldırının neden olduğu ortalama maliyet ise önceki yıla göre % 67 oranında artmıştır.

- Tüm dışsal kayıpların % 40'ını "Enformasyon Hırsızlığı *(Information Theft)*", % 28'ini ise ticari faaliyet veya verimlilik kayıpları oluşturmaktadır.

- Tüm içsel maliyetlerin % 45'ini, "Kurtarma *(Recovery)*" ve "Tespit *(Detection)*" faaliyetleri için yapılan işgücü ve nakit ödemeleri oluşturmaktadır.

- Tüm sektörler farklı seviyelerde de olsa siber suçlardan etkilenmektedirler. Savunma, altyapı, enerji ve finans sektörlerindeki firmalar; perakende, konaklama ve tüketici ürünleri sektörlerindeki firmalara göre çok daha yüksek yıllık ortalama maliyetler ile karşı karşıya kalmaktadırlar.

- SIEM[9] Teknolojilerini ve GRC[10] Uygulamalarını kullanan firmaların katlanmak zorunda kaldıkları ortalama yıllık maliyetler, bunları kullanmayanlara oranla çok daha düşüktür.

İnternet kullanımının hızla yayılmasının siber suçlarda dramatik bir artışa yol açtığına dikkati çeken Waters ise, siber suçları önlemeye yönelik

---

[9] *Security Information and Event Management* (Güvenlik Bilgisi ve Olay Yönetimi): SIEM çözümleri olarak da adlandırılan bu siber güvenlik uygulamaları, önceleri siber güvenlik alanındaki farklı ürün kategorilerini oluşturan SIM (*Security Information Management)* ve SEM (*Security Event Management*) çözümlerinin birleştirilmesi ile ortaya çıkmıştır. Bu kapsamda SEM teknolojisi, ağ donanımı ve uygulamaları tarafından oluşturulan güvenlik uyarılarının gerçek zamanlı olarak analiz edilmesini sağlarken; yazılım, cihaz veya yönetilebilir hizmetler olarak gelebilen SIEM çözümleri ise güvenlik verilerini kaydetmek ve uyumluluk sağlamak üzere raporlama için kullanılmaktadırlar (Wikipedia [web], 2012c).

[10] *Governance, Risk Management, and Compliance* (Yönetişim, Risk Yönetimi ve Uyumluluk): Bir örgütün yönetişim, risk yönetimi ve uyumluluk alanlarına yönelik yaklaşımlarını kapsayan şemsiye bir terim olup; kaynakların verimli kullanılması maksadıyla yönetişim, risk yönetimi ve uyumluluk faaliyetlerinin bütünleştirilmesi ve birleştirilmesi faaliyetlerini kapsamaktadır (Wikipedia [web], 2012a).

-bir anlamda standart ve hatta rutin- çabaları ise şu başlıklar altında sıralamaktadır (Waters ve diğerleri, 2008: 47);

- Ağları ve enformasyonu korumak,
- Suç teşkil eden eylemi tespit etmek,
- Suçu soruşturmak,
- Suçluları kovuşturmak.

Nitekim siber suçlara ve onları önlemeye yönelik çabalara ilişkin genel bir değerlendirme yapılması durumunda; siber uzayın genişlemesine paralel olarak siber tehditlerin sürekli olarak arttığı bir dünyada, gerek siber güvenliğin sağlanmasında, gerekse de siber suçlarla mücadelede en önemli araç olan "siber hukuk" ya da "bilişim hukuku"nun, kişisel maddi çıkar sağlama amacının ön planda yer aldığı ve internet tabanlı olarak işlenilen yasadışı eylemlere yoğunlaşmış olduğunu ileri sürmek yanlış olmayacaktır.

ç. Elektronik Savaş ve Enformasyon Savaşı

Çalışmanın bu bölümünde, siber güvenlik olgusunun kapsamının belirlenmesine ilişkin olarak önceden dikkat çekilmiş olan bazı tercihlere dayalı olarak, siber uzay ve onun güvenliği ile yakından ilişkili iki kilit kavram olan "Elektronik Savaş" ve "Enformasyon Savaşı" ele alınmıştır.

Bahse konu kavramlar ile ilişkilendirmek suretiyle siber güvenliğin kapsamının; elektronik savaş olgusu üzerinden özellikle cihaz ve sistem boyutunda, enformasyon savaşı olgusu üzerinden ise veri ve amaç boyutunda genişletilmesi mümkündür. Çok daha geniş bir görüş açısı sağlayan bu yeni perspektif ile bakıldığı zaman siber güvenliğin temel ve öncelikli var olma amacı; kişilerin veya toplumun korunmasından ziyade,

siber uzay ve onunla bağlantılı cihaz, veri ve hizmetlerin korunması olarak netlik kazanmaktadır.

(1) Elektronik Savaş *(Electronic Warfare)*

Çalışmanın siber uzaya ilişkin kısmında da dikkat çekildiği üzere; askeri bakış açısına göre siber uzay, sadece bilgisayarlardan meydana gelmemekte ve aynı zamanda elektromanyetik spektrumu da içermektedir. Bu kapsamda D.C. Schleher'e göre (1993: 109-183'den aktaran Özçelik, 2006: 3); "Elektronik harp kavramı, temel olarak, potansiyel düşman elektronik savaş sistemlerinin kabiliyetleri hakkında istihbarat bilgisi toplamak amacıyla bu sistemlerden yayılan elektromanyetik sinyalleri toplama ve analiz etme, mevcut düşman elektronik savaş sistemlerinden yayılan elektromanyetik sinyalleri algılama ve tanıma ile elektronik iletişim ve silah sistemlerinin düşmanlar tarafından etkin bir şekilde kullanılmasını engellemek amacıyla elektromanyetik sinyaller üretme ve gönderme faaliyetlerini kapsamaktadır."

Dolayısı ile Schleher'in tanımının merkezinde yer alan "elektronik savaş" teknolojisine dayanılarak geliştirilebilecek olan tehditlerin de siber uzaya yönelik güvenlik kaygılarını yansıtan siber güvenliğin kapsamı içerisine dahil edilebilmeleri mümkündür. Ancak gerek sayıca az ve oldukça profesyonel bir kitlenin ilgi alanına girmesi, gerekse de dördüncü nesil savaş konseptinin "ayaklanma *(insurgency)*" merkezli insan eylemlerine odaklanmış olması nedenleriyle elektronik savaş olgusunun genel olarak kamuoyundaki bilinirliği sınırlı kalmaktadır.

1984-1990 yılları arasında Avustralya Savunma Bakanlığı da yapmış olan, Batı Avustralya Üniversitesinden Sosyal ve Politik Teori Profesörü Kim C. Beazley; ülkesinin Afganistan'da bulunan birliklerine 2002 yılında yaptığı bir çalışma ziyareti kapsamında, Bagram Üssünde yaptığı incelemelerde edindiği izlenimleri şöyle ifade etmektedir (Waters ve diğerleri, 2008: xix):

"Orada, Tümenin lojistiğinden sahadaki birimlere kadar her şeyi kontrol etmek üzere, kişisel bilgisayarların olduğu masaların arkasında oturan askerler gördük. Elektromanyetik alandaki ABD hâkimiyeti ile onun siber uzayda kullanımı arasındaki etkileşime şahit olduk. Uydular, devam eden çarpışmaya ve onun içerisindeki kuvvetlerin iletişimlerine odaklanmışlardı. Tümen Komutanı, kuvvetlerinin ve onlarla çarpışanların tam konumlarına sahipti."

Fahrenkrug ise, siber uzay ile elektronik savaş arasındaki ilişkiyi oldukça net ve çarpıcı bir biçimde şöyle ortaya koymaktadır ([web], 2007):

"Siber uzayın askeri tanımı, onun salt bilgisayar ağlarından daha fazlası olduğunu kabul eder. Daha da önemlisi, ağ sistemlerinin elektromanyetik enerjinin kullanılması vasıtasıyla yaratılmış olmaları nedeniyle; siber uzayda savaşmak, zorunlu olarak, şu anda elektronik savaş olarak kabul edilen yetenekleri içerecektir. Doğrudan internete bağlı olmayan ağlar dahi, ağın elektronik bileşenlerini taramak veya bozmak üzere elektromanyetik enerjinin kullanılması suretiyle, potansiyel olarak erişilebilir ve saldırılabilir hale gelebilir. Bu ordu için önemli bir ayrımdır."

Siber uzay ve elektronik savaş olguları arasında kurulan bu ilişki, dar anlamda siber savaşın, geniş anlamda ise siber güvenliğin kapsamını genişleten ve onları gerçek -fiziksel- dünyaya oldukça yaklaştıran bir nitelik taşımaktadır. Siber savaş ve siber güvenlik üzerinde benzeri bir etkiye sahip olan diğer bir olgu ise, yine bu çalışma kapsamında ele alınmış olan, enformasyon savaşıdır.

Avustralya Savunma Kuvvetlerinin enformasyon üstünlüğünü sağlamak üzere dönüşmesi gerektiğini savundukları ve enformasyon operasyonları *(information operations)*'na ilişkin bir dizi varsayımsal senaryoya yer verdikleri ortak çalışmaları 2005 yılında yayımlanmış olan Waters ve Ball'a göre (2005'den aktaran Waters ve diğerleri, 2008: 1); enformasyon operasyonları -bahse konu varsayımsal senaryolarda da yer verildiği üzere-, bir düşman hava saldırısının siber bir saldırı ile mağlup edilmesini, düşman donanmasının bir elektronik savaş saldırısı ile hareketsiz bırakılmasını, düşman hava savunma sistemlerine yönelik karıştırma ve aldatma uygulanmasını, düşman komuta kontrol ve iletişim sistemlerinin yok edilmesini veya devre dışı bırakılmasını ve düşman bilgisayar ağlarının çökertilmesini kapsayabilmektedir.

Siber saldırıların yanı sıra elektronik savaş uygulamalarını da içeren enformasyon operasyonlarının siber güvenliğin kapsamı içerisinde değerlendirmeye alınmaları ile birlikte; siber güvenlik olgusunun kapsamı hem ciddi bir biçimde genişletmekte, hem de gerçek -fiziksel- dünyaya hiç olmadığı kadar yakınlaşmaktadır.

Fahrenkrug'un da ifade ettiği üzere ([web], 2007); siber uzayın elektromanyetik çevre içerisindeki fiziksel bir alan olarak tanımlanması, siber uzayda savaşmayı da fiziksel operasyonlar ile alakalı bir hale getirmektedir. Bu çerçevede Fahrenkrug; -kara, hava, deniz ve uzay ile birlikte- bir savaş alanı olarak görülen siber uzayda yürütülecek siber operasyonların, düşmanı etkilemek üzere diğer savaş alanlarında da yürütülecek olan enformasyon operasyonlarını hem destekleyeceği, hem de geliştireceği görüşündedir.

Bu noktada elektronik savaş kapsamında yer almamakla birlikte, elektronik cihazların yaydıkları elektromanyetik salınımlar üzerinden enformasyon güvenliğine yönelik belki de en ciddi tehdidi oluşturan Tempest Radyasyonu'na değinmek uygun olacaktır. Zira Tempest Radyasyonu, gerek enformasyonun ve dolayısı ile de verinin korunması boyutunda, gerekse de bilişim sistemlerinin donanımsal ve fiziki güvenliklerinin sağlanması boyutunda doğrudan siber güvenliğin kapsamı içerisinde yer almaktadır. Bu çerçevede "Tempest" olgusunun günümüzde gereğince ele alınmamasında; kamuoyunun yeterince bilgilendirilmemiş olmasının ve söz konusu salınımın elektronik cihazların çalışmalarının doğal bir sonucu olarak -pasif bir şekilde- ortaya çıkmasının etkili olduğunu ileri sürmek mümkündür.

Bilgisayarların, enformasyon sızıntısına neden olacak biçimde ve seviyede elektromanyetik radyasyon yaydıklarının askeri kurumlar tarafından 1960'lı yılların başından bu yana bilindiğine dikkati çeken Kuhn ve Anderson (1998: 124); ciddi endişe yaratan bu olgunun, verilerin elektromanyetik olarak yayımlanması sorununu gidermek üzere ABD hükümeti tarafından yürütülen resmi bir program kapsamında kullanılan şifreli bir sözcük olan "Tempest"e atfen, "Tempest Radyasyonu" olarak adlandırıldığını ifade etmektedir.

ABD hükümeti tarafından, söz konusu kelimenin bir kısaltma olmadığının ve herhangi bir özel anlam taşımadığının açıklanmasına rağmen (Wikipedia [web] 2012d); pek çok kaynakta "Tempest" kelimesinin bir kısaltma olarak kabul edilerek değişik açılımlarına yer verildiğini görebilmek de mümkündür.

(2) Enformasyon Savaşı *(Information Warfare)*

Enformasyon altyapıları ile ulusal güvenlik arasındaki bağlantının ciddi bir biçimde, ilk kez İkinci Dünya Savaşı sonrasında ve özellikle askeri literatürde kurulduğuna dikkati çeken Dunn Cavelty (2008: 41); bu nedenle de bahse konu bağlantının, yaygın bir biçimde askeri düşüncenin bir parçası olarak kabul edildiğini ifade etmektedir.

Anderson ve Sloan'a göre (2009: 270); enformasyon odaklı savaş, düşük ve yüksek yoğunluklu çatışmalar ile ilişkili olup, kısmen de olsa komuta, kontrol, iletişim ve istihbarat maksatlı bilgisayar altyapılarının fiziksel saldırılar, hackleme veya bilgisayar virüsleri vasıtası ile doğrudan hedef alındıkları "Stratejik Enformasyon Savaşı"nı da içerebilmektedir.

Geleneksel tanımlara oldukça yaklaşan ve "enformasyon" merkezli bir tanımlama yapma yoluna giden Ivan Goldberg'e göre ise (Tanwar, 2005: 21);

> "Enformasyon savaşı; kendininkileri korurken, düşmanın enformasyonunu, enformasyon bazlı süreç ve sistemleri ile bilgisayar bazlı ağlarını engellemek, istismar, tahrip ve yok etmek üzere, enformasyonun ve enformasyon sistemlerinin saldırı ve savunma maksatlı kullanılmasıdır."

Siber savaş, elektronik savaş ve siber sabotaj olgularını bünyesinde birleştiren enformasyon savaşının, gerçek hayattaki somut halini ve ABD'deki profilini ise; 1990'lı yıllardaki çalışmalarına ve anılarına dayanarak, ABD'li Gazeteci William M. Arkin şöyle ortaya koymaktadır (Priest ve Arkin, 2011: 58):

"J39, Genelkurmay Başkanlığı emrindeki bir kurmay makamıydı ve Pentagon'un derinlerindeki bürolardan oluşan bir yuvada faaliyet gösteriyordu. Daire, en yüksek gizlilikteki siber savaş programlarını, cihazları patlatmak yerine bozan silahları, düşmanın elektrik güç şebekesinde kısa devre yaptırabilecek yüksek güçlü mikrodalgaları ve yükleyici karbon fiberleri kullanan elektronik veya bilgisayar kontrolleri gibi cihazları yönetti.

Siber sabotajı da içeren bir dizi gizemli faaliyeti de kapsayan J39 programları, Özel Teknik Operasyonlar (STO) olarak isimlendirildiler ve dünyanın belirli bir bölgesinde savaşmakla görevli olan her askeri komutanlıkta, hızla ortaya çıkmaya başladılar."

Ulusal Savunma Üniversitesinden Martin Libicki'nin, enformasyon savaşının yedi değişik biçimi olduğunu ileri sürdüğü ifade eden Waters ve çalışma arkadaşları ise; her biri enformasyon savaşı olgusunun farklı boyutlarına vurgu yapan söz konusu biçimleri -Libicki'ye atfen- şöyle sıralamaktadırlar (Libicki, 1995: 7'den aktaran Waters ve diğerleri, 2008: 37-38):

"* Komuta ve kontrol sistemlerine saldırmak suretiyle komuta ile kuvvetleri ayırmanın hedeflendiği, Komuta Kontrol Savaşı *(Command and Control Warfare)*.

* Enformasyonu toplamak, faydalanmak ve korumak suretiyle diğer saldırı biçimlerini desteklemeyi hedefleyen, İstihbarat Tabanlı Savaş *(Intelligence-based Warfare)*.

* Aktarım ve formatlara odaklanmak suretiyle iletişime saldıran, Elektronik Savaş *(Electronic Warfare)*.

* İnsan zihnine saldıran, Psikolojik Savaş *(Psychological Warfare)*.

* Küresel Enformasyon Altyapısı *(Global Information Infrastructure)*'nı kapsayan, Hacker Savaşı *(Hacker Warfare)*.

* Belirli enformasyonları idare etmek suretiyle bir ekonomiyi kontrol etmeyi hedefleyen, Ekonomik Enformasyon Savaşı *(Economic Information Warfare)*.

* Terörizm, simülasyon ve gerçeklik kontrolünün kuramsal biçimlerini bir araya getiren, Siber Savaş *(Cyber Warfare)*."

Libicki'nin sınıflandırması esas alındığı zaman da net bir biçimde görülebileceği üzere; gerek "veri", gerekse de "donanım", "cihaz" ve "sistem" bağlamında siber güvenlik alanındaki tartışmaların merkezinde yer alan pek çok endişe ve olgunun, enformasyon savaşının ve dolayısı ile de enformasyon güvenliğinin kapsamı içerisinde değerlendirilebilmesi mümkündür. Nitekim NATO'nun Kosova'ya yönelik 1999 yılındaki müdahalesi, enformasyon savaşı olgusunun gerçek boyutlarını açık bir biçimde ortaya koyması açısından oldukça önemli bir örnektir.

"Müttefik Kuvvet Operasyonu *(Operation Allied Force)*" olarak bilinen bahse konu operasyon kapsamında karşı tarafa zarar verebilmek için, propaganda, dezenformasyon ve elektronik savaş gibi enformasyon savaşı unsurlarının her iki tarafça da kullanıldığına dikkati çeken Dunn Cavelty (2008: 73); operasyon süresince internetin artan bir şekilde kullanılmış olmasının söz konusu çatışmanın "siber uzayda yapılan ilk savaş" veya "internet üzerindeki ilk savaş" olarak nitelendirilmesine neden olduğunu ifade etmektedir.

Libicki'nin yukarıda yer verilmiş olan sınıflandırmasında dikkati çeken önemli bir diğer husus da; "enformasyon" unsurunun, hem kişinin yürüttüğü düşünme faaliyetinin bir parçası olan soyut bir gerçeklik olarak "bilgi" kimliği üzerinden, hem de elektronik savaş teknolojisinin odaklandığı somut bir gerçeklik olarak "veri" kimliği üzerinden ele alınmakta olmasıdır.

"İçerik" ve "biçim" üzerinden ulaşılan bu noktada; Hindistan Silahlı Kuvvetlerinden S.P. Tanwar'ın, enformasyon savaşına yönelik farklı yaklaşımlar arasında yapmış olduğu karşılaştırmaya da yer vermek uygun olacaktır. Bu kapsamda enformasyon savaşının, "savaşta enformasyonu kullanmak" ve "bir savaş biçimi" olmak üzere iki şekilde yorumlandığını belirten Tanwar (2005: 19-20); savaşın daha etkili bir şekilde yürütülebilmesi için enformasyondan azami seviyede faydalanılmasını savunan ilk grubun karşısında, medya, enformasyon ve iletişim teknolojilerindeki hızlı gelişmeye bağlı olarak enformasyon savaşını bağımsız bir savaş biçimi olarak kabul etme eğiliminde olan ve ağırlıklı olarak enformasyon uzmanlarından oluşan ikinci grubun yer aldığını ifade etmektedir.

2. KURAMSAL ÇERÇEVE

Çalışma yöntemine ilişkin olarak giriş kısmında da belirtildiği üzere oldukça net ve kesin sınırlara sahip olan bu çalışma; siber güvenliğin sağlanması kaygısı ile asimetrik tehditleri karşılamak üzere, belirli bir zaman dilimi -11 Eylül 2001 tarihinden günümüze- ve belirli bir yapı -ABD- içerisinde, belirli bir etkinin -11 Eylül Saldırıları- sonucu olarak ortaya çıkmış olan belirli tepkilerin -hukuksal ve politik- nitelik ve biçimlerinin tespit edilmesine yönelik bir çabanın eseridir.

Siber güvenlik olgusunun çalışma kapsamında ele alınış biçimine ilişkin olarak ise, burada bir kez daha ifade etmek gerekir ki; siber güvenliğin, çoğunlukla bilgisayar odaklı enformasyon teknolojilerine ve uygulamalarına vurgu yapan "teknik boyutu" ile, ulusal güvenlik kaygıları üzerinden siyasal ve hukuksal uygulamalara vurgu yapan "sosyal boyutu" arasında ciddi bir ayrım bulunmaktadır. Bu çerçevede, bir ülkenin ulusal güvenliğini bütüncül bir şekilde sağlamakla sorumlu olan üst seviye güvenlik karar alıcılarının; nasıl ki terörle mücadele kapsamında başvurulabilecek asimetrik çatışma ya da örtülü operasyon biçimleri konusunda uzmanlık seviyesinde teknik derinliğe sahip olmaları beklenilemez ise, bilgisayar ve enformasyon teknolojileri alanında da benzeri bir uzmanlık beklentisi içerisinde bulunulmaması gerekir. Siber güvenliğin teknik boyutunun çok daha derin ve karmaşık olmasının yanı sıra söz konusu boyut çoğu zaman için akademik kuruluşların ve özel sektör firmalarının faaliyet alanları ile de kesişmektedir. Dolayısı ile gerek tümüyle teknik mahiyette olması ve gözlem yapma yoluyla tam olarak kavranamayacak bir karakter taşıması, gerekse de kamu ve özel sektörün karma bir faaliyet alanı oluşturması nedeniyle; siber güvenliğin "teknik boyutu" bu çalışmanın kapsamı dışında bırakılmıştır.

Çalışma, "faydacı" bir yaklaşım çerçevesinde ele alındığında ise; ileride yapılabilecek daha ayrıntılı ve derinlemesine yapısal ya da tarihsel çözümleme çalışmaları için fikir verici bir kavramsal ve kurumsal çerçeveyi sağlama potansiyeline sahip olduğu değerlendirilmektedir. Her ne kadar,

bilimselliğin asli kaynağı olan nesnelliğin korunması maksadıyla azami gayret sarf edilmiş ise de; bu çalışmanın kapsamına, bu kapsam içerisinde yer aldığı iddia edilen olgu, kavram, terim ve ilişkilere, söz konusu ilişkilerin biçimlerine, niteliklerine ve sonuçlarına ilişkin olarak yapılmış olan her türlü tespit elbette ki eleştiriye açıktır.

Önceden de ifade edildiği üzere belirli bir teorinin gölgesinde yer almayan ve belirli bir hipotezi haklı çıkarma kaygısı taşımayan bu çalışma kapsamında olguları ve tespitleri daha anlaşılır kılmak maksadıyla; güvenlik tehditleri ve politikaları ile ilişkilendirilebileceği değerlendirilen bazı teorik yaklaşımlara çalışmanın kuramsal çerçeve kısmında yer verilmiştir.

Bu kapsamda, siber güvenliğin de bir alt dalını oluşturduğu ulusal güvenliğe ilişkin olarak geliştirilen algıların, alınan kararların ve karar alıcı davranışlarının çözümlenmesinde ve değerlendirilmesinde, siyaset bilimi, uluslararası ilişkiler, sosyoloji, psikoloji, ekonomi veya tarih gibi birçok disiplinde tekil ya da disiplinlerarası bir yaklaşımla geliştirilmiş olan çok sayıda kuramdan faydalanılabilmesi mümkündür. Böyle bir ortam içerisinde, tehdit algılarının ve güvenlik politikalarının ortaya çıkış süreçlerinin bu çalışmanın kapsam ve amacı dışına taşılmaksızın sağlıklı bir biçimde ortaya konulabilmesi maksadıyla; gerek sadeliği ve özlü anlatımı, gerekse de çalışma konusu ile doğrudan ilişkili içerik ve yaklaşımı nedeniyle, M. Dunn Cavelty'nin *"Cyber Security and Threat Politics"* isimli çalışmasında ortaya konulmuş olan kuramsal çerçeve örneği benimsenmiştir.

a. Güvenlikleştirme Teorisi *(Securitisation Theory)*

Dunn Cavelty'e göre (2008: 24); tehdit politikalarını ortaya çıkaran mekanizmaları tam olarak anlayabilmek için iki aşamalı bir yaklaşıma ihtiyaç duyulmaktadır. Bu kapsamda "ilk çerçeveleme" ve "güvenlikleştirme hamlesi"ni içeren ilk aşamanın, "mesele"nin başarılı bir şekilde güvenlik gündeminin bir parçası olma yoluna girmesi ile ilk politik

tepkilerin ortaya çıkmasına kadar geçen dönemi kapsadığını ifade eden Dunn Cavelty; ikinci aşamanın ise "mesele" güvenlik gündeminde yerini aldığı zaman başladığı görüşündedir.

Ulusal ve uluslararası sistem içerisindeki güvenlik arayış ve uygulamalarını açıklamak kaygısı ile geliştirilmiş olan Güvenlikleştirme Teorisini, Kopenhag Okulu ve onun karşısında yer alan Paris Okulu üzerinden ele alan Dunn Cavelty; bahse konu teoriyi özellikle güvenlik algısının üretilmesi ve güvenlikleştirme süreçleri noktasında, "Çerçeveleme Teorisi *(Framing Theory)*" ve "Gündem Belirleme Teorisi *(Agenda-Setting Theory)*" ile de ikame etmektedir (2008: 24-40).

(1) Kopenhag Okulu

Sosyal birer gerçeklik yaratma noktasında bireylerin sözlü ifadelerinin en az fiili davranış ve tutumları kadar önemli olduğunu savunan "Söz Edimi Teorisi *(Speech Act Theory)*"ne dayalı olarak geliştirilmiş olan "Güvenlikleştirme *(Securitisation)*" kavramı, zaman içerisinde Kopenhag Okulu ile bir anlamda bütünleşmiştir. Güvenlikleştirme merkezli çalışmaları kapsamında, "Söz Edimi Analizi *(Speech Act Analysis)*" ve "Söylem Analizi *(Discourse Analysis)*"ne büyük önem veren Kopenhag Okulunun önde gelen isimleri arasında; Barry Buzan, Ole Waever ve Jaap de Wilde yer almaktadır (Dunn Cavelty, 2008: 25)

Kopenhag Okuluna hakim olan temel yaklaşımın temsilcisi Buzan'a göre, bir meselenin gerçek bir tehdit yaratmasının zorunlu bir sonucu olarak değil, kilit ajanlar tarafından başarılı bir şekilde böyle bir tehdit yaratıyormuş gibi sunulduğu ve bu durum resmileştirildiği için bir güvenlik sorunu haline geldiğine dikkati çeken Dunn Cavelty (2008: 25); meselenin güvenlik gündemine alınmış olmasının, "güvenlikleştirilmesi" sonucunu doğuracağını da vurgulamaktadır.

"Bir dili konuşmak, kurallarla belirlenmiş bir davranış biçimi ile meşgul olmaktır" görüşünün sahibi ve söz edimi teorisinin önemli isimlerinden John R. Searle'ye göre (1999: 16); *"dilsel iletişim tümüyle dilsel eylemleri içerir"*. Searle'nin, "dil" olgusunun özünde sahip olduğu simgeselliğe ve eylemselliğe ilişkin tespitlerinden hareketle; somut delillerin varlığına ihtiyaç duyulmaksızın, bir olgunun -uygun bir biçimde- "tehlikeli" veya "tehditkar" olarak nitelendirilmesinin, o olgunun tehlikeli veya tehditkar olarak algılanmasına yol açabileceğini ileri sürmek mümkündür.

Güvenlikleştirme süreci bu çerçevede ele alındığında; bir "mesele"nin özünde var olduğu ileri sürülen tehlikenin, o tehlikeye ilişkin herhangi bir tecrübe, bilgi ve dolayısı ile de algı sahibi olmayan bir topluluğa kabul ettirilebilmesi için esas itibariyle sözcüklerden ve sözlü iletişimden faydalanılmaktadır. Böylelikle, "tehdit" olarak nitelendirilen ve o andan itibaren de tartışmaların içerisinde bu yeni kimliği ile yer alan "mesele", "gerçek" bir güvenlik tehdidi olarak algılanmaya başlanmaktadır. Bu dönüşümün tamamlanmasının ve tehdidin varlığına ilişkin mutabakatın sağlanmasının ardından güvenlik gündeminde yerini alan "mesele", böylelikle başarılı bir şekilde "güvenlikleştirilmiş" olmaktadır.

Bahse konu güvenlikleştirme sürecini, tehdidin niteliğine ilişkin pek çok faktörün yanı sıra güvenlikleştirme eylemini doğrudan gerçekleştiren veya bu sürece müdahil olan aktörlerin de şekillendirdiklerine dikkati çeken Dunn Cavelty; Buzan ve çalışma arkadaşlarına atfen, güvenlikleştirme süreçlerine ilişkin bir çalışmada, "mesele" ile ilişkili olarak aşağıdaki soruların yanıtlarının alınmasının amaçlandığını ifade etmektedir (Buzan ve diğerleri, 1998: 32'den aktaran Dunn Cavelty, 2008: 25):

- Güvenlikleştirme eylemini kim gerçekleştirir? (Aktör)
- Hangi sorunlar güvenlikleştirilir? (Tehdit Konusu)
- Güvenlikleştirme kim veya ne için gerçekleştirilir? (Referans Nesne)
- Neden güvenlikleştirmeye başvurulur? (Niyet ve Amaçlar)

- Hangi sonuçları elde etmek için güvenlikleştirmeye başvurulur? (Çıktı)

- Hangi şartlar altında güvenlikleştirme gerçekleştirilir? (Yapı)

Bir güvenlik tehdidine ilişkin olarak ortaya çıkan algının, belirlenen politikaların, geliştirilen stratejilerin ve alınan karşı tedbirlerin tam ve doğru olarak analiz edilebilmesi için, yukarıdaki sorulara verilecek cevaplar hayati önemdedir. Söz konusu cevaplar; gerek güvenlikleştirme sürecinde etkili olan faktörlere ve aralarındaki ilişkilere, gerekse de var olduğu kabul edilen "tehdit"in ne kadar "gerçek" olduğuna ilişkin yürütülen araştırmalar için, hem bir başlangıç noktası oluşturmakta, hem de önemli ipuçlarını içermektedir.

Dunn Cavelty'nin de dikkat çektiği üzere (2008: 25); güvenlikleştirme sürecinde etkili olan faktörlerden "aktör" ve "referans nesne"ye büyük önem veren Buzan ve çalışma arkadaşları, "güvenlik" olgusunu da ayırt edici karakteristikleri ve dinamikleri üzerinden beş ayrı sektöre bölerek ele almaktadır. Uluslararası ilişkiler odaklı geleneksel güvenlik değerlendirmelerinden de kaçınılmaz olarak uzaklaşılmasını içeren bu yaklaşım çerçevesinde, "kendilerine özgü etkileşim biçimlerine sahip olan" bahse konu sektörler şöyle sıralanmaktadırlar (Buzan ve diğerleri, 1998: 7):

- Kuvvete dayalı zorlama ilişkilerini içeren, "askeri sektör *(military sector)*",

- Yetki, yönetim biçimi ve onaylama ilişkilerini içeren, "siyasi sektör *(political sector)*",

- Ticaret, üretim ve mali ilişkileri içeren, "ekonomik sektör *(economic sector)*",

- Kollektif kimlik ile ilişkileri içeren, "sosyal sektör *(societal sector)*",

- İnsan faaliyetleri ile gezegenin biyosferi arasındaki ilişkileri içeren, "çevresel sektör *(environmental sector)*".

Bu çerçevede siber güvenlik olgusu; enformasyon teknolojilerinin kazandığı yaygınlık, bu teknolojilere yönelik artan bağımlılık ve ağ merkezli yaşam biçimlerinin hızla benimsenmesi üzerinden ele alındığı zaman görülecektir ki, yukarıda sıralanmış olan sektörlerin tamamında siber tehditlerin yaratılabilmesi mümkündür. Dolayısı ile böyle bir ihtimalin varlığının da, güvenlikleştirme girişimlerini teşvik etmesi kaçınılmazdır.

(2) Paris Okulu

Kopenhag Okulu tarafından özellikle söyleme dayalı olarak geliştirilmiş olan yaklaşım ve tezlerin karşısında ise Paris Okulu yer almaktadır. Güvenlikleştirmeyi bir süreç olarak ele almış olmasına rağmen yöntem kısmına fazlaca eğilmemiş olan Kopenhag Okulu ile karşılaştırıldığında, Paris Okulu daha eylem odaklı bir karaktere sahip görünmektedir.

Kopenhag Okulundan farklı olarak Paris Okuluna göre, güvenlikleştirme sürecinin tek bir aktörün ürünü olmayıp, farklı kapasite ve tezleri olan -güvenlik profesyoneli- aktörlerin çatışmasını ve bu çatışmanın sonuçlarını içerdiğini ifade eden Dunn Cavelty'ye göre (2008: 26-27); sadece hitabete indirgenemeyecek olan böyle bir güvenlikleştirme süreci, söylemin desteklenmesi maksadıyla kaynakların kapsamlı bir seferberliğini de gerektirmektedir. Bu çerçevede güvenlikleştirme süreci içerisinde hayati öneme sahip aktörler olan "güvenlik profesyonelleri"ni üreten ve devletin bürokratik uzantıları olan belirli bazı kurumların, toplumun koruyucusu olma rollerini devamlı olarak yeniden tanımlamak suretiyle, varlıklarını meşrulaştırma ihtiyacı içerisinde olmalarına vurgu yapan Dunn Cavelty (2008: 27); söz konusu meşrulaştırmanın güvenlikleştirme uygulamaları ile yapıldığı kanaatindedir.

Bu çerçevede Dunn Cavelty, Paris Okulu tarafından güvenlikleştirmeye ilişkin olarak yürütülen çalışmalarda yanıt aranılan temel soruları şöyle sıralamaktadır (2008: 27):

- Mücadeleyi kim kazanmıştır?
- Mücadele ne zaman kazanılmıştır?
- Mücadele hangi nedenlerle kazanılmıştır?

Kopenhag Okulu ile karşılaştırıldığında Paris Okulunun, güvenlikleştirilen olgudan ziyade onun benzeri olgular ile girmiş olduğu mücadele sonunda sağlamış olduğu başarıyı kendisine merkez olarak aldığı; dolayısı ile de daha teknik ve yöntem odaklı olduğu ileri sürülebilir. Başka bir ifadeyle, Kopenhag Okulunun "Neden" sorusu ile yaklaştığı bir olguya, Paris Okulu "Nasıl" sorusu ile yaklaşmaktadır.

Güvenlikleştirme teorisine ilişkin olarak yaptığı değerlendirmeler kapsamında siber güvenliğe ilişkin kavramsal ve kuramsal çerçevenin önemini de ortaya koyan bir biçimde, söylem hakimiyeti mücadelesine de dikkat çeken Dunn Cavelty; kullanılan teknik terimler üzerinden sağlanılan dilsel hakimiyetin, taraflar arasındaki söylem mücadelesinin sonucunun belirlenmesinde kritik önemde olduğunu ifade etmektedir (2008: 27).

Bu kapsamda Dunn Cavelty'nin de atıfta bulunduğu M. Townson, -aynı dil ile sınırlı olan- mikro seviyedeki "dilsel hakimiyet *(linguistic dominance)*" mücadelelerinin aşağıda belirtilmiş olan üç mekanizmayı içerdiğini ileri sürmektedir (Townson, 1992: 25-26):

- Belirli bir grubun, amaçlarına hizmet etmek üzere, kendi terminolojisini oluşturmaya çabalarını içeren; "İsimlendirme *(Naming)*",
- Niteliklerine sahip olunduğu ve olumlu anlamlar taşıdığı iddia edilen (demokrasi, özgürlük vb.) bazı terimler ortaya atılırken ve bunların politik rakip tarafından kullanılması reddedilirken, aynı zamanda olumsuz anlamlar ile yüklü (komünist, kapitalist vb.) terimler oluşturulması ve bunların rakip ile ilişkilendirilmesi çabalarını içeren; "Referanslandırma *(Referencing)*",
- Bir kelimenin gerçek anlamına yalnızca belirli bir grubun vakıf olduğu ve rakibin bu gerçek anlamı ya hatalı olarak sunduğu ya da çarpıttığı iddiasını içeren; "Simgeleştirme *(Signifying)*".

Bu perspektiften bakıldığında görülebileceği üzere; güvenlikleştirme süreçleri içerisinde geliştirilen söylemlerde kullanılan sözcük, kavram veya terimlerin gerçek ve teknik anlamlarının ötesinde, onlara yüklenmiş olan örtülü anlam ve amaçları da taşıyabilmeleri mümkündür.

b. Çerçeveleme Teorisi *(Framing Theory)*

Çerçeve analizi, Dunn Cavelty'nin ifade ettiği üzere (2008: 29); güvenlik gündemine girmeyi başaran meselelerin sağladıkları bu başarı ile bilişsel yönleri arasında, meselelerin özel karakteristiklerine vurgu yapan ve kilit aktörler tarafından da faydalanılan "çerçeveler" üzerinden kurulmuş kuvvetli bir bağlantı olduğu tespitine dayanmaktadır.

Bu kapsamda "Çerçeveleme Teorisi *(Framing Theory)*", söyleme dayalı güvenlikleştirme örneklerinden biraz daha farklı olarak, olgu veya olaylara ilişkin içeriğin sunulma biçimi ve istenilen bir sonucu yaratacak şekilde manipüle edilmesi ile çok daha yakında ilişkili görünmektedir. Çizilen resim, anlatılan hikâye ve bunlar üzerinden verilen mesajlar ile bireylerin düşüncelerinin istenilen bir noktaya doğru nasıl yönlendirildiklerini açıklanması kaygısı, söz konusu teorinin "iletişim" odaklı karakterini de ortaya koymaktadır.

Medya stratejilerine ilişkin yaptığı çalışması ile tanınan Ryan'ın "Haber" örneği üzerinden yaptığı tanımlamaya göre (Ryan, 1991: 53); "Çerçeveleme", anlatanlar ve dinleyenler için anlam ifade edecek bir hikaye oluşturmak üzere, bilgi parçalarının seçildiği ve düzenlendiği bir süreci ifade eder. Ryan'ın da çalışmasında özellikle dikkat çektiği gibi; *"framing"* kelimesi, ilki "bir şeyin çevresinin/sınırlarının tespit edilmesi", ikincisi ise "bilinçli bir şekilde aldatmak" olmak üzere ikili bir anlam ve kullanıma sahiptir.

Güvenlikleştirme perspektifinden bakıldığı zaman ise "Çerçeveleme"yi, belirli ajanların neyin risk veya tehdit olarak kabul

edileceğine, bu tehdite nasıl bir tepki verileceğine ve bu tepkinin verilmesinden kimin sorumlu olacağına ilişkin yorumlayıcı şemalar geliştirdikleri bir süreç olarak betimleyen Dunn Cavelty (2008: 29-30); çerçeveleme teorisinin yanıt aradığı soruları şöyle sıralamaktadır:

- Çerçeveler sosyal eylemleri nasıl etkilerler?
- Hangi çerçeveler hangi gerekçeler için özellikle başarılıdır?
- Çerçeveler nasıl değiştirilebilirler?

Çerçeveleme süreçlerinin merkezinde yer alan "çerçeveler"in güvenlikleştirme süreçleri içerisindeki rollerinin ortaya konulması noktasında ise; kamuoyunun sahip olduğu dünya görüşlerinin ve benimsediği varsayımların üzerine eğilen "stratejik çerçeve analizi" çalışmaları özel bir öneme sahiptir. Bu perspektife dayalı olarak, stratejik çerçeve analizi alanında çalışmalar yürütmekte olan ABD merkezli Frameworks Enstitüsüne göre (Frameworks [web], 2012); özellikle haber kuşaklarında yer alan ve bir araya geldikleri zaman bireylerin zihinlerindeki "beklenti yapıları *(structure of expectation)*" ile edinilmekte olan yeni bilgiler arasındaki bağlantının kurulmasını sağlayan "unsurlar" şöyle sıralanabilmektedir:

"* Metaforlar *(Metaphors)*
* Haberciler *(Messengers)*
* Görseller *(Visuals)*
* Mesajlar *(Messages)*
* Hikayeler *(Stories)*
* Sayılar *(Numbers)*
* Bağlam *(Context)*"

Bu kapsamda bireyler üzerinde istenilen yönlendirmenin sağlanılması noktasında, yukarıdaki unsurları içeren "çerçeveler"in çok daha başarılı olması beklenilebilir.

Güvenlikleştirme kapsamında değerlendirilebilecek olan ve bireyleri eylemde bulunmaya yönlendirmeyi amaçlayan, politik nitelikli çerçeveleme biçimlerini ise; Snow ve Benford aşağıdaki başlıklar altında sınıflandırmaktadırlar (Snow ve Benford, 1988: 199-202'den aktaran Dunn Cavelty, 2008: 30; Johnston ve Noakes, 2005: 5-6):

- Potansiyel taraftarlara yönelik olarak problemin, olayların ve sorumluların yeniden tanımlanmasını içeren; "Teşhis Koyucu Çerçeveleme *(Diagnostic Framing)*",
- Çözümleri ve bu çözümlerin başarılı olabilmesi için gerekli olan strateji, taktik ve hedefleri içeren; "Yol Gösterici Çerçeveleme *(Prognostic Framing)*",
- Kişilerin müşterek bir harekete katılmaları ve eyleme geçmeleri için gerekli nedenleri içeren; "Teşvik Edici Çerçeveleme *(Motivational Framing)*".

c. Gündem Belirleme Teorisi *(Agenda-Setting Theory)*

Belirli bazı meseleler siyasal öneme sahiplerken diğerlerinin siyaseten böyle bir öneme sahip olmamalarının nedenlerinin -ABD'li siyaset bilimci- John W. Kingdon tarafından geliştirilmiş olan "Gündem Belirleme Teorisi *(Agenda-Setting Theory)*" kapsamında ortaya konulmuş olduğunu ifade eden Dunn Cavelty'ye göre (2008: 33);

> "Buna ek olarak, gündem belirleme -teorisi-; meselelerin 'nasıl' ve 'ne zaman' siyasal gündemin birer parçası haline geldiklerinin yanıtlarını verirken, yaşanılan sürece ve gerekli koşullara ilişkin olarak da ayrıntılı bir açıklama sağlar."

Eustis ise Kingdon'un yaklaşımının, her biri birbirinden bağımsız olan "mesele *(problem)*", "siyasalar *(policies)*" ve "siyaset *(politics)*" akımları arasında varolan bir etkileşime dayandığına dikkati çekmektedir. Eustis'in Kingdon'a atfen vurguladığı üzere (Kingdon 1995: 166'dan aktaran Eustis, 2000: 3); genellikle kritik zamanlarda ortaya çıkan söz

konusu etkileşim, değişimin yaratılabilmesini ve meselelerin politik gündeme alınmalarını sağlacak olan bir "fırsat penceresi *(window of opportunity)*"nin açılmasını sağlamaktadır.

Esas itibari ile ABD siyasal sistemi içerisindeki kamu politikası oluşturma süreçlerini açıklamak üzere inşa edilmiş olan bu teorinin ve merkezinde yer alan "akım"ların kapsamının daha kolay anlaşılabilmesi için genelleştirilmeleri uygun olabilir. Böyle bir genelleştirmenin sonucunda, mevcut olgu, olay ve koşullara ilişkin olarak; "mesele" akımının -mikro seviyede- daha bireysel veya kurumsal yaklaşımları, "siyasalar" akımının -orta seviyede- hükümet merkezli ve profesyonellik ağırlıklı yaklaşımları, "siyaset" akımının ise -makro seviyede- daha kitlesel ve ülkesel politik yaklaşımları temsil ettiğini düşünmek yanlış olmayacaktır.

Harekete geçirici bir olgu veya olay karşısında her üç akımın da bir araya gelmesine bağlı olarak açılan "fırsat penceresi" üzerinden mevcut algı, anlayış ve politikalardaki değişikliklerin tetiklendiğini belirten Thomas A. Birkland (2010: 297-298); bu duruma örnek olarak, uçak kazaları veya terörist saldırılar sonrasında açılan fırsat pencerelerinin yönlendirmesi ile düzenleyici kurumlar tarafından daha sıkı emniyet ve güvenlik standartlarının benimsenmesi durumlarını göstermektedir.

Dunn Cavelty'nin de dikkat çektiği üzere; meseleler tanımlanmadıkça ne tehdidin çerçevelenmesi, ne de güvenlikleştirme sürecinin başlatılabilmesi mümkündür. Bu nedenle, belirli koşulların nasıl ve ne zaman "mesele" olarak tanımlandıkları özellikle güvenlikleştirme süreçleri açısından oldukça büyük bir önem taşımaktadır (Dunn Cavelty, 2008: 34). Bu çerçevede Dunn Cavelty, koşulların mesele halini aldıklarının resmi görevliler tarafından "ne zaman" ve "nasıl" fark edildiğine ilişkin olarak -Kingdon'a atfen- şu üç faktöre dikkat çekmektedir (Kingdon, 2003: 90-115'den aktaran Dunn Cavelty, 2008: 34):

> "* İstatistik, özel çalışmalar veya bütçe rakamları biçiminde somutlaşarak ortada bir problem olduğunu açık bir biçimde gösteren ve az ya da çok sistemik mahiyette olan; 'Gösterge *(Indicator)*',

* Kriz, felaket veya bir politika yapıcının kişisel tecrübesi olarak ortaya çıkabilen; 'Odaklayıcı Olaylar *(Focusing Events)*'.

* Sistematik izleme ve değerlendirme çalışmaları, şikayetler veya rutin sosyal çalışmalar biçiminde, olayların normal akışının bir parçası olarak ortaya çıkan geri besleme mesajlarına dayanan; 'Resmi ve Gayrı Resmi Geri Besleme *(Formal and Informal Feedback)*'."

Odaklayıcı olaylar haricinde, akademik ve bürokratik bir anlayışın hakimiyetini de örtülü olarak tespit eden bu yaklaşım çerçevesinde; normal şartlar altında, her üç akımın da bir araya getirilerek bir fırsat penceresinin açılmasını sağlayacak sinerjinin ortaya çıkartılması pek de mümkün görünmemektedir. Dolayısı ile bu kapsamda "Gündem Belirleme Teorisi"; özellikle güvenlik alanındaki belirli koşulların "mesele" olarak tanımlanmalarının niçin genellikle odaklayıcı olaylara bağlı olduğunun ve kaçınılmaz bir biçimde de "tepkisel" karakter taşıdığının açıklanması noktasında da oldukça önemlidir.

Siber tehditlere ilişkin algıyı ve güvenlik politikalarını, yukarıda yer verilmiş olan kuramsal yaklaşımları içine alan "karma" bir anlayış ile ele almayı tercih eden Dunn Cavelty'ye göre (2008: 38); *"tehdit çerçeveleri (threat frames), kilit aktörlerin değerlerinin, kaynaklarının ve inançlarının bir sonucu olarak ortaya çıkmaktadırlar.*". Bu kapsamda Dunn Cavelty, bir tehdit çerçevesinin şu üç ana parçadan meydana geldiğini ileri sürmektedir (2008: 38-39):

"1) bir 'teşhis koyucu çerçeve *(diagnostic frame)*', tehdidin kaynağı ve yöneldiği nesne üzerinden ifade edilen; 2) bir 'yol gösterici çerçeve *(prognostic frame)*', çözümlere, stratejilere, taktiklere ve amaçlara ilişkin teklifleri içeren; 3) bir 'teşvik edici çerçeve *(motivational frame)*', destekçilerin harekete geçirilmesine yönelik."

Dunn Cavelty, çalışmasının kuramsal çerçeveye ilişkin kısmının sonunda, siber tehditler ile ilişkili güvenlikleştirme veya çerçeveleme girişimlerini konu alan söylem analizi çalışmalarında başvurulabilecek anahtar kavramları ise şöyle sıralamaktadır (2008: 38):

- Bilgisayar Tabanlı Saldırı *(Computer-based Attack)*
- Bilgisayar İhlali *(Computer Intrusion)*

- Kritik Enformasyon Altyapıları *(Critical Information Infrastructures)*
- Kritik Altyapılar *(Critical Infrastructures)*
- Siber Saldırı *(Cyber-Attack)*
- Siber Güvenlik *(Cyber-Security)*
- Siber Terörizm *(Cyber-Terrorism)*
- Siber Tehdit *(Cyber Threat)*
- Siber Güvenlik Açığı *(Cyber-Vulnerability)*
- Elektronik Pearl Harbor *(Electronic Pearl Harbor)*
- Enformasyon Operasyonları *(Information Operations)*
- Enformasyon Savaşı *(Information Warfare)*
- Ulusal Güvenlik *(National Security)*
- Enformasyon Altyapısındaki Zafiyetler *(Vulnerabilities of Information Infrastructure)*

Tehdit algılarının ve güvenlik politikalarının oluşturulması kapsamında, yukarıda yer verilmiş olan kuramsal yaklaşımların aktöre, aktörün tercihlerine ve bireylerin yönlendirilmelerine yaptıkları vurgu gözönünde bulundurulduğunda; Dunn Cavelty tarafından yukarıda sıralamış olan kavramların her birinin, en somut biçimde ortaya çıktıkları anlarda ve olaylarda dahi, her bir aktör tarafından kendi amaçları ve tecrübeleri doğrultusunda farklı biçimlerde tanımlanabilmelerinin ve çerçevelendirilebilmelerinin mümkün olduğu açıktır. Bu çerçevede, özellikle güvenlik çalışmaları alanında faaliyet gösteren, etik ve bilimsel nesnellik kaygılarına sahip olan araştırmacıların; hem ele aldıkları kavramlara ve onların kapsamlarına ilişkin olarak mümkün olduğunca geniş ve çok taraflı bir yaklaşımı benimsemeleri, hem de mutlak doğruluk

ve kesinlik iddialarından uzak kalmaları ahlaki ve bilimsel bir zorunluluk halini almaktadır.

İKİNCİ BÖLÜM

ABD'DEKİ İSTİHBARAT VE GÜVENLİK YAPILANMASININ ASİMETRİK TEHDİT VE SİBER GÜVENLİK BAĞLAMINDA GEÇİRDİĞİ DEĞİŞİM

1. İSTİHBARAT VE GÜVENLİK AYGITI

Çalışmanın bu kısmında, gerek konu ve kapsam dışına taşmamak, gerekse de çalışmanın hacmini daha da fazla arttırmamak maksadıyla; ABD'deki mevcut ulusal güvenlik yapılanmasının ve ilişkiler sisteminin bir bütün olarak, 11 Eylül Saldırıları sonrası dönemde asimetrik savaş bağlamındaki terörle -savaş- mücadele süreci içerisindeki rolüne ve geçirdiği değişime yer verilecektir. Bu çerçevede ABD'deki istihbarat ve güvenlik yapılanmasına ilişkin bilgilendirme asimetrik tehdit ve siber güvenlik bağlamı ile sınırlandırılmıştır.

"Devlet" ile "Güvenlik" arasındaki ilişkinin "Ulusal Güvenlik" kavramı üzerinden ortaya konulduğunu ifade eden Dobrowolsky ve çalışma arkadaşları (2009: 15-19); 11 Eylül Saldırıları sonrasında ABD'nin güvenlikleştirme yaklaşımında ortaya çıkan değişimi ise, biraz da eleştirel bir biçimde, "benzeri görülmemiş" olarak nitelemektedirler.

Terörle savaşmaya odaklanan ve asimetrik tehdit algısının öne çıktığı bu yeni ulusal güvenlik anlayışı; sadece analiz, politika ve strateji geliştirme ya da operasyon alanlarında değil, doktrin ve örgütlenme alanlarında da oldukça etkili olmuştur. Bu kapsamda en kritik değişikliklerin; terörle mücadelede silahlı kuvvetlerin rolü ile istihbarat ve güvenlik aygıtının örgütsel yapısına ilişkin olarak yaşandığını ileri sürmek mümkündür.

Terörizme ilişkin olarak sahip olunan algının, mücadele politikaları ve stratejileri üzerindeki etkisini vurgulayan Yalda ve White'a göre (2009: 64);

> "Terörist çatışmaların doğasına ilişkin tanımsal tartışmaların özünde, terörizmin esasen askeri ya da polisiye bir sorun olma niteliğine bakılmaksızın, bir tepki ve sorumluluk meselesi yer alır. Askeri bir problem olarak kabul edilmesi durumunda terörizm, ilan edilmemiş veya yarı ilan edilmiş bir savaş olarak ele alınacaktır. Ceza hukuku gözlüğü ile bakıldığında ise; mahkemelerin ilgi alanına giren, sürece bağlı olarak sivil haklar ve insan haklarının korunmasını da içeren, polisiye bir sorun haline gelecektir."

Nitekim yetki ve sorumluluğa ilişkin olarak böyle bir tanım sorununun yok sayılması, bu sorunun çözüme kavuşturulmasının daha "rahat" dönemlere bırakılması ya da mücadele stratejisinde "karma" bir çözümün tercih edilmesi gibi nedenlerle, terörle mücadelede silahlı kuvvetlerin ve kolluk kuvvetlerinin sıklıkla bir arada kullanıldıkları görülmektedir.

Siyasal şiddet ve terörizm alanındaki çalışmaları ile tanınan Paul Wilkinson, terörle mücadelenin karakteri üzerinde de çeşitli etkilere sahip olan bu durumu, şöyle özetlemektedir (1996: 1):

> "Terörle mücadeleye yönelik sürekli arayış içerisinde, hem iç hem de dış tehditler bağlamında, demokratik toplumların askeri kuvvetlerinin rolü de değerlendirilmektedir. Askeri kuvvetlerin müdahil olması, hukukun üstünlüğü ve demokratik süreçler çerçevesinde terörizmi yenmek için mutlak bir kararlılık sağlarken, oldukça hassas bir durum da yaratmaktadır. Kovuşturulmak ve mahkûm edilmek üzere teröristlerin adalet önüne çıkartılmalarına yönelik yoğun çaba bazen sert tedbirlerin alınmasını gerektirebilmektedir."

Bu çerçevede, yasadışı eylemlerde bulunma ve bu kapsamda şiddet uygulama yolunu seçmiş olan terörist örgütlenmeler karşısında, ait oldukları ülkenin neredeyse tüm kaynaklarına başvurabilecek, organize, disiplinli, kararlı ve hepsinden önemlisi kırsal alanlar başta olmak üzere çok değişik ortamlarda teknik ve taktik olarak çok farklı silahlı çatışma imkan ve kabiliyetlerine sahip olan silahlı kuvvetlerin; özellikle, terör

örgütlerinin şiddet eylemlerine yönelik kapasitelerinin azaltılmasında oldukça etkili birer araç olacakları açıktır.

Yetki ve sorumluluk bağlamında ortaya çıkan bahse konu tanım sorununun yanı sıra, terörle mücadele stratejilerinin askeri bir boyut kazanmalarında ve zaman içerisinde de bu boyutun ağırlığının artmasında etkili olan -birbirleri ile de yakından ilişkili- bazı olguların varlığına da dikkat çekmek gerekir. Bu olgulardan ilki çatışmanın biçim ve niteliğine ilişkin iken, diğeri çatışma ile bağlantılı kavramsal çerçeveye ilişkindir.

Çalışmanın önceki kısmında da dikkat çekildiği üzere; ekonomik ve sosyal gelişmişlik seviyesinin arttığı -ya da yüsek olduğu- toplumlar, gerilla savaşının yürütülmesi için uygun zemini ya da dokuyu sağlayamamaktadırlar. Özellikle siyasal şiddet perspektifinden ele alındığında; bireysel hayat standartlarını yükseltme kaygısı içerisinde olan nüfusunun büyük çoğunluğunun kentlerde yaşadığı bir ülkenin topraklarında, nufüs yoğunluğunun tek haneli rakamlara yaklaştığı yerlerde siyasal içerikli şiddet eylemleri yapılması politik dinamiklerle açıklanmaya çalışılan terörizm olgusu için fazla anlamlı değildir. Dolayısı ile bu gibi ülkelerde, şehirlerde bir araya gelerek siyaseten görmezden gelinemeyecek bir güce ulaşan ve nüfusun büyük bir kısmını oluşturan kitlelerin azınlık tarafından iradelerinin kırılarak siyaseten yönlendirilebilmeleri için gerekli baskı -şiddet- unsurunu sağlayan olgu ve asli tehdit kaynağı "terörizm" adı altında ortaya çıkmaktadır. Başka bir deyişle siyasal şiddet, gerçek anlamda etkili olabilmek için –politik etkiye sahip olan- kitleleri takip etmektedir. Bu çerçevede terörizmin, tümüyle iç dinamiklere dayalı bir dizi politik şiddet eyleminden ziyade, o ülkenin istikrarsızlaştırılmasını amaçlayan ve dış destekli olarak yürütülen bir "vekaleten savaş *(proxy war)*" niteliği kazanması durumunda ise; örtülü olarak askeri nitelik taşıyan böyle bir ulusal güvenlik tehdidi karşısında, yalnızca kolluk kuvvetlerine dayanılarak başarıya ulaştırılamayacağı açık olan terörle mücadele politikaları kapsamında silahlı kuvvetlerin görevlendirilmesi de kaçınılmaz bir hal almaktadır.

Silahlı kuvvetlerin ülke içi kullanımını sınırlandıran -ABD'deki *Posse Comitatus Act* benzeri- kanunlara sahip olan ülkelerde terörle

mücadele kapsamında silahlı kuvvetlerden ya da askeri kapasiteden meşru bir şekilde faydalanılabilmesi için, özellikle güvenlikleştirme süreçleri çerçevesinde "asimetrik savaş" benzeri kavramlara başvurulması kaçınılmazdır. Başka bir deyişle; devasa boyutlardaki bir -askeri- güvenlik kapasitesinin terörle mücadele kapsamında yok sayılarak atıl durumda bırakılmaması maksadıyla, güvenlikleştirme süreci çerçevesinde terörizm tehdidine askeri bir nitelik kazandırılması zorunludur. Dolayısı ile, "terör" olaylarının şiddet tabanlı polisiye vakalar olmaktan çıkarak birer ulusal güvenlik tehdidine dönüştürüldükleri noktada; terörle mücadelede silahlı kuvvetlerin kullanılmasını öngören politikalar ve buna dayalı stratejiler de, hem yasallık, hem de siyasal meşruiyet kazanmaktadır.

Nitekim El Kaide Örgütü ile Afganistan'daki Taliban Yönetimi arasındaki ilişkilere dair, 11 Eylül Saldırıları sonrasında yapılan tartışmalarda da "melez savaş" ve "vekaleten savaş" konseptlerine yer verildiği görülmektedir. Bu kapsamda El Kaide Terör Örgütü eylemlerinin ABD'ye yönelik olarak melez savaş konsepti ile yürütülen küresel bir vekaleten savaş olarak nitelendirilip nitelendirilemeyeceği hususu, 11 Eylül Saldırıları sonrası dönemde yaşanılan pek çok şeyin anlaşılması için mutlaka sorulması gereken hayati bir sorudur.

Elbette ki bu noktada, terörizm ile kent olgusu arasında yukarıda kurulmuş olan ilişkinin geçerliliğine ilişkin bazı sorularla da karşılaşılabilmesi mümkündür. Fidel Castro'nun *"Şehir, devrimcilerin ve olanakların mezarlığıdır."* sözüne gerilla savaşı kuramcılarının çoğunluğunun katıldığını ifade eden Robert Moss'a göre (2010: 475);

> "Clausewitz'in zamanından bu yana, genel olarak kabul edilmiştir ki; gerilla savaşı ancak, asilerin geniş bir şekilde yayılabilecekleri kırsal alanlar üzerinde ve üs olarak kullanılabilecek düzensiz ve zorlu araziye hakim olmak suretiyle yürütülebilir."

Bununla birlikte terörizmi "kent militanlığı *(urban militancy)*"nın pek çok biçiminden biri olarak nitelendiren Moss (2010: 479); amaç açısından net bir biçimde olmasa da, yöntem ve örgütlenme açısından terörizm ile gerilla savaşını birbirlerinden şöyle ayırmaktadır:

"Ayaklanmaların, siyasal grevlerin, öğrenci gösterilerinin ve getto isyanlarının aksine, terörizm bir azınlık tekniğidir ve kent şartları altında güvenliği sağlama ihtiyacı oldukça standart bir örgütlenme biçimini dayatır: terörist grupların üyeleri, her birinde bir bağlantı elemanı bulunan ve üç ila beş kişiden oluşan "hücre *(cell)*"lere veya "ateş grupları *(firing groups)*"na bölünürler. Bu durum ihanet veya polis sızması ihtimalini net bir biçimde sınırlandırmakla birlikte, aynı zamanda "siyasal kışkırtma *(political agitation)*" ihtimalini de sınırlandırır.

Terörist politik bir araca sahipken; kent gerillası devrim için bir stratejiye sahiptir."

Bu çerçevede kritik önemde olan husus, daha önceden de dikkat çekilmiş olduğu üzere, yaşanılan çatışmanın tümüyle iç dinamiklere dayalı bir dizi politik şiddet eylemi olarak nitelendirilip nitelendirilemeyeceğidir.

Temel insan hakları belgelerinden bir tanesini oluşturan ABD Anayasasının ve ABD Silahlı Kuvvetlerinin kolluk görevlerinde kullanılmalarını yasaklayan *Posse Comitatus Act* düzenlemesinin varlığı gözönünde bulundurulduğunda; ABD'de yalnızca kolluk kuvvetleri merkezli bir yaklaşımla geliştirilmek zorunda kalınacak "terörle mücadele" politikaları kapsamında, sahip olunan devasa boyutlardaki askeri kapasitenin atıl durumda kalmasının kaçınılmaz olduğu açıktır. Dolayısı ile dördüncü nesil savaş, melez savaş, asimetrik savaş ya da siber savaş kavramları ile ilişkilendirilmek suretiyle terörizme askeri bir nitelik kazandırılması, özellikle şehirlerde ve siber uzayda ulusal güvenliği sağlamak üzere ABD askeri kapasitesinin serbest bırakılması anlamına gelmektedir.

Nitekim benzeri bir şekilde, 11 Eylül Saldırıları sonrasında "güvenlik -ve savaş- üzerinden yönetme" anlayışına kayışın, terörizmi asimetrik savaş olarak yeniden tanımladığını ve bakış açısındaki bu değişikliğin hem sivil, hem de askeri açıdan ulusal ve küresel uygulamaları etkilediğini ifade eden Yalda ve White (2009: 64); bu süreçte insan hakları ve temel özgürlüklerin de yeniden tanımlandıklarına dikkati çekmektedirler.

Yalda ve White tarafından yapılmış olan yukarıdaki tespit, eleştirel yaklaşımın basit bir yansıması olmanın ötesindedir. Zira bu noktada asimetrik savaş kavramı, taraflar arasındaki dengesizliği vurgulayan teknik

kimliğinden sıyrılarak hem "teröre karşı savaş" isimlendirmesini, hem de bu savaş kapsamında karşı gücün üyelerine yönelik olağanüstü uygulamaları siyaseten ve hukuken meşrulaştırmaktadır. Karşı gücün üyelerinin sivil birer şahıs olarak sahip oldukları -ve belki de, çatışma ortamında onlara avantaj sağlayabilecek olan- kişi haklarının ve sivil özgürlüklerin ciddi bir biçimde sınırlandırılabilmesi için gerekli zemini de oluşturan böyle bir kavramsal yaklaşım; meşruiyet kazandırdığı yeni güvenlik tedbirleri ve güvenlik politikaları üzerinden, tehdit kaynaklarını olduğu kadar bir bütün olarak kişi hak ve hürriyetlerini de etkilemektedir.

Bu noktada Yalda ve White'ın "tepki ve sorumluluk" yaklaşımına geri dönüldüğünde; terörizme verilecek tepkinin ve derecesinin ne olduğu ile bu tepkinin verilmesinin kimin sorumluluğunda olacağına ilişkin yapılacak tespit ve tercihlerin, terörle mücadele politikalarının ve stratejilerinin karakteri üzerinde belirleyici nitelikte olması kaçınılmazdır.

Bir bütün olarak değerlendirildiklerinde, güvenlik politikalarına ilişkin olarak yukarıda yer verilmiş olan tespitlerin işaret ettikleri asıl önemli husus -ve belki de örtülü kaygı-; silahlı kuvvetlerin veya kolluk kuvvetlerinin tek başlarına ya da karma bir biçimde terörle mücadelede yer almaları durumundan ziyade, kişi hak ve hürrriyetlerine yönelik baskıların ve haksız uygulamaların ortaya çıkması ihtimalidir. Bu kapsamda savunma ve güvenlik bilimlerinin varlığının reddedilemeyeceği günümüzde; ulusal güvenliğe yönelik yarattığı tehdit yadsınamayacak olan "terörizm" olgusu ile mücadelede atıl durumda kalabilecek olan askeri kapasitenin de -gerekli nesnelliğin ve bilimselliğin sağlanmış olması şartı ile- kullanıma sunulmuş olması takdir edilmesi gereken ve optimal bir davranış olacaktır. Elbette ki bu çerçevede unutulmaması gereken en önemli husus; sosyal bir gerçekliğe sahip olan her olayın, olgunun, örgütün, toplumun, ülkenin ve hatta dönemin kendisine özgü nitelikleri olduğudur. Farklı olanlar arasında yapılacak benzetmeler ve genellemeler anlaşılırlığı arttırırlarken, indirgemeci bir yaklaşıma yol açmak suretiyle de gerçeklikten uzaklaşılmasına zemin hazırlayabileceklerdir.

ABD'nin terörle mücadele stratejilerinin askeri bir karakter kazanmaya başlamasına paralel olarak ortaya çıkan diğer bir eğilim ise;

11 Eylül Saldırıları öncesi dönemdeki tehdit algısına göre yapılandırılmış olan "yaşlı" kurumların örgütsel yapılarında, göreceli olarak güç kaybına yol açacak biçimde, değişikliklere gidilmesi ve "yeni" kurumların oluşturulmasıdır. Çoğunlukla 11 Eylül Saldırılarının tahmin edilmesindeki ve önlenmesindeki başarısızlıkların bir bedeli olarak değerlendirilen bu durum, ABD'deki istihbarat ve güvenlik yapılanması üzerinde oldukça büyük bir etki yaratmıştır.

Bu çerçevede Priest ve Arkin'in de dikkat çektiği üzere (2011: 86); 2001 yılının son üç ayında, aralarında İç Güvenlik Bakanlığının çekirdeğini teşkil eden birimin de bulunduğu, 21 yeni örgüt kurulmuştur. Örgütlenmedeki bu ivmelenme ile; 2002 yılında 34, 2003 yılında 39, 2004 yılında 30, 2005 yılında 34, 2006 yılında 27, 2007-2009 arasındaki dönemde ise her yıl 24 veya daha fazla yeni örgüt oluşturulmuştur. Örgütlenme odaklı bahse konu eğilimin ulaştığı son noktayı Priest ve Arkin şöyle ortaya koymaktadır (2011: 86):

> "Arkin, iki yıllık bir araştırmanın sonunda ağzı açık kalmış bir biçimde ortaya çıktı: ABD çapındaki en az 17000 noktada terörle mücadele, iç güvenlik ve istihbarat ile ilişkili programlarla ilgili -tümü "Çok Gizli" gizlilik seviyesinde faaliyet gösteren- 1074 adet federal hükümet örgütü ve yaklaşık iki bin özel şirket bulunmaktaydı."

ABD'deki istihbarat ve güvenlik aygıtına yönelik söz konusu yeniden yapılandırma ve güçlendirme eğiliminin dikkat çekici boyutlara ulaştığı bu noktada, Anthony Giddens'in *"İstesek de istemesek de, totaliter iktidara doğru eğilim endüstrileşmiş savaş gibi çağımızın farklı bir özelliğidir"* tespiti (2005: 401) -göreceli ve kısmen de olsa- geçerlilik kazanmaktadır. Zira Giddens'e göre (2005: 393-394); "Bilgi kodlanması, halkın faaliyetlerinin belgelenmesi" ve "faaliyetlerin gözlemlenmesi, yoğunlaşmış polislik" üzerinden "izlemeye odaklanılması" totaliter yönetimin unsurları arasındadır.

11 Eylül Saldırıları sonrasında ABD'de kabul edilen yasal düzenlemeler ve güvenlik aygıtının güçlendirilmesi eğilimi bu çerçevede ele alındığında; yeni oluşturulmuş, yetenek ve kapasitesi hali hazırda sorgulanmakta olan yaygın ve derin nitelikteki bu yapılanmanın ilerideki

dönemlerde tam kapasite ile çalışabilmesi durumunda, ABD'nin terörle mücadele üzerinden istihbarata dayalı olarak yönetilen bir "gözetleme toplumu" haline gelmesi şaşırtıcı olmayacaktır.

"Top Secret America" isimli çalışmalarında, 11 Eylül Saldırıları sonrasında oluşturulan yeni güvenlik mimarisini nicelik açısından olduğu kadar nitelik ve yeterlilik açısından da tartışmaya açan Priest ve Arkin'e göre (2011: 54);

> "11 Eylül Saldırılarından sekiz yıl sonra göreve gelen Başkan Obama, Saldırılara tepki olarak, aslında ulusal güvenlik kurumları arasında halen kendi rollerini bulamamış durumdaki en büyük iki bürokrasinin -Ulusal İstihbarat Direktörü Ofisi ve İç Güvenlik Bakanlığı- yaratıldığını keşfedecekti. Pek çok kişi, özellikle ulusal güvenlik amatörleri tarafından doldurulduğuna ve geçmişteki maaşlarının iki katına şimdi yüklenici[11] olarak hizmet eden eski federal çalışanlara dayandığına inandıkları İç Güvenlik Bakanlığı hususunda hayal kırıklığına uğramıştı. İstihbarat teşkilatlarının özel firmalar lehine tecrübe kaybetmeleri sorunu o kadar ciddi idi ki; CIA Başkanı Michael Hayden tarafından, özel sektöre geçmek üzere teşkilattan ayrılan herhangi bir çalışanın, yüklenici olarak teşkilata dönmesi on iki ay süreyle yasaklamıştı. '*Bir üretme çiftliği sistemi haline gelmemizi istemiyordum*' dese de, sorun devam etmişti."

Nicelik ve nitelik açısından ortaya çıkan bu dikkat çekici durumun yanı sıra söz konusu yeniden yapılanma eğiliminin bazı politik yansımaları da olabileceği değerlendirilmektedir. Lois M. Davis ve çalışma arkadaşları tarafından 2010 yılında RAND için hazırlanmış olan bir raporda, Chalk ve Rosenau'ya atfen ifade edildiği üzere (2004: 19'dan aktaran Davis ve diğerleri, 2010: 2); *"Washington'un 11 Eylül Saldırıları sonrasındaki iç istihbarat mimarisinin makyajı federal hükümet merkezli bir yaklaşımı yansıtmaya devam etmektedir."*. Aynı rapora göre (Davis ve diğerleri, 2010: 2);

> "FBI gibi federal kurumların yerel yönetimler ile istihbarat paylaşımında isteksiz oldukları hususu yaygın bir eleştiridir. Önceleri federal istihbarat kurumları, eyalet ve yerel kolluk kuvvetlerince sağlanan terörizm ile bağlantılı bilgiler hakkında az da olsa şüphecilerdi."

[11] Metinde kullanılan orijinal ifade, sözleşme karşılığı hizmet veren kişi veya firmaları karşılayan ve "müteahhit" ya da "yüklenici" anlamlarına gelebilen, "contractor"dur. İncelenmekte olan metin ile uyumlu olması maksadıyla, "yüklenici" olarak çevrilmiştir.

Federal bir yönetim yapısına sahip olan ABD'de 11 Eylül Saldırıları sonrasında yürürlüğe konulmuş olan terörle mücadele odaklı yasaların iç güvenlik ve istihbarat konularında federal kurumlara tanıdıkları yetkiler gözönünde bulundurulduğunda; enformasyon ve istihbarat akışının, karşılıklı olmaktan ziyade yerelden merkeze doğru ve tek yönlü olduğuna dair eleştiriler şaşırtıcı gelmemektedir.

Elbette ki, "eski" yapının sahip olduğu kazanımlar ve yetkiler üzerine, yeni tehdit algılamalarının ve güvenlik politikalarının sağladığı yetki, kaynak ve avantajların eklenmesi ile ortaya çıkan bu "yeni" güvenlik yapısının verimli bir hale gelebilmesi için, belirli bir sürenin geçmesi gerektiği açıktır. Ancak ne kadar kusursuz olduğu düşünülürse düşünülsün verimlilik üzerinden bir değerlendirmeye tabi tutulan her güvenlik yapılanması, kaçınılmaz olarak bir paradoks ile karşı karşıya kalmaktadır. Görevini tam olarak yerine getirerek güvenlik tehdidinin gerçekleşmesini engelleyen bir güvenlik yapılanması, ortada somutlaşmış bir tehlike var olmaması nedeniyle muhtemelen işlevsiz olmakla va kaynakları boşa harcamakla suçlanırken; aralıksız bir biçimde oldukça kritik güvenlik tehditlerini bertaraf eden bir güvenlik yapılanması ise, mevcut tehlikeleri etkili ve mutlak bir biçimde ortadan kaldıramadığı için verimsiz ve başarısız olmakla itham edilebilecektir.

Bugünkü hukuksal ve siyasal çerçevesi içerisinde "İstihbarat Topluluğu *(Intelligence Community)*" olarak isimlendirilen ABD'deki istihbarat ve güvenlik aygıtı, Lerner'in de ifade ettiği üzere (2004b: 202); birbirlerinden oldukça farklı seviye ve yapıdaki istihbarat ve güvenlik örgütlenmelerini merkezi olmayan bir şekilde bir araya getirmekte olup, müstakil veya bütünleşik bir varlığa sahip değildir.

11 Eylül Saldırıları sonrası dönemde, "2004 tarihli İstihbarat Reformu ve Terörizmin Önlenmesi Yasası *(Intelligence Reform and Terrorism Prevention Act of 2004)*" kapsamında oluşturulmuş bir makam olan Ulusal İstihbarat Direktörü (DNI), İstihbarat Topluluğunun yönetilmesi ve ulusal istihbaratın koordinasyonu ile görevlendirilmiştir. DNI öncesi dönemde İstihbarat Topluluğunun yönetilmesi sorumluluğu ise, aynı zamanda CIA Başkanı da olan Merkezi İstihbarat Direktörü (DCI)'ne aittir.

Bu çerçevede, 11 Eylül Saldırıları sonrası dönemde istihbarat ve güvenlik aygıtı içerisinde CIA'nın kontrol ve rolünün gerilediğinin ileri sürülmesi mümkündür.

İstihbarat Topluluğu günümüz itibariyle, aşağıda yer alan 17 kurumdan meydana gelmektedir (IC [web], 2012):

- Hava Kuvvetleri İstihbaratı
- Kara Kuvvetleri İstihbaratı
- Merkezi Haberalma Teşkilatı (CIA)
- Sahil Güvenlik İstihbaratı
- Savunma İstihbarat Teşkilatı (DIA)
- Enerji Bakanlığı, İstihbarat ve Karşı İstihbarat Ofisi
- İç Güvenlik Bakanlığı, İstihbarat ve Analiz Ofisi
- Dış İşleri Bakanlığı, İstihbarat ve Araştırma Bürosu
- Hazine Bakanlığı, İstihbarat ve Analiz Ofisi
- Uyuşturucuyla Mücadele Teşkilatı (DEA)
- Federal Soruşturma Bürosu (FBI)
- Deniz Piyadeleri İstihbaratı
- Ulusal Coğrafi İstihbarat Teşkilatı (NGA)
- Ulusal Keşif Ofisi (NRO)
- Ulusal Güvenlik Teşkilatı (NSA)
- Deniz Kuvvetleri, Donanma İstihbarat Ofisi (ONI)
- Ulusal İstihbarat Direktörü Ofisi (ODNI)

Küresel çıkarlara sahip olması nedeniyle küresel tehditlere de muhatap olan ABD'nin karşı karşıya olduğu tehditlerin nitel ve nicel fazlalığının, İstihbarat ve güvenlik aygıtı içerisinde yer alan -federal- kurumların nitel çeşitliliğinin ve nicel fazlalığının temel nedenini oluşturduğunu ileri sürmek mümkündür.

İstihbarat Topluluğu şemsiyesi altında yer alan tüm kurumları doğrudan veya dolaylı olarak asimetrik tehdit ya da siber güvenlik ile bir şekilde ilişkilendirebilmek mümkün olmakla birlikte; çalışmanın bu kısmında, siber güvenliğin sağlanmasının asli görevleri arasında bulunduğu federal kurumlara yer verilecektir.

2. FEDERAL SORUŞTURMA BÜROSU *(FEDERAL INVESTIGATION BUREAU)*

Asimetrik tehdit bağlamında ele alındığında, ABD'deki ulusal güvenlik yapılanmasının merkezinde FBI yer almaktadır. 11 Eylül Saldırıları sonrası dönemde kabul edilen ve terörle mücadeleye odaklanmış olan yasal mevzuatın incelenmiş olduğu bu çalışmanın ileriki bölümlerinde de görülebileceği üzere; söz konusu saldırılar sonrasında FBI'nın siber güvenlik alanındaki rolü yerinde sayarken -ve hatta göreceli olarak gerilerken-, terörle mücadele alanındaki rolü daha da güçlenerek pekişmiştir.

Bu çerçevede, "İç Güvenlik Yasası (HSA)"nın kazananının İç Güvenlik Bakanı olması ile benzer bir biçimde, "ABD Vatanseverlik Yasası (USA PATRIOT Act)"nın da kazananının Adalet Bakanı olduğunu ileri sürmek mümkündür. Gerek karşı-istihbarat, gerekse de terörizm ve federal suçlarla mücadele görevleri kapsamında elde ettiği neredeyse sınırsız yetki, kaynak ve muafiyetin tüm ABD'yi -ve hatta bazı durumlarda başka ülke topraklarını da- kapsadığı dikkate alındığında, karşı karşıya olunan güvenlik örgütünün asimetrik tehditler ile mücadele kapasitesi çok daha açık bir şekilde ortaya çıkmaktadır.

FBI'nın terörle mücadele programlarının 1996 yılında "Terörle Mücadele Merkezi *(Counterterrorism Center)*" altında merkezileştirildiğini ve siber terörizmin FBI tarafından ulusal güvenliğe yönelik yükselen bir tehdit olarak tanımlandığını ifade eden Kushner; FBI'nın terörle mücadeledeki merkezi rolüne şöyle dikkat çekmektedir (2003: 134):

> "Geçen 20 yıl boyunca her iki partiden de başkanlar terörist tehditlere karşı, FBI'nın yetkilerini genişlettiler. Başkan Reagan, ABD'de terörle mücadelede FBI'yı başat kurum olarak belirledi. 1984 ve 1986 yıllarında ise, ABD vatandaşlarının öldürüldüğü, saldırıya uğradığı, rehin alındığı yerlerde veya belirli ABD çıkarlarına saldırıda bulunulduğu durumlarda FBI'ya yetkilerini yurtdışında da kullanma imkanı sağlayan yasalar Kongreden geçti. FBI'nın soruşturma yetkilerini genişleten ve şüpheli teröristlerin sınırdışı edilmesini kolaylaştıran Terörle Mücadele ve Etkin Ölüm Cezası Yasası *(Anti Terrorism ve Effective Death Penalty Act)* Başkan Bill Clinton tarafından imzalandı. Başkan George W. Bush tarafından ise, 2001 yılı Ekim ayında ABD Vatanseverlik Yasası imzalandı ki; bu yasa ile, FBI'ya daha fazla mali kaynak sağlanmış, gözetleme/takip yetenekleri geliştirilmiş ve ajanlarının "Büyük Jüri" bilgilerine erişmesine izin verilmiştir. FBI'nın yetkileri, kamu alanlarının ve internetin izlenmesi hususlarında daha geniş bir hareket alanı sağlayacak biçimde, 2002 yılında da genişlemiştir."

Lerner'in de belirttiği üzere (2004a: 265); siber tehditlerle cevap vermek ve altyapıya yönelik tehditlere ilişkin bilgilerin koordinasyonunu sağlamak maksadıyla federal seviyede görev yapacak olan Ulusal Altyapı Koruma Merkezi (NIPC), 1998 yılında FBI bünyesinde kurulmuştur.

11 Eylül Saldırıları öncesindeki dönemde ABD'deki siber tehdit algılamasının esas itibariyle siber suçlar ağırlıklı ve "bilgisayara yetkisiz erişim" odaklı olması nedeniyle siber tehditlere yönelik tedbirler de, doğal olarak, bir kolluk teşkilatı olan FBI'nın bünyesinde alınmıştır. 11 Eylül Saldırıları sonrasındaki dönemde ise, asimetrik tehditlerin ön plana çıkmasına paralel olarak kritik altyapı tesislerinin siber tehditlerden korunması hususu da bir ulusal güvenlik önceliği halini almıştır. Nitekim bahse konu algı değişiminin bir göstergesi olarak da; NIPC, FBI bünyesinden ayırılarak İç Güvenlik Bakanlığına bağlanmıştır.

3. İÇ GÜVENLİK BAKANLIĞI *(DEPARTMENT OF HOMELAND SECURITY)*

2002 yılında kurulmuş olan İç Güvenlik Bakanlığının terörizmle mücadele ve siber güvenliğin sağlanmasının yanı sıra sınır güvenliği, göç kontrolü ve doğal afetlere müdahale gibi başlıklar altında da pek çok görevi bulunmaktadır. 11 Eylül Saldırıları sonrası dönemde özellikle kritik altyapının korunması kapsamında, diğer birçok alanda olduğu gibi siber güvenlik alanında da dağınık bir yapı sergileyen federal kurumlar İç Güvenlik Bakanlığı bünyesinde toplanmışlardır. Bu çerçevede İç Güvenlik Bakanlığı bünyesine katılmış veya bağlanmış olan 22 kurumdan, doğrudan siber güvenlik ile ilişkili olanlar şöyle sıralanabilirler (DHS [web], 2012):

- Federal Bilgisayar Olaylarına Müdahale Merkezi *(Federal Computer Incident Response Center)*; önceden ABD Genel Hizmetler İdaresi (GSA)'ne bağlıdır.
- Ulusal İletişim Sistem Dairesi (NCS); önceden Savunma Bakanlığına bağlıdır.
- Ulusal Altyapı Koruma Merkezi (NIPC); önceden FBI'ya bağlıdır.
- Ulusal Enerji Güvenliği ve Güvence Programı *(Energy Security and Assurance Program)*; önceden Enerji Bakanlığına bağlıdır.
- ABD Gizli Servisi (USSS); önceden Hazine Bakanlığına bağlıdır.

Yukarıda sayılan kurum ve kuruluşlardan ABD Gizli Servisi haricinde kalanlar, İç Güvenlik Bakanlığına bağlanmalarının ardından yeniden yapılandırılmışlardır.

İç Güvenlik Bakanlığı teşkilat yapısı içerisinde, asimetrik tehditlere ve siber güvenliğe yönelik faaliyetler esas itibariyle Ulusal Koruma ve

Programlar Müdürlüğü (NPPD) tarafından yürütülmektedir. Bu kapsamda, bahse konu müdürlük bünyesinde bulunan (DHS [web], 2011a);

- Siber Güvenlik ve İletişim Dairesi (CS&C), ülkenin siber ve iletişim altyapısının güvenlik, esneklik ve güvenilirliğinin sağlanmasından,

- Altyapı Koruma Dairesi (IP), ülkenin kritik altyapısına yönelik olarak terör eylemlerinden kaynaklanan riskleri azaltmak üzere yürütülen ulusal çabaların yönlendirilmesinden sorumludur.

a. Ulusal Siber Güvenlik Bölümü *(National Cyber Security Division)*

İç Güvenlik Bakanlığı teşkilat yapısı içerisinde, siber güvenlikten doğrudan sorumlu olan birim Ulusal Siber Güvenlik Bölümü (NCSD)'dür. Ulusal Siber Güvenlik Bölümü (NCSD); Ulusal Koruma ve Programlar Müdürlüğü (NPPD) bünyesinde bulunan Siber Güvenlik ve İletişim Dairesi (CS&C)'ne bağlı olarak faaliyet göstermektedir.

Görevi, "siber uzayın ve ABD'nin siber varlıklarının korunması" olarak özetlenebilecek olan NCSD'nin stratejik amaçları; etkili bir ulusal siberuzay müdahale sisteminin kurulması ve kritik altyapının korunması için bir siber risk yönetimi programının hayata geçirilmesidir. NCSD bu kapsamdaki faaliyetlerini aşağıda belirtilen üç ana platformda yürütmektedir (DHS [web], 2010b):

- Ulusal Siber Müdahale Sistemi *(National Cyberspace Response System)*

- Federal Ağ Güvenliği *(Federal Network Security)*

- Siber Risk Yönetimi Programları *(Cyber Risk Management Programs)*

Ulusal Siber Müdahale Sistemi; US-CERT Operasyonlarının yanı sıra ciddi bir siber olayın gelişmesi durumunda US-CERT, kolluk kuvvetleri

ve İstihbarat Topluluğunu da içerecek şekilde ulusal müdahaleyi koordine edecek asli mekanizma olan Ulusal Siber Müdahale Koordinasyon Grubu (NCRCG)'nu da içermekte olması ile ön plana çıkmaktadır. Siber Risk Yönetimi Programları kapsamında ise, hazırlık seviyesinin ölçülmesi maksadıyla 2006 yılı Şubat ayında, 2008 yılı Mart ayında ve 2010 yılı Eylül ayında icra edilmiş olan "Siber Fırtına *(Cyber Storm)*" siber tatbikatları özellikle dikkati çekmektedir. 2010 yılı Eylül ayında icra edilen "Siber Fırtına III" tatbikatına; tüm önemli federal kurumlar, 11 eyalet, 12 yabancı ülke ve 60 özel sektör firması katılmıştır (DHS [web], 2010b).

b. ABD Bilgisayar Acil Durum Hazırlık Takımı *(United States Computer Emergency Readiness Team)*

Önceden ABD Genel Hizmetler İdaresi (GSA)'ne bağlı olarak faaliyet gösteren ve federal hükümetin askeri nitelikli olmayan bilgisayar ağlarının güvenliğinden sorumlu olan Federal Bilgisayar Olaylarına Müdahale Merkezi *(Federal Computer Incident Response Center)*, İç Güvenlik Bakanlığına bağlanmasının ardından yeniden örgütlenerek "ABD Bilgisayar Acil Durum Hazırlık Takımı (US-CERT)" adını almıştır. US-CERT, 2003 yılında yayımlanan "Güvenli Siber Uzay için Ulusal Strateji" belgesini uygulamaya geçirmek de dahil olmak üzere siber güvenlik hazırlık durumunun ve siber güvenlik koordinasyonunun sağlanmasından sorumlu olan NCSD'nin operasyonel kolu olarak faaliyet göstermektedir (US-CERT [web], 2012).

c. Ulusal Altyapı Koruma Merkezi *(National Infrastructure Protection Center)*

Ulusal Altyapı Koruma Merkezi (NIPC)'nin kritik altyapılara yönelik siber saldırılara müdahale etmek üzere 1998 yılında PDD-63 sayılı

başkanlık emri ile FBI bünyesinde kurulmuş olduğunu belirten Turner (2006: 129); söz konusu emir kapsamında NIPC'nin tehdit değerlendirmeleri ve uyarılar yayınlamasının, güvenlik açığı ve kolluk soruşturmaları yürütmesinin ve yapılacak siber saldırılara ulusal çapta karşılık vermesinin öngörüldüğünü ifade etmektedir.

Görevlerinden de anlaşılabileceği üzere, 11 Eylül Saldırıları öncesi dönemde kritik altyapının siber güvenliğinin sağlanması noktasında NIPC; özellikle istihbarat, analiz ve kolluk faaliyetlerinin yönlendirilmesinde merkezi bir konuma sahiptir.

2002 yılında İç Güvenlik Bakanlığına bağlanmasının ardından görev ve yetkileri bakanlık bünyesinde yer alan Harekat Koordinasyon Dairesi *(Office of Operations Coordination)* ve Altyapı Koruma Dairesi *(Office of Infrastructure Protection)* arasında paylaştırılan NIPC tasfiye edilmiştir (DHS [web], 2012).

NIPC'nin tasfiyesi sonrasında, özellikle siber tehditlerin analiz ve değerlendirilmesi noktasında Ulusal Siber Güvenlik ve İletişim Entegrasyon Merkezi *(National Cybersecurity and Communications Integration Center – NCCIC)* ön plana çıkmıştır.

ç. Ulusal Siber Güvenlik ve İletişim Entegrasyon Merkezi *(National Cybersecurity and Communications Integration Center)*

Ulusal Siber Güvenlik ve İletişim Entegrasyon Merkezi (NCCIC), siber uzay ve iletişim alanlarını birçok boyutta kesintisiz olarak izlemek suretiyle enformasyon alanında ortak bir operasyon resmi oluşturmak ile görevlidir. Bu açıdan bir "Harekat Merkezi" niteliği gösteren ve 7 gün 24 saat esasına göre faaliyet göstermekte olan NCCIC, siber saldırılara karşı Ulusal Müdahale Merkezi *(National Response Center)* olarak da görev yapmaktadır (DHS [web], 2011b).

d. Endüstriyel Kontrol Sistemleri Acil Durum Hazırlık Takımı *(Industrial Control Systems Computer Emergency Readiness Team)*

Endüstriyel Kontrol Sistemleri Acil Durum Hazırlık Takımı (ICS-CERT); NCCIC'nin operasyonel bir bileşeni olup, kontrol sistemlerinin siber tehditlere karşı korunmasına odaklanmıştır. ICS-CERT, İç Güvenlik Bakanlığı bünyesinde yer alan Kontrol Sistemleri Güvenlik Programı (CSSP) tarafından US-CERT ile koordineli bir biçimde yönetilmektedir (US-CERT [web], 2012b).

Bu çerçevede ICS-CERT, özellikle SCADA Sistemlerini hedef alabilecek siber sabotaj eylemlerine ilk müdahalede bulunacak olan siber güvenlik birimidir.

e. ABD Gizli Servisi *(United States Secret Service)*

1865 yılındaki asıl kuruluş amacı "para sahteciliği ile mücadele" olan ABD Gizli Servisi (USSS)'nin bir kolluk kuvveti olarak günümüzdeki görev kapsamı, sahteciliğe ilişkin diğer görevlerinin yanı sıra ABD'nin finansal ödeme sistemlerinin bütünlüğünün korunmasını da içermektedir. Kuruluşundan bugüne kadar geçen zaman içerisinde özellikle ödeme yöntemlerinde yaşanılan gelişmelere paralel olarak ABD Gizli Servisinin görev kapsamı ve tanımı da sürekli olarak genişlemiştir. Bu çerçevede (USSS [web], 2010a);

> "Günümüzde bilgisayarların ve diğer "çip"li cihazların suç eylemlerini kolaylaştırmakta veya söz konusu eylemlerin hedefinde yer almakta olmaları, ABD Gizli Servisini "siber suçlar" ile mücadeleye müdahil olmaya zorlamaktadır."

Bu kapsamda, "Bilgisayar Dolandırıcılığı *(Computer Fraud)*" ve "Erişim Cihazı Dolandırıcılığı *(Access Device Fraud)*" suçları ABD Gizli

Servisinin bilgisayar bağlantılı sahtecilik ve dolandırıcılık suçları ile mücadelesinde özellikle ön plana çıkmaktadırlar (USSS [web], 2010b).

ABD Gizli Servisi tarafından siber suçlar ile mücadele kapsamında 1995 yılında oluşturulmuş olan New York Elektronik Suçlar Görev Kuvveti *(New York Electronic Crimes Task Force)*'nin göstermiş olduğu başarının bir sonucu olarak; ABD Vatanseverlik Yasası (USA PATRIOT Act) ile bahse konu "görev kuvveti" konseptinin tüm ABD çapında hayata geçirilmesi görevi ABD Gizli Servisi Direktörüne verilmiştir.

Nitekim sağlanılmış olan bu yasal yetkiye dayanılarak, başlangıçta sadece sekiz büyük metropol alanda bölgesel bir "Elektronik Suçlar Görev Kuvvetleri (ECTFs)" ağı kurulması için harekete geçilmiş olup; söz konusu görev kuvvetleri ağı, 2007 yılı itibariyle 24 görev kuvvetini kapsayacak şekilde genişlemiştir (USSS [web], 2010c).

11 Eylül Saldırıları öncesi dönemde ABD Hazine Bakanlığına bağlı olarak faaliyet göstermekte olan ABD Gizli Servisi, İç Güvenlik Yasası (HSA)'nın 2002 yılında yürürlüğe konulması ile birlikte İç Güvenlik Bakanlığı (DHS)'na bağlanmıştır. Bu değişiklik 11 Eylül 2001 tarihinden sonraki dönemde ABD'deki siber tehdit algısında yaşanılan, çıkar amaçlı siber suçlardan kritik altyapı tesislerine yönelik asimetrik tehditlere yönelik kayışın bir göstergesi olması açısından da oldukça önemlidir.

4. ULUSAL GÜVENLİK TEŞKİLATI *(NATIONAL SECURITY AGENCY)*

ABD Savunma Bakanlığına bağlı olarak faaliyet gösteren Ulusal Güvenlik Teşkilatı (NSA) hem istihbari, hem de askeri boyutu olan ikili bir kimliğe sahiptir. NSA'nın Sinyal İstihbaratı (SIGINT) odaklı görevlerinin yanı sıra ABD Silahlı Kuvvetlerine kriptoloji desteği, bilgisi ve yardımı sağlamakla görevli olan "Merkezi Güvenlik Servisi (CSS)" de NSA bünyesinde bulunmaktadır (NSA [web], 2011a). NSA Başkanı bir asker olup, aynı zamanda CSS'nin Başkanlık ve ABD Siber Komutanlığı

(USCYBERCOM)'nın Komutanlık görevlerini de yürütmektedir. Bu kapsamda, organik olarak birbirlerine bağlı olan ve "NSA/CSS" olarak anılan "NSA" ve "CSS" ile bu kurumlarla herhangi bir organik bağı bulunmayan "USCYBERCOM", NSA Başkanının şahsında birleşmektedirler.

ABD Siber Komutanlığı (USCYBERCOM) 2009 yılında kurulmuş olup, ABD Stratejik Komutanlığı (USSTRATCOM) altında faaliyet göstermektedir. NSA/CSS ve USCYBERCOM'un görevleri ile aralarındaki ilişki, NSA Resmi İnternet Sitesinin "Sık Sorulan Sorular" kısmında yer alan "NSA/CSS ve ABD Siber Komutanlığının rolleri arasındaki farklar nelerdir?" sorusuna verilen resmi yanıt ile açık bir biçimde ortaya konulmaktadır (NSA [web], 2011b):

> "Aynı başkanı paylaşmalarına rağmen, NSA/CSS ve USCYBERCOM aynı görevi paylaşmamaktadırlar. NSA, Sinyal İstihbaratı (SIGINT) ile ulusal güvenlik bilgileri ve sistemleri için "Enformasyon Güvencesi *(Information Assurance)*" faaliyetlerini yürütür. USCYBERCOM ise, ABD Federal Kanunlarının 10.ncu (Geleneksel Askeri Faaliyetler) ve 32.nci (Ulusal Muhafızlar ve Yedekleri) Başlıkları kapsamında faaliyet gösterir.
>
> NSA/CSS birbirleri ile bağlantılı iki göreve sahiptir: (SIGINT olarak bilinen) Sinyal İstihbaratı ve Enformasyon Güvencesi. NSA, SIGINT vasıtasıyla Amerika'nın düşmanlarının gizli tutmak istedikleri enformasyonu toplarken; Enformasyon Güvencesi vasıtasıyla da, Amerika'nın hayati ulusal güvenlik enformasyonunu ve sistemlerini başkalarının hırsızlık ve zarar vermesinden korur. Birlikte ele alındıklarında, SIGINT ve Enformasyon Güvencesi görevleri üçüncü bir fonksiyon için asli önemdedirler: Askeri bir operasyon olan, "Ağ Savaşı *(Network Warfare)*"nı yürütmek.
>
> USCYBERCOM, ABD Stratejik Komutanlığı *(US Strategic Command)* altındaki bir alt-komutanlıktır. Ordunun enformasyon ağlarının işletilmesini ve savunulmasını idare eder. ABD Siber Komutanlığı; Savunma Bakanlığı Enformasyon Ağlarının korunmasına ve savunulmasına yönelik faaliyetleri günlük olarak planlar, koordine, entegre, senkronize eder ve hayata geçirirken, askeri görevlere tam spektrumlu bir destek sağlamak üzere Savunma Bakanlığı Siber Uzay Operasyonlarını da koordine eder.

> USCYBERCOM'un da hizmet alıcılarından birisi olduğu NSA/CSS; benzersiz kuvveti, yetenekleri ve yetkileri ile, Savunma Bakanlığının siber uzay operasyonlarını planlamasına ve icrasına kritik destek sağlar.

Yukarıdaki ABD'nin elektronik güvenlik, enformasyon güvenliği ve siber güvenlik alanlarındaki kritik -askeri- imkan ve kabiliyetleri resmi olarak Savunma Bakanlığı çatısı altında toplanmış olmakla birlikte; söz konusu imkan ve kabiliyetler fiilen NSA bünyesinde ve NSA Başkanının şahsında bir araya gelmektedirler. Dolayısı ile gerek asimetrik tehditler, gerekse de siber güvenlik bağlamında NSA oldukça hayati bir konumu işgal etmektedir.

Çalışmanın önceki kısımlarında da ifade edildiği üzere, 1878 tarihli *"Posse Comitatus Act"* ile ABD Silahlı Kuvvetlerinin kolluk görevlerinde kullanılması yasaklanmıştır. Bu kapsamda bahse konu yasanın terörle mücadele politikaları ve stratejileri çerçevesinde bypass edilmek istenmesi durumunda; "terörizm" tanımına asimetrik tehdit konsepti üzerinden askeri bir nitelik kazandırılması veya esasen askeri nitelikli olan ve askeri kapasiteyi kullanan kurumların askeri olmayan kimlikleri üzerinden tanımlanmaları gibi alternatif davranış tarzlarının geliştirilmesi mümkündür. Bu çerçevede kurumsal kimliğinin askeri boyutu fazlaca ön planda yer almayan ve İstihbarat Topluluğunun ulusal güvenlik hizmeti üreten bir üyesi olan NSA, özellikle siber güvenlik alanında *"Posse Comitatus Act"* hükümlerinin bypass edilebilmesi için oldukça uygun bir platform niteliği taşımaktadır.

5. ULUSAL İSTİHBARAT DİREKTÖRÜ OFİSİ *(OFFICE OF DIRECTOR OF NATIONAL INTELLIGENCE)*

İstihbarat Topluluğunun yönetilmesinden ve ulusal istihbaratın koordinasyonundan sorumlu olan Ulusal İstihbarat Direktörü (DNI) makamı, 2004 tarihli İstihbarat Reformu ve Terörizmin Önlenmesi Yasası (IRTPA) ile ihdas edilmiştir.

İstihbarat Topluluğuna yönelik görev ve sorumluluklarının haricinde Ulusal İstihbarat Direktörü (DNI), ulusal güvenlik ile ilişkili istihbarat konularında ABD Başkanına, Ulusal Güvenlik Konseyi (NSC)'ne ve İç Güvenlik Konseyi (HSC)'ne danışmanlık yapmakla da görevlidir. Ulusal İstihbarat Direktörüne bağlı olarak faaliyet gösteren Ulusal İstihbarat Direktörü Ofisi (ODNI) ise; askeri, yurtdışı ve iç güvenlik istihbarat faaliyetlerinin etkili bir şekilde bütünleştirilebilmesi için faaliyet göstermektedir (ODNI [web], 2012).

a. Ulusal Terörle Mücadele Merkezi *(National Counterterrorism Center)*

13354 sayılı Başkanlık İdari Emrine istinaden 2004 yılı Ağustos ayında kurulan ve aynı yıl çıkartılan İstihbarat Reformu ve Terörizmin Önlenmesi Yasası (IRTPA) ile yasal dayanağına kavuşan Ulusal Terörle Mücadele Merkezi (NCTC), Ulusal İstihbarat Direktörü Ofisi (ODNI)'ne bağlı olarak faaliyet göstermektedir. NCTC'nin asli görevi, İstihbarat Topluluğu için müşterek istihbarat üretilmesi ve müşterek operasyonel planlama yapılmasıdır (NCTC [web], 2012).

Terörle mücadele ile ilgili her türlü istihbaratın analizinde ve entegre edilmesinde ABD hükümetinin asli kurumu olan NCTC; gerek tehdit analizleri yapabilmek ve kurumlar arası bilgi paylaşımını sağlamak, gerekse de İstihbarat Topluluğu üyelerine bilgi bankası hizmeti verebilmek üzere 30'dan fazla askeri, istihbarat, kolluk ve iç güvenlik ağını kendi çatısı altında bir araya getirmektedir (NCTC [web], 2012).

NCTC tarafından yürütülen analiz ve planlama faaliyetleri kapsamında ise, terörizmle mücadeledeki ulusal önceliklerin hayata geçirilebilmesi için "Teröre Karşı Savaş Ulusal Uygulama Planı (NIP)", yayımlanmıştır. Bahse konu plan, ilki 2006 yılı Haziran ayında, ikincisi ise 2008 yılı Eylül ayında olmak üzere iki defa ABD Başkanı tarafından onaylanmıştır (NCTC [web], 2012).

Görevlerinden de anlaşılabileceği üzere NCTC, 11 Eylül Saldırıları sonrası dönemde terörizmle mücadelede İstihbarat Topluluğunun "füzyon merkezi" olarak faaliyet göstermektedir.

Bu kapsamda Posner, özellikle terörizmle mücadelenin entellektüel boyutunda NCTC'nin ön plana çıkan rolüne şöyle dikkati çekmektedir (2005: 47):

> "CIA'nın küçük paramiliter yeteneklerinin Savunma Bakanlığına devredilmesi teklifi, 9/11 Komisyonu'nun[12] örgütsel önerilerinin CIA'yı zayıflatmakta olduğu gerçeğinin altını çizmekteydi. CIA Başkanı, Merkezi Haberalma Direktörü (DCI) olarak konumunu kaybetmek üzereydi. CIA'nın analiz kapasitesinin bir kısmı, Ulusal İstihbarat Direktörü (DNI)'nün kadrosuna kayabilirdi. CIA Terörle Mücadele Merkezi, CIA'nın dışında ki bir Ulusal Terörle Mücadele Merkezi tarafından büyük oranda ikame edilebilirdi (Bunlar, düşman tehdidinin belirli bir cinsini ortadan kaldırmak için izleme ve planlama yapmak üzere analistlerin, bilgi toplayıcıların ve harekat planlamacılarının bir araya geldikleri füzyon merkezleridir)."

11 Eylül Saldırıları sonrasında ortaya çıkan yeni istihbarat ve güvenlik yapılanmasının verimliliğine ilişkin ciddi tartışmaların yapılmakta olduğunu ifade eden Priest ve Arkin ise; 2009 yılına kadar görevde kalmış olan eski bir üst düzey istihbarat yöneticisinin Ulusal Terörle Mücadele Merkezi (NCTC)'ne ilişkin olarak yapmış olduğu aşağıdaki tespitlere çalışmalarında yer vermektedirler (2011: 84):

> "Analistlerin üzerinde çalıştıkları şeyler konusunda muazzam bir çakışma olduğunu gördüm. Sistemli ve titiz bir işbölümü yoktu. İstihbaratın doruk noktası olması, en hassas ve zor elde edilen bilgi parçacıklarını biraraya getirmesi maksadı ile 2003 yılında kurulmuş olan devasa büyüklükteki Ulusal Terörle Mücadele Merkezi (NCTC)'nin personeli olan analistler; CIA, FBI, NSA veya DIA'nınkilerden daha orijinal veya daha iyi raporlar üretemedikleri için, istihbarat makamlarının gözünde düşük puana sahiplerdi."

Elbette ki, yukarıda sunulan eleştirel yaklaşıma karşılık olarak, ABD'deki istihbarat ve güvenlik aygıtının içerisinden geçtiği yeniden

[12] ABD Kongresi tarafından 11 Eylül Saldırılarını araştırmak üzere oluşturulan söz konusu komisyonun tam adı; "ABD'ye Yapılan Terörist Saldırılara İlişkin Ulusal Komisyon *(The National Commission on Terrorist Attacks Upon the United States)*"dur.

yapılanma sürecinin olumlu ya da olumsuz etki ve sonuçlarının ortaya konulabilmesi için daha fazla zamana ihtiyaç duyulduğunun ileri sürülebilmesi mümkündür. Bu çerçevede söz konusu yeniden yapılanma sürecine yönelik kapsamlı ve nesnel bir değerlendirme fırsatının ortaya çıkabilmesi için, ABD tarafından yürütülen "Teröre Karşı Savaş"ın sona ermesinin beklenilmesi muhtemel görünmektedir.

ÜÇÜNCÜ BÖLÜM

ASİMETRİK TEHDİT BAĞLAMINDA SİBER GÜVENLİĞİN SAĞLANMASINA YÖNELİK YASAL DÜZENLEMELER

Çalışmanın bu bölümünde, 11 Eylül Saldırıları sonrasında asimetrik tehdit bağlamında ABD'deki siber tehdit algısında yaşanılan değişimin somutlaştığı noktalar olarak, ilgili hukuksal düzenlemeler ele alınmışlardır. Önceki kısımlarda da ifade edildiği üzere, siber güvenliğin bir parçasını oluşturduğu ulusal güvenliğe yönelik tehditler özellikle küreselleşmeye ve enformasyon teknolojilerinde yaşanılan hızlı gelişmelere paralel bir biçimde değişikliğe uğramaktadır. Bu çerçevede terörizm ya da organize suç gibi kimi geleneksel tehditler teknolojiye vurgu yapan bir değişim geçirebildikleri gibi, siber sabotaj örneğinde olduğu gibi tümüyle yeni tehditler de ortaya çıkabilmektedir.

Bununla birlikte özellikle "asimetrik tehdit" ve "siber tehdit" kavramları üzerinden ifade edilen son dönem güvenlik önceliklerinin yanı sıra 11 Eylül Saldırıları ile yaşanılan "asimetrik tehdidin somutlaşması" tecrübesi de siber güvenlik ile ilişkili olarak ABD'de yürürlüğe konulan yasal düzenlemeleri ve hayata geçirilen hükümet politikalarını derinden etkilemiştir.

1. SİBER GÜVENLİK İLE İLİŞKİLİ YASAL DÜZENLEMELER

ABD'de yapılan yasal düzenlemelerin, siber güvenliğin hukuksal boyutu üzerindeki yadsınamayacak ve yönlendirici etkisi; gerek ABD'nin sahip olduğu küresel politik etkinin, gerekse de siber uzay ile bağlantılı olgu ve uygulamaların diğer ülkelere nazaran daha fazla içselleştirilmiş olmasının bir sonucudur. Nitekim Yaycı, ABD'nin sahip olduğu söz konusu etkiyi şöyle ifade etmektedir (2007: 46):

"ABD, gerek bilgisayarların kullanımı gerekse buna bağlı olan internet ağlarının kullanımı ile teknolojik gelişmelerin en hızlı ilerlediği ve bu yöndeki düzenlemelerin de en süratli şekilde yürürlüğe konulduğu ve diğer ülkeler tarafından da örnek alınan, onlara bu konuda öncülük eden bir ülkedir."

Dolayısı ile ABD tarafından siber güvenliğe ilişkin olarak geliştirilen yasal mevzuat hem ulusal, hem de uluslararası seviyede gerek vatandaşları, gerekse de hukuksal yaklaşımlar üzerinde belirgin bir etki yaratma kapasitesine sahip görünmektedir.

Enformasyon Sistemlerini[13] bir bütün olarak kabul eden Fischer, 1878-2011 yılları arasındaki tarihsel süreç içerisinde ABD'de yapılmış ve siber güvenlik ile ilişkilendirilebilecek olan yasal düzenlemeleri incelediği çalışmasında (2011: 2-3); ABD'de siber güvenlik ile ilişkilendirilebilecek elliden fazla yasa olmasına rağmen, halen siber güvenliğe yönelik herhangi bir çerçeve yasa bulunmamasına dikkat çekerek, 2002 yılı sonrasında da kapsamlı bir düzenlemenin yapılmamış olmasına vurgu yapmaktadır.

Bahse konu yasal düzenlemeler "asimetrik tehdit" ve "siber güvenlik" kavramları bağlamında değerlendirildikleri zaman, gerek kapsamlarının, gerekse de etkilerinin genişliği nedeni ile inceleme konusu yapılabilecek olan yasal düzenlemeler; "ABD Vatanseverlik Yasası (USA PATRIOT Act)" ve "İç Güvenlik Yasası (HSA)" olarak netlik kazanmaktadır. Anılanların haricinde kalan birçok kanunda da bu çalışmanın konu ve kapsamı ile ilişkilendirilebilecek çeşitli hükümler yer almakla birlikte; ABD Vatanseverlik Yasası ve İç Güvenlik Yasası, tehdit algısının genel karakterini yansıtmaları ve kendilerinden sonraki güvenlik politikalarını şekillendirmeleri ile ön plana çıkmaktadırlar.

---

[13] Çalışmasının giriş kısmında, siber güvenliğin kapsamına ilişkin tartışmalara kısaca değinen Fischer; bu çerçevede, ABD Federal Kanunlar Külliyatının 44.ncü Başlığı *(USC Title 44)* altındaki 3502.nci Madde içerisinde yer alan "Enformasyon Sistemi" ve "Enformasyon Kaynakları" tanımlarına atıfta bulunmaktadır. Bahse konu maddeye göre (Cornell [web], 2012f);
"Enformasyon Sistemi; enformasyonun toplanması, işlenmesi, bakımı, kullanımı, paylaşımı, dağıtılması veya alınması için örgütlenmiş enformasyon kaynaklarının bağımsız bir birleşimidir. Enformasyon Kaynakları; enformasyon ve personel, ekipman, mali kaynak, enformasyon teknolojisi gibi ilişkili kaynaklardır."

Siber güvenlik ile ilişkili olarak Fischer'ın çalışmasında yer almakta olan diğer kanunlar genel bir değerlendirmeye tabi tutulduklarında ise, bu düzenlemelerdeki hakim kaygının, asimetrik tehdit bağlamında siber güvenliğin sağlanmasından ziyade;

- Ticaretten sağlığa kadar pek çok alanda, özellikle kişisel verilerin veya yürütülen faaliyete ilişkin bilgilerin gizliliğinin ve güvenliğinin sağlanması,

- Kritik altyapının korunması ve özellikle elektrik şebekesinin güvenliğinin sağlanmasına yönelik teknik düzenlemelerin yapılması olduğu dikkati çekmektedir.

Bu kapsamda, siber güvenliğin sağlanmasına yönelik olarak teknik boyutları ön plana çıkan yasal düzenlemelere verilebilecek en iyi iki örnek ise (Fischer, 2011: 35-37);

- Özellikle siber güvenliğe ilişkin teknik araştırmaların teşvik edilmesini amaçlayan "2002 tarihli Siber Güvenlik Araştırma ve Geliştirme Yasası *(Cyber Security Research and Development Act 2002)*",

- Enformasyon ve hizmetlerin ulaşılabilir olarak tutulmalarında federal kurumları yönlendirici mahiyetteki asli mevzuat olarak "2002 tarihli E-Hükümet Yasası *(E-Government Act of 2002)*"dır.

Fischer'ın da ifade ettiği üzere (2011: i);

> "Siber güvenlik alanındaki federal rol karmaşıktır. Bu hem federal sistemlerin güvenliğinin sağlanmasını, hem de federal olmayan sistemlerin korunmasında yardımcı bir rolün yerine getirilmesini içerir. Mevcut yasal mevzuata göre, tüm federal kuruluşlar kendi sistemlerine ilişkin siber güvenlik sorumluluklarına ve kendi faaliyet alanlarına özel, kritik altyapı ile ilişkili birçok sorumluluğa sahiptir."

ABD hukuk sistemi içerisindeki elliden fazla yasal düzenlemenin doğrudan veya dolaylı olarak siber güvenliğin değişik boyutlarına vurgu yaptığını belirten Fischer (2011: i); kapsayıcı bir çerçeve kanun bulunmamasına dikkat çekmektedir.

11 Eylül Saldırılarından sonraki dönemde ABD'de, siber güvenlik ile doğrudan ilişkili olan veya bu alanda çeşitli hükümler içeren pek çok yasa yürürlüğe girmiş olmakla birikte; bahse konu yasalar genellikle, siber güvenlik alanında tespit edilen belirli idari veya yasal boşlukların doldurulmasını ya da güvenliğin geliştirilmesi için belirli standartların, mekanizmaların veya programların oluşturulmasını amaçlamışlardır.

Nitekim siber suçlarla etkin bir şekilde mücadele edilebilmesi için uygun bir uluslararası ortama duyulan ihtiyaca vurgu yapan "2010 tarihli Uluslararası Siber Suç Raporlama ve İşbirliği Yasası *(International Cybercrime Reporting and Cooperation Act of 2010)*" ya da kritik altyapı güvenliğinin sağlanması noktasında İç Güvenlik Bakanlığının düzenleyici yetkilerini arttıran -siber güvenlik ile ilişkili olarak ABD'de kabul edilmiş son kanun olan- "2012 tarihli Siber Güvenlik Yasası *(Cybersecurity Act of 2012)*" açısından da durum farklı değildir.

2. ABD VATANSEVERLİK YASASI (USA PATRIOT ACT)

"Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001" ya da resmi kısaltması ile "USA PATRIOT Act" isimli bahse konu kanunun temel amaçları; giriş kısmında da açıkça belirtildiği üzere, ABD'de ve dünyada terörizm eylemlerinin caydırılmasının ve cezalandırılmasının yanı sıra terörizmle mücadele alanında kolluk kuvvetlerinin sahip oldukları soruşturma araçlarının geliştirilmesidir.

Türkçeye tam olarak "Terörizmi Önlemek ve Engellemek için Gereken Uygun Araçları Sağlamak Suretiyle Amerika'nın Birleştirilmesine ve Kuvvetlendirilmesine İlişkin 2001 tarihli Yasa" şeklinde çevrilebilecek olan bahse konu kanunun isminde geçen "önlemek", "engellemek" ve "gerekli araçlar" gibi ifadeler, yasanın ruhuna hakim olan ve özellikle insan hakları savunucularının eleştirilerine kaynaklık eden ulusal güvenlik ve terörle mücadele odaklı istihbarat ve güvenlik anlayışını yansıtması

bakımından da oldukça anlamlıdır. ABD Vatanseverlik Yasası kapsamında, özellikle federal kurumların ve görevlilerin yetkilerinin arttırılmasına, uluslararası terör örgütleri ve yabancı ülke gizli istihbarat faaliyetleri ile mücadeleye odaklanmış olan düzenlemeler dikkati çekmektedir.

İlk bakışta kapsamlı bir terörle mücadele yasası izlenimi vermekle birlikte, ABD Vatanseverlik Yasası; ulusal güvenliğin sağlanmasına ilişkin olarak zaten varolan hukuki ve idari altyapının terörizm bağlamında asimetrik tehditler ile de mücadele edebilecek şekilde yeniden yapılandırılmasını ve eksikliklerin giderilmesini öngören bir şemsiye yasa mahiyetindedir. Bahse konu yasa ile, her ne kadar özellikle terörizmin finansmanı ile mücadele noktasında küresel bir yaklaşım öngörülmekte ise de, esas itibariyle ülke içerisinden kaynaklanan asimetrik tehditlerle mücadelede kapasitenin arttırılması amaçlanmaktadır. Bu kapsamda federal kurumlar kuvvetlendirilirken ve federal görevlilerin yetkileri ciddi bir biçimde arttırılırken, gerekli görüldüğü yerlerde federal seviyede yeni kurumlar da ihdas edilmektedir.

Genel olarak değerlendirildiği zaman ABD Vatanseverlik Yasası, adı ile de mütenasip bir şekilde, "Vatanseverlik" vurgusu üzerinden kişi hak ve hürriyetlerinde önemli fedakârlıkların yapılmasını öngören, eyaletler ve yerel yönetimler karşısında federal hükümeti daha da güçlendiren bir yasal düzenleme özelliği göstermektedir.

Gerek sahip olduğu terörizm algısının, sadece şiddet odaklı eylemleri değil, bir bütün olarak "her türlü asimetrik tehdidi" içermesi ve gerekse de enformasyon teknolojilerine ilişkin birçok hükmü içermesi nedeniyle ABD Vatanseverlik Yasası; 11 Eylül Saldırıları sonrası dönemde, asimetrik tehdit bağlamında ortaya çıkan siber tehdit algısının ve geliştirilen güvenlik politikalarının tespit edilebilmesi için temel bir belge niteliğindedir.

Bu çalışmanın ilgili kısımlarında da ortaya konulduğu üzere, 11 Eylül Saldırıları ile birlikte asimetrik tehditlerin gerçek kapasitelerinin ne kadar yüksek olabileceğinin farkına varan ABD kamuoyunun terörizme

ilişkin pek çok algısı pekişirken, ülke içerisinden kaynaklanan -yeni- bir asimetrik tehdit algısı da net bir biçimde ortaya çıkmıştır. Bu kapsamda ABD Vatanseverlik Yasası, 11 Eylül Saldırıları sonrasında ortaya çıkmış olan travmatik algıları ve tepkisel politikaları yansıtmaktan ziyade, önceki dönemlerde yaşanılan birçok terör eyleminden de izler taşıyan çok yönlü ve kapsamlı bir asimetrik tehdit algısını ve güvenlik yaklaşımını içermektedir.

Nitekim, ABD Vatanseverlik Yasası'na eleştirel bir biçimde yaklaşan Jennifer Van Bergen'e göre ([web], 2002); gerek şeklen 11 Eylül Saldırıları öncesinde hazırlanmış olan bazı kanun tekliflerini içermesi, gerekse de ruhen "1996 tarihli Terörle Mücadele ve Etkin Ölüm Cezası Yasası *(Antiterrorism and Effective Death Penalty Act of 1996)*" ile ortaya çıkan "ulusal güvenlik adına kişi hak ve hürriyetlerinden vazgeçilmesi" eğiliminin son halkasını oluşturması nedeniyle, ABD Vatanseverlik Yasası 11 Eylül 2001 tarihinden önce hazırlanmış ve yazılmış olan bir yasadır.

Yukarıdaki yaklaşım çerçevesinde, 11 Eylül Saldırılarının açmış olduğu travmatik "fırsat penceresi" sayesinde, geçmiş dönem tecrübelerinden kaynaklanan bir asimetrik tehdit algısına dayanılarak önceden hazırlanmış olan güvenlik politikalarının ve stratejilerinin hem kolay, hem de hızlı bir biçimde kabul edilmiş ve benimsenmiş olduklarını ileri sürmek mümkündür.

Siber güvenlik açısından ele alındığı zaman, ABD Vatanseverlik Yasası'nın siber suçlara ilişkin olarak federal kanunlarda önemli değişiklikler içerdiğini ifade eden Dunn Cavelty (2008: 104); bahse konu değişiklikler sonrasında "siber terörizm" olgusunun oldukça geniş yorumlanabilecek bir hale getirilmiş olmasından kaynaklanan çeşitli sorunlara dikkat çekmektedir. Nitekim Dunn Cavelty'ye göre, "bilgisayar vasıtası ile öldürme" olarak nitelendirdiği durumda verilebilecek olan ömür boyu hapis cezası, ABD Vatanseverlik Yasası kapsamında getirilen olağanüstü nitelikli düzenlemelere önemli bir örnek teşkil etmektedir.

Skibell de benzeri bir biçimde, 1986-2003 yılları arasındaki dönemde siber suçlara ilişkin olarak ABD'de yapılmış olan yasal

düzenlemeleri incelediği çalışmasında (2003: 921); yasal düzenlemelerin hedefinde yer alan bilişim suçlusu ile gerçek hayatta söz konusu düzenlemelere göre yasal takibata uğrama ihtimali olan kişiler arasındaki ciddi bir uyumsuzluğa dikkat çekmektedir. Cezalandırıcı nitelikte olduğunu iddia ettiği hakim yaklaşımın uzun vadeli etkilerine de vurgu yapan Skibell'e göre (2003: 911):

> "Hakim yaklaşım zaman içerisinde, "Bilgisayara Zararsız Erişim *(Harmless Computer Trespass)*" ile "Ağır Bilişim Suçu" *(Felonious Computer Crime)*" arasındaki gerçek ayrımın üstünü örtmüş, ayrıca yanlış yönlendirilmiş ve etkisiz bir bilişim suçları politikasının da ortaya çıkmasına neden olmuştur."

Sınırları belirsiz bir "terörizm" algısının hakim olduğu bu yaklaşımının yanı sıra kolluk kuvvetlerine sağlamış olan oldukça geniş -ve kimilerine göre aşırı- yetkiler de, ABD Vatanseverlik Yasası'na yönelik ayrı bir eleştiri konusunu oluşturmaktadır.

Dunn Cavelty'nin de ifade ettiği üzere; ABD Vatanseverlik Yasası ile federal kurumlara sağlanmış olan bazı yetkiler, bahse konu kanunda yer alan *"Sunset"* maddesi gereğince, 2006 yılında yeniden ABD Kongresinin onayına sunulmuştur. Bu kapsamda bahse konu yetkilerin, sivil özgürlüklere ilişkin birçok koruma tedbiri ile birlikte yeniden kabul edildiğini belirten Dunn Cavelty (2008: 105); 2007 yılında ABD Adalet Bakanlığı müfettişleri tarafından yapılan denetimlerde ortaya çıkartıldığı üzere, FBI tarafından ABD Vatanseverlik Yasası'na hatalı ve yasadışı olarak başvurulduğu durumların da varlığına dikkat çekmektedir.

Bu noktada, ABD Kongresi tarafından oluşturulan "9/11 Komisyonu" tarafından tespit edilmiş olan zaafiyetlerin giderilmesi maksadıyla hayata geçirilen "İstihbarat Reformu"nu, ABD Vatanseverlik Yasası ile karşılaştırmalı olarak ele alan bir hukuk adamının görüşlerine yer vermek de uygun olacaktır. İstihbarat Reformunu, yeni bir iç istihbarat teşkilatı oluşturulması yerine rekabet halindeki mevcut istihbarat teşkilatlarının "zorla" bir araya getirilmesi yönünden eleştiren ABD Yedinci Çevre Temyiz Mahkemesi *(United States Court of Appeals for the Seventh Circuit)* yargıçlarından Richard A. Posner'e göre (Posner, 2005: 200):

> "Komisyon, "güvenlik karşılığında özgürlükten vazgeçme" gibi hassas bir mesele ile istemeyerek yüzyüze geliyordu. Komisyon, büyük olasılıkla yanlış olmasına rağmen, yaygın bir kanaat olduğu için; -yeni- bir iç istihbarat teşkilatının, sivil hakları, İstihbarat Reformu Yasası'ndaki benzer terörle mücadele düzenlemeleri ile genişletilen ABD Vatanseverlik Yasası'ndan çok daha fazla zayıflatacağına inandı."

Asimetrik tehditler ile karşı karşıya kalınabilecek -neredeyse- her nokta ve duruma ilişkin bir düzenleme içeren ABD Vatanseverlik Yasası; Posner'in yukarıdaki yorumundan da anlaşılabileceği üzere, hem kendisi dışındaki tedbirleri kısmen de olsa anlamsızlaştırmakta, hem de kişi hak ve hürriyetlerine yönelik potansiyel bir tehdit odağı yaratmaktadır.

Böyle bir ortam içerisinde devlet kurumlarının ve görevlilerinin sahip oldukları yetkiler karşısında kişi hak ve hürriyetlerinin korunması söz konusu olduğunda, bireylerin hassas ve belki de şüpheci davranmaları pek de şaşırtıcı olmamalıdır. Zira, Rollings-Magnusson da ifade ettiği üzere (2009: 216);

> "İnsan hak ve hürriyetleri, devletin gücünün sınırlarını gösterirler. Her hak, uzun ve fedakarca mücadeleler sonucunda, zorlukla kazanılmıştır. Krallar ve hükümetler, güce dayalı hükümranlıklarından kolayca vazgeçmek istememişlerdir."

Çalışmanın bundan sonraki kısmında, ABD Vatanseverlik Yasası'nın asimetrik tehdit bağlamında siber güvenlik ile ilişkilendirilebilecek kısımları ayrıntılı bir biçimde incelenecek olup; bahse konu kanun metninin orijinalinden yapılabilecek okumalar sırasında, referans alınan kanun metnine ve üzerinde değişiklik yapılan kanunların önceki biçimlerine eşzamanlı olarak başvurulmasının anlaşılırlığı arttıracağı değerlendirilmektedir. Mevcut mevzuata bazı bağlaç, kelime veya cümlelerin eklenmesi ya da çıkartılması biçiminde yapılan değişikliklerin daha iyi anlaşılabilmesi içinse, ait oldukları "Federal Kanun Başlığı"na[14] ilişkin bir ön çalışma yapılması faydalı olacaktır.

---

[14] Federal kanunların kodifikasyonuna dayanan ve toplam 51 adet "Başlık *(Title)*"tan oluşan bu yasal mevzuat yapısı içerisinde; örneğin Federal Ceza ve Ceza Muhakemesi Usulüne ilişkin mevzuata ulaşmak için, *"United States Code: Title 18 - Federal Crimes and Criminal Procedure (USC Title 18)"*e başvurulmalıdır. Söz konusu kodifikasyon sonucunda ortaya çıkan yasal mevzuatın bütünü ise, çalışmanın bundan sonraki kısımlarında "Federal Kanunlar Külliyatı" olarak anılacaktır.

Bu çalışma kapsamında, ABD Kongre Kütüphanesi resmi internet sitesinden alınmış olan nihai kanun metninden ve Cornell Üniversitesi Hukuk Fakültesi Yasal Mevzuat Bilgi Enstitiüsü (LII) veritabanıındaki Federal Kanunlar Kodifikasyonundan faydalanılmış olup; çalışmanın altbaşlıklarının belirlenmesinde ABD Vatanseverlik Yasası'nda yer alan orijinal bölüm başlıklarına ve sıralamaya sadık kalınmıştır.

Her ne kadar terörle mücadele ve ulusal güvenlik açıklarını kapatmak noktasında ortak amaçları paylaşmakta oldukları bir gerçek ise de, birbirleri ile yakından ilişkili ya da bağlantılı olmayan bazı düzenlemelerin aynı bölümler içerisinde yer almaları ABD Vatanseverlik Yasası'nın bir bütün olarak anlaşılmasını zaman zaman zorlaştırabilmektedir. Bu kapsamda anlaşılırlığı arttırmak maksadıyla; bahse konu kanun metni, maddeleri üzerinden incelemeye konu edilmiş ve ilgili olduğu değerlendirilen her bir kanun maddesine çalışma metni içerisinde ayrı birer paragraf olarak yer verilmiştir.

a. Birinci Bölüm: İç Güvenliğin Terörizme Karşı Geliştirilmesi

Mevcut iç güvenlik hizmetlerinin iyileştirilmesi için yapılan bazı idari ve mali düzenlemelerin yer aldığı birinci bölüm içerisinde, siber güvenlik ile ilişkilendirilebilecek olan maddeler ve öngördükleri düzenlemeler şöyle sıralanabilirler.

1) "FBI Teknik Destek Merkezi için Arttırılmış Finansman" başlıklı 103.ncü madde kapsamında; 1996 tarihli Terörle Mücadele ve Etkin Ölüm Cezası Yasası ile FBI bünyesinde kurulmuş olan "Teknik Destek Merkezi *(Technical Support Center)*"nin terörizmle mücadeledeki ihtiyaçlarını karşılamak üzere, 2002-2004 yılları arasında 200 milyon ABD Dolarlık bir ilave mali kaynak tahsis edilmiştir.

2) "Ulusal Elektronik Suç Görev Kuvveti Girişiminin Genişlemesi" başlıklı 105.nci madde kapsamında; kritik altyapı ve mali

ödeme sistemlerine yönelik muhtemel terörist saldırılar da dahil olmak üzere elektronik suçların değişik biçimlerini tespit etmek, önlemek ve soruşturmak maksadıyla, "New York Elektronik Suçlar Görev Kuvveti" modeline dayanan bir elektronik suç görev kuvvetleri şebekesinin ulusal seviyede geliştirilmesi için gerekli faaliyetlerde bulunmak üzere ABD Gizli Servisi Direktörü görevlendirilmiştir.

b. İkinci Bölüm: Takip Prosedürlerinin Geliştirilmesi

ABD Vatanseverlik Yasası'nın, kişi hak ve hürriyetlerine ilişkin olarak en çok eleştiri almış olan bu bölümünde; yetkili federal kurumlar tarafından istihbarat toplanmasına, suçla mücadele faaliyetleri kapsamında yürütülmekte olan teknik takip prosedürlerine, iletişimin tespiti ve dinlenmesine ilişkin düzenlemeler yer almaktadır. Bu kapsamda;

- Terörizm ve siber suçlar ile ilişkili olarak telli, sözlü ve elektronik iletişimin tespit edilmesinin adli uygulamalar kapsamına dahil edilmesi,

- Suç soruşturmalarına ilişkin elde edilen bilgilerin, ilgili ve yetkili federal kurumlar arasında paylaşımının arttırılmasına yönelik düzenlemeler yapılması,

- Telli ve sözlü iletişimin tespitine ve ifşa edilmesine ilişkin olarak istihbarat faaliyetleri çerçevesinde federal hükümete sağlanmış olan istisnaların kapsamına elektronik iletişimin de dahil edilmesi özellikle dikkati çekmektedir.

Bu bölüm içerisinde yer alan değişiklik ve düzenlemeler genel olarak değerlendirildikleri zaman; biyometrik veriler başta olmak üzere kişisel verilerin toplanmasının, federal kurumların elektronik iletişimin kendisine ve iletişim altyapısına ulaşımının kolaylaştırılmasının ve ulusal güvenlik ile ilişkili istihbarat faaliyetlerine ilişkin kolaylaştırıcı

düzenlemelerin ABD Vatanseverlik Yasası'na yönelik eleştirilerin büyük bir kısmına kaynaklık etmelerinin şaşırtıcı olmadığı görülmektedir.

ABD Vatanseverlik Yasası'nın ikinci bölümü içerisinde, siber güvenlik ile ilişkilendirilebilecek olan maddeler ve öngördükleri düzenlemeler şöyle sıralanabilirler:

1) "Bilgisayar Dolandırıcılığı ve İstismarı Suçları ile İlgili Telli, Sözlü ve Elektronik İletişimin Takibi Yetkisi" başlıklı 202.nci madde ile; Federal Ceza Kanununun[15] bilgisayarlar ile bağlantılı dolandırıcılık suçlarına ilişkin hükümlerinin cürüm işlemek maksadıyla ihlal edildiği durumlar, haklarında telli, sözlü ve elektronik iletişimin tespitine başvurulabilecek suç kategorileri arasına dahil edilmiştir.

2) "Telli, Sözlü ve Elektronik İletişimin Tespit ve İfşa Edilmesine İlişkin Sınırlamalardaki İstihbarat Muafiyetlerine Açıklık Getirilmesi" başlıklı 204.ncü madde ile; telli ve sözlü iletişimin tespit ve ifşa edilmesine ilişkin olarak belirli bazı istihbarat faaliyetleri çerçevesinde federal hükümete sağlanmış olan istisnaların kapsamına elektronik iletişim de dahil edilmiştir.

3) "Mahkeme Emrine Uygun Olarak Sesli Posta Mesajlarına Elkonulması" başlıklı 209.ncu madde ile; esas itibari ile bir bilgisayar sistemine dayalı olarak faaliyet göstermelerine rağmen telli iletişim altyapısını kullanan "Sesli Mesaj *(Voice Mail)*" servislerinde yer alan mesajlara yargıç kararı ile el konulabilmesine imkan tanıyacak biçimde, Federal Ceza Kanununda bazı değişiklikler yapılmıştır. Bu çerçevede ilgili kanun maddesi, "telli" ve "elektronik" ifadelerinin metinde birlikte yer alacakları biçimde yeniden düzenlenmiştir.

4) "Elektronik İletişim Kayıtlarına İlişkin Celplerin Kapsamı" başlıklı 210.ncu madde ile; Federal Ceza Kanununda yer alan önceki düzenleme iptal edilerek, elektronik iletişim veya uzaktan erişim hizmeti veren hizmet sağlayıcılar, üyelerine veya müşterilerine ait aşağıdaki

[15] Anlayış kolaylığı sağlamak maksadıyla, çalışmanın bundan sonraki kısımlarında; "Federal Ceza ve Ceza Muhakemesi Usulüne ilişkin Mevzuat *(United States Code: Title 18 - Federal Crimes and Criminal Procedure)*"ı karşılamak üzere, "Federal Ceza Kanunu" ifadesi kullanılmıştır.

bilgileri mahkeme celbi ile yetkilendirilmiş hükümet kurumlarına vermekle yükümlü tutulmuşlardır:

> "(A) İsim;
>
> (B) Adres;
>
> (C) Yerel ve uzun mesafe telefon bağlantı kayıtları veya görüşme zaman ve sürelerine ilişkin kayıtlar;
>
> (D) Verilen hizmetin süresi (başlangıç tarihi de dahil olmak üzere) ve faydalanılan hizmetlerin türleri;
>
> (E) Geçici olarak atanan herhangi bir ağ adresini de içerek biçimde, Telefon, cihaz veya diğer abonelik ya da kimlik numarası;
>
> (F) Bir abonenin aldığı hizmetler için yaptığı ödemenin kaynağı ve araçları (herhangi bir kredi kartı veya banka hesabını da içerek biçimde);"

5) "Yaşamı ve Uzuvları Korumak için Elektronik İletişimin Acil İfşası" başlıklı 212.nci madde ile; Federal Ceza Kanununda bazı değişiklikler yapılmak suretiyle hizmet sağlayıcılara, herhangi bir kişinin kendisine ait bilgilerinin vakit geçirmeksizin ifşa edilmesini gerektirecek kadar hayati veya ciddi fiziksel yaralanma tehlikesi içerisinde bulunduğu acil bir durumun varlığına inanılması durumunda, iletişim ve müşteri kayıtlarını hükümet kurumları ile paylaşma izni verilmiştir.

6) "FISA[16] Kapsamında Pen Register ve Trap and Trace Kullanma Yetkisi" başlıklı 214.ncü madde ile; uluslararası terörist örgütlerin ve yabancı istihbarat örgütlerinin ABD topraklarındaki faaliyetleri ile mücadele esaslarını düzenleyen 1978 tarihli Yabancı İstihbarat Takip Yasası çerçevesinde *"Pen Register"* ve *"Trap and Trace"* cihazları[17] kullanılmak suretiyle yürütülebilecek soruşturmaların kapsamı genişletilmiştir.

---

[16] *Foreign Intelligence Surveillance Act of 1978* (1978 tarihli Yabancı İstihbarat Takip Yasası)

[17] *Pen Register* cihazı *(Wikipedia [web], 2011a); "belirli bir telefon hattından aranılan tüm numaraları kayıt altına alan elektronik bir cihazdır.".* Günümüzde anlam genişlemesine uğrayan bu terim; internet iletişimini de içerecek biçimde yukarıdaki işlevi yerine getiren her türlü cihaz ya da programı kapsayacak biçimde kullanılmaktadır (Wikipedia [web], 2011a).
Trap and Trace cihazı *(Wikipedia [web], 2011b); "bir telekomünikasyon sistemi üzerinden geçen tüm iletişim sinyallerini kaydetmek ve takip etmek üzere kullanılan elektronik bir cihazdır.".* İşlevsel olarak büyük benzerlikler gösteren ve günümüzde aynı bilgisayar programları tarafından ikame edilebilen *Pen Register* ve *Trap and Trace* cihazları, çoğunlukla terimsel olarak da bir arada kullanılmaktadırlar (Wikipedia [web], 2011b).

7) "Pen Register ve Trap and Trace Cihazlarının Kullanılmasına İlişkin Yetkilerin Tadili" başlıklı 216.ncı madde ile; hükümet kurumları tarafından yalnızca *"Pen Register"* cihazlarının kullanımının yetkilendirildiği Federal Ceza Kanunundaki ilgili düzenlemenin kapsamına *"Trap and Trace"* cihazları da dahil edilmiştir.

Yine bu madde kapsamında yapılan değişiklikler ile *"Pen Register"* ve *"Trap and Trace"* cihazlarının yasal tanımları, ağ iletişimini ve internet trafiğini de kapsayacak biçimde revize edilirken[18]; bahse konu cihazları kullanacak olan kurumlara, iletişimin muhteviyatını takip etmeyecek uygun teknolojiyi kullanma yükümlülüğü getirilmiştir.

8) "Bilgisayara Yetkisiz Erişimin Tespiti" başlıklı 217.nci madde ile; "Yetkisiz Erişen *(Computer Trespasser)*" tanımı Federal Ceza Kanununa dahil edilmiştir. Korunmuş bir bilgisayara[19] yetkisiz olarak erişen kişi için öngörülen bu tanıma göre;

---

[18] ABD Vatanseverlik Yasası ile aldığı -ve hali hazırda geçerli olan- biçimi ile, bahse konu cihazların Federal Ceza Kanununun 3127.nci maddesinde yer alan yasal tanımları şöyledir (Cornell [web], 2012d):
"(3) 'Pen Register' terimi, telli veya elektronik iletişimin iletildiği ya da sağlandığı bir araç veya tesis tarafından iletilen arama, yönlendirme, adresleme veya sinyal bilgilerini kaydeden ya da çözümleyen bir cihaz ya da süreç anlamına gelmekle birlikte; bu bilgiler herhangi bir iletişimin muhteviyatını içeremez. Bu tanımı ile terim; telli veya elektronik iletişim hizmeti sağlayanların ya da müşterilerinin faturalandırma maksadıyla, iletişim sağlayıcıların faturaya esas iletişim hizmetini sağlandığını ispatlamak maksadıyla veya maliyet muhasebesi hizmeti ya da ticari faaliyetinin normal akışı içerisindeki benzer amaçlarla telli iletişim hizmeti sağlayanların veya kullananların istifade ettikleri herhangi bir cihaz veya süreci kapsamaz.
(4) 'Trap and Trace' terimi, belirli bir kaynak numaranın tanımlanması için 'gelen' elektronik veya diğer sinyalleri yahut bir telli veya elektronik iletişim kaynağının tanımlanması için gerekli diğer arama, yönlendirme, adresleme ve sinyal bilgilerini yakalayan bir cihaz ya da süreç anlamına gelmekle birlikte; bu bilgiler herhangi bir iletişimin muhteviyatını içeremez."

[19] ABD Vatanseverlik Yasası'nın bu maddesi çerçevesinde; "Korunmuş Bilgisayar *(Protected Computer)*" tanımı için yine Federal Ceza Kanununun 1030.ncu maddesindeki yasal tanıma atıfta bulunulmak suretiyle, söz konusu tanım yaygınlaştırılmıştır. Bu kapsamda, Federal Ceza Kanununun 1030.ncu maddesinde yer alan "Bilgisayar *(Computer)*" ve "Korunmuş Bilgisayar *(Protected Computer)*" tanımları şöyledir (Cornell [web], 2012b):
"(e) Bu kısımda kullanıldığı hali ile-
(1) 'Bilgisayar' terimi, mantıksal, aritmetik veya depolama işlevleri gören elektronik, manyetik, optik, elektrokimyasal veya diğer yüksek hızlı bir veri işleme aracı anlamına gelmekle ve doğrudan böyle bir cihazla ilişkili olan ya da çalışmak için böyle bir cihaza bağlı olan her türlü veri depolama veya iletişim tesisatını da içermekle birlikte; bu tanım, otomatik daktilo veya dizgicileri, elde taşınabilir hesap makinelerini veya diğer küçük cihazları kapsamaz.
(2) 'Korunmuş Bilgisayar' terimi aşağıdakilere haiz olan bir bilgisayar anlamına gelir-
(A) Münhasıran finansal bir kuruluşun veya ABD Hükümetinin kullanımında bulunan veyahut böyle bir kullanım için münhasıran bir bilgisayarın bulunmaması durumunda finansal bir kuruluş veya ABD Hükümeti tarafından ya da onlar için kullanılan ve suçu oluşturan davranışın, finansal bir kuruluş veya ABD Hükümeti tarafından ya da onlar için kullanılmasını etkilediği -ya da-,
(B) -ABD'nin eyaletlerarası veya yurtdışı ticaretini ya da iletişimini etkileyecek biçimde kullanılması halinde ABD sınırları dışında bulunan bir bilgisayarıda kapsayacak biçimde- eyaletlerarası veya yurtdışı ticaret ya da iletişimde kullanılan veyahut etkileyen."

"(21) 'İhlalci'-

(A) Yetkisi olmaksızın "korunmuş bir bilgisayara" giriş yapan ve bu nedenle de eylemi kapsamında bahse konu korunmuş bilgisayara, bilgisayar vasıtasıyla veya bilgisayardan yapmış olduğu iletişimde makul bir gizlilik beklentisine sahip olmayan kişi anlamına gelir;

(B) Korunmuş bilgisayara kısmen veya tamamen giriş yapmak için, korunmuş bilgisayarın sahibi veya işletmeni ile aralarında varolan bir sözleşme ilişkisi bulunan kişiyi kapsamaz."

Yine aynı madde ile öngörülen düzenlemeye göre; aşağıdaki şartların karşılanması durumunda, yetki sınırları içerisinde olup olmamasına bakılmasızın devlet görevlilerinin görevleri gereği, "bir bilgisayar ihlalcisinin korunan bir bilgisayara, korunan bir bilgisayar üzerinden veya korunan bir bilgisayardan ilettiği telli veya elektronik iletişimi tespit etmeleri" durumu yasadışı olarak kabul edilmeyecektir. Tümünün bir arada bulunması gereken söz konusu şartlar şöyledir:

"Eğer-

(I) Korunan Bilgisayarın sahibi veya işletmeni, ihlalcinin korunan bilgisayar üzerindeki iletişiminin tespiti için yetkilendirir ise;

(II) Yetki Aşımı[20] yapan kişi bir soruşturmada yasal olarak görevlendirilmiş ise;

(III) Yetki aşımı yapan kişi, ihlalciye ait iletişimin içeriğinin soruşturma ile ilgili olacağına inanmak için makul gerekçelere sahip ise; ve

(IV) Böyle bir tespit durumu, İhlalciye gelen veya ondan iletilenler haricindeki iletişimi kapsamıyor ise."

9) "FISA Kapsamındaki Telefon Dinleme ile Uyum için Dokunulmazlık" başlıklı 225.nci madde ile; FISA kapsamında yer alan bir acil durum yardım talebinin veya bir mahkeme emrinin gereğini yerine getirmek üzere bilgi, donanım veya teknik yardım sağlayan telli veya

[20] Yasa metninde kullanılan ifade *"acting under color of law"* şeklinde olup; "Yetki Aşımı" olarak çevrilmesi tercih edilmiştir. *"Color of Law Abuses"* vakalarının soruşturulmasında ABD çapında asli yetkili kurum olan FBI'nın tanımlamasına göre (FBI [web], 2012);
"Bahse konu vakalar, yasal yetkilerinin sınırları içerisinde veya ötesinde hareket eden hükümet görevlilerinin eylemlerini içerir. Görev dışı eylemler; failinin, resmi statüsü ile bir şekilde ilişkili olduğunu iddia etmesi durumunda bu kapsamda değerlendirilebilirler."

elektronik iletişim hizmeti sağlayıcı, mülk sahibi, yeddiemin veya diğer kişiler -her türlü yönetici, çalışan, temsilciyi de içermek üzere- aleyhine mahkeme yoluna başvurulamayacağı öngörülmüştür.

10) ABD Vatanseverlik Yasası'nın ikinci bölümünde yer alan bazı düzenlemelerin son geçerlilik tarihlerine ilişkin "Sunset"[21] başlıklı 224.ncü maddeye göre; 203(a), 203(c), 205, 208, 210, 211, 213, 216, 219, 221 ve 222.nci maddeler ve bu maddelerle yapılmış olan değişikler hariç olmak üzere, yasanın ikinci bölümü ve bu bölüm kapsamında yapılmış olan değişiklikler 31 Aralık 2005 tarihi itibariyle -kendiliğinden- yürürlükten kalkacaklardır.

c. Üçüncü Bölüm: 2001 tarihli Uluslararası Para Aklamanın Azaltılması ve Terörizme Karşı Finansman Yasası

ABD Vatanseverlik Yasası'nın bu bölümünde yer alan düzenlemeler terörizmin uluslararası finansmanının önlenmesine odaklanmakta ve bu amaçla; gerek ABD'de, gerekse de diğer ülkelerde belirli politikaların ve kurumların oluşturulmasının, ticari sırların ve mali bilgilerin uluslararası terörizm soruşturmaları ve istihbarat analizleri kapsamında kullanılmak üzere ABD kurumları ile paylaşılmasının sağlanmasını öngörmektedir. Bu kapsamda; para aklama, mali suçlar ve terör örgütlerinin finansmanının önlenmesi maksadıyla alınacak tedbirler ve uygulanacak prosedürler genel olarak ABD Hazine Bakanlığı sorumluluğunda bulunmaktadır.

ABD Vatanseverlik Yasası'nın üçüncü bölümünde, siber güvenlik ile ilişkilendirilebilecek olan maddeler ve öngördükleri düzenlemeler şöyle sıralanabilirler:

---

[21] *"Sunset Provision/Clause"*: Kanun, yönetmelik veya diğer bir yasal düzenlemede yer alan, sonradan geçerlilik süresinin uzatılmasını öngören her hangi bir yasama girişiminde bulunulmadıkça, yasal düzenlemenin etkisinin belirli bir tarihten sonra sona ermesini öngören bir kamu politikası tedbirdir (Wikipedia [web], 2012ç).

1) "Yabancı Yolsuzluk Suçlarının Para Aklama Suçları Kapsamına Alınması" başlıklı 315.nci madde ile; Federal Ceza Kanunu çerçevesinde "Kara Para"ya kaynaklık ettiği kabul edilen yasadışı faaliyetlerin kapsamına, yine Federal Ceza Kanununun 1030.ncu maddesinde yer alan "Bilgisayar Dolandırıcılığı ve İstismarı Suçları" da dahil edilmiştir.

2) "Yurtiçi Döviz ve Yükümlülüklerin Taklit Edilmesi" başlıklı 374.ncü ve "Yabancı Döviz ve Yükümlülüklerin Taklit Edilmesi" başlıklı 375.nci madde ile; taklit etme eyleminde kullanılmak üzere üretilen, ticareti yapılan veya edinilen malzemelerin kapsamına analog, dijital ve elektronik "görüntüler *(images)*" de dahil edilmiştir.

ç. Dördüncü Bölüm: Sınırın Korunması

ABD Vatanseverlik Yasası'nın, kişi hak ve hürriyetlerine ilişkin olarak eleştiri aldığı bir diğer bölüm ise, dördüncü bölümdür. Bu bölüm, biyometrik veriler de dahil olmak üzere kişisel verilerin toplanması, kimlik tespitinde kullanılacak teknolojik altyapı standartlarının tespit edilmesi, suç kayıtlarının hükümet kurumları arasında paylaşımının sağlanması, göçmenlik ve vize politikalarının sıkılaştırılması gibi düzenlemeleri bünyesinde barındırmaktadır.

Dördüncü bölüm kapsamında yer alan düzenlemelerin diğer bir özelliği ise; terörizmle mücadelenin yanı sıra göçmenlik ve vize politikalarının geliştirilmesinde de yönlendirici nitelikte olan, "terörizm" ve ilişkili kavramların yasal tanımlarında çeşitli değişiklikleri öngörmeleridir. Bu kapsamda söz konusu tanımların, küçük rötuşlarla ya da yalnızca bazı bağlaçların eklenmesi veya çıkartılması yoluyla değiştirildiği dikkati çekmekte; bu suretle kapsamları genişletilen tanımlar üzerinden de, federal kurumların ve soruşturma süreçlerinin lehine önemli değişiklikler yapıldığı görülmektedir.

ABD Vatanseverlik Yasası'nın dördüncü bölümü içerisinde doğrudan siber güvenlik ile ilişkilendirilebilecek bir düzenleme bulunmamaktadır.

d. Beşinci Bölüm: Terörizm Soruşturmalarının Önündeki Engellerin Kaldırılması

ABD Vatanseverlik Yasası'nın, ikinci ve dördüncü bölümleri ile benzer bir şekilde, kişi hak ve hürriyetlerine ilişkin olarak çeşitli eleştirilere konu olan bu bölümünde; terörizmle mücadele kapsamında yapılan soruşturmaları kolaylaştırmak maksadıyla verilebilecek para ödüllerine, DNA verilerinin karşılaştırılmasına, kişilere ait eğitim kayıtlarının federal kurumlara açılmasına, federal kurumlar ile eyalet ve yerel kolluk kuvvetleri arasında koordinasyonun sağlanmasına ilişkin münferit düzenlemeler yer almaktadır.

ABD Vatanseverlik Yasası'nın beşinci bölümünde, siber güvenlik ile ilişkilendirilebilecek olan madde ve öngördüğü düzenlemeler şöyledir:

"Gizli Servis Yetkisinin Genişletilmesi" başlıklı 506.ncı madde ile Federal Ceza Kanunu değiştirilmek suretiyle;

1) Federal Ceza Kanununun 1030.ncu maddesinde yer alan bilgisayar bağlantılı dolandırıcılık suçları kapsamında ABD Gizli Servisine, bu konuda yetkilendirilmiş başka bir resmi kurum bulunması durumunda dahi, kendi soruşturmasını yürütme yetkisi verilmiş,

2) Federal Ceza Kanununun ilgili maddesi gereğince ABD Gizli Servisinin görev alanına giren suç vakaları haricinde; casusluk ve yabancı karşı istihbarat ile, ulusal savunma, dış ilişkiler veya "Yasak Veri *(Restricted Data)*"[22] gerekçeleriyle yetkisiz olarak açıklanmalarına karşı

[22] Yasak Veri *(Restricted Data)* teriminin tanımlanmış olduğu 1954 tarihli Atom Enerjisi Yasası'nda yer aldığı hali ile (NRC, 2002: 15);
"Yasak Veri terimi, aşağıdakilere ilişkin tüm veriler anlamına gelir; ancak 142.nci Bölüm kapsamında gizliliği kaldırılan veya Yasak Veri kategorisinden çıkartılan verileri kapsamaz:

koruma altına alınmış bilgilerle ilişkili olan her türlü "bilgisayar bağlantılı dolandırıcılık suçu"nda soruşturma yetkisi öncelikli olarak FBI'ya verilmiş,

3) ABD Gizli Servisinin arayabileceği ve tutuklayabileceği kişilere ilişkin mevcut düzenleme genişletilerek; *"erişim aracı dolandırıcılığı (access device fraud)*[23]*, sahte kimlik belgesi veya cihazları, federal olarak sigortalanmış herhangi bir mali kurum içerisindeki veya o kuruma yönelik her türlü dolandırıcılık, suç eylemi veya yasadışı eylem"* bahse konu arama ve tutuklama yetkisinin kapsamına dahil edilmiştir.

e. Altıncı Bölüm: Terörizm Kurbanlarına, Kamu Güvenliği Görevlilerine ve Ailelerine Sağlanan İmkânlar

Bu bölüm içerisinde yer alan düzenlemeler ile; terör eylemleri kurbanlarına, bu eylemlerden zarar gören kamu görevlilerine ve bunların ailelerine sağlanacak olan mali ve sosyal yardımlara ilişkin mevcut mevzuatta çeşitli iyileştirmeler yapılmıştır.

Altıncı bölüm içerisinde doğrudan siber güvenlik ile ilişkilendirilebilecek bir düzenleme bulunmamaktadır.

---

(1) Atomik silahların tasarım, üretim veya kullanımı,
(2) Özel nükleer materyalin üretimi -veya-
(3) Enerji üretiminde özel nükleer materyalin kullanımı."

[23] "Erişim Cihazı *(Access Device)*" ve "Sahte Erişim Cihazı *(Counterfeit Access Device)*"nın Federal Ceza Kanununun 1029.ncu maddesinde yer alan yasal tanımları şöyledir (Cornell [web], 2012a):
"(e) Bu kısımda kullanıldığı hali ile-
(1)Erişim Cihazı; para, mal, hizmet veya değerli herhangi bir başka şeyi elde etmek ya da -tümüyle kağıt kaynaklı bir transfer haricinde- bir fon transferi başlatmak üzere tek başına veya başka bir erişim cihazı ile birlikte kullanılabilen, her türlü kart, plaka, kod, hesap numarası, elektronik seri numarası, mobil tanımlama numarası, kişisel tanımlama numarası ya da diğer tanımlayıcı telekomünikasyon hizmet, ekipman veya cihazları veyahut hesap erişimi sağlayan diğer araçlar anlamına gelir.
(2) Sahte Erişim Cihazı; gerçek bir erişim cihazının her türlü taklit, hayali, tahrif edilmiş, sahte veya tanımlanabilir bileşeni ya da sahte bir erişim cihazı anlamına gelir."

f. Yedinci Bölüm: Kritik Altyapı Koruması İçin Arttırılmış Bilgi Paylaşımı

ABD Vatanseverlik Yasası'nın tek bir maddeden oluşan yedinci bölümü ile, 1968 tarihli Suç Kontrolü ve Asayişe İlişkin Çerçeve Yasa değiştirilmek suretiyle; özellikle birden fazla kolluk kuvvetinin yetki alanına giren terörist eylemlerin soruşturulmasında ve kovuşturulmasında işbirliğinin arttırılabilmesi için, kurumlar arasında emniyetli bilgi paylaşım sistemlerinin kurulması öngörülmüştür. Söz konusu düzenleme ile gerek federal, eyalet ve yerel seviyedeki kolluk kuvvetleri arasında, gerekse de aynı seviyede faaliyet gösteren kolluk kuvvetleri arasında işbirliği ve bilgi paylaşımının arttırılması amaçlanmıştır.

g. Sekizinci Bölüm: Terörizme Karşı Ceza Kanunlarının Güçlendirilmesi

ABD Vatanseverlik Yasası'nın sekizinci bölümü, "Siber Terörizm *(Cyberterrorism)*" ve "Siber Güvenlik *(Cybersecurity)*" kavramlarına doğrudan atıfın yapıldığı tek bölümdür. Daha önceki bölümlerde yer alan "siber suç" odaklı düzenlemeler ile karşılaştırıldığında, tehdit algısındaki değişimi de ortaya koyan bu terminoloji değişikliği oldukça önemlidir; zira bahse konu değişiklik ile, hem "Bilgisayar Dolandırıcılığı *(Computer Fraud)*" olgusundan "Siber Terörizm" olgusuna geçilmekte ve "Siber Uzay" bir gerçeklik olarak kabul edilmekte, hem de gerçekleşebilecek tehdidin olası ciddiyetine daha yoğun bir vurgu yapılmaktadır. Güvenlik tehdidini yaratacak kişilere ilişkin algıda da ciddi bir kaymaya işaret eden yine bu terminoloji değişikliği ile; "Dolandırıcılık *(Fraud)*" kavramının anlamı içerisinde örtülü olarak yer alan "kendisi lehine haksız mali çıkar sağlama" güdüsünün yerine, "Terörizm" kavramı ile oldukça açık bir şekilde ifade edilen "politik amaçlarla başkaları aleyhine zarar verme" güdüsü konulmaktadır. Böylelikle, her ikisi de yasadışı olan bahse konu olguların merkezinde ortak bir "araç" olarak bilgisayarların yer

almasına rağmen; gerek "amaç", gerekse de "sonuç" üzerinden ikili bir tehdit sınıflandırması yaratılmaktadır.

Sekizinci bölümde yer alan düzenlemeler hem siber güvenlik, hem de kritik altyapının korunması kapsamında, "sabotaj" tipi eylemlere odaklanmış olup; çalışmanın ilerleyen kısımlarında da ortaya konulacağı üzere, kritik altyapıya yönelik terörist saldırılar için oldukça ağır yaptırımlar öngörülmüştür. Bu kapsamda asıl kritik önemde olan husus ise; her hangi bir kritik altyapı tesisine yönelik yapılacak "bilgisayar tabanlı" her türlü girişimin siber sabotaj veya siber terör eylemi olarak kabul edilip edilemeyeceğidir.

Bahse konu yasanın bu bölümü ile ilgili olarak dikkati çeken bir diğer husus da, "siber sabotaj" olgusuna ilişkin olarak ortaya çıkan, güvenlik zaafiyeti yaratmamak adına kavramsal çerçevenin olabildiğince geniş çizilmesi kaygısına paralel bir biçimde; "siber suç" ve "siber terörizm" olgularının kavramsal çerçevelerinin çizilmesinde kritik önemde olan bazı olgu ve kavramların yasal tanımlarında, caydırıcılığı sağlamak adına bir takım değişikliklerin yapılmış olmasıdır. Bu kapsamda özellikle "Korunmuş Bilgisayar *(Protected Computer)*", "Zarar *(Damage)*" ve "Kayıp *(Loss)*" gibi kavramların yasal tanımlarında yapılan değişiklikler, dolaylı bir biçimde de olsa, suç veya tehdit kategorilerinin kavramsal çerçevelerinin çizilmesinde etkili olmaktadırlar.

ABD Vatanseverlik Yasası'nın sekizinci bölümünde, siber güvenlik ile ilişkilendirilebilecek olan maddeler ve öngördükleri düzenlemeler şöyle sıralanabilirler:

1) "Federal Suç Olarak Terörizmin Tanımı" başlıklı 808.nci madde ile; "Bilgisayar Dolandırıcılığı ve İstismarı"na ilişkin olarak Federal Ceza Kanununda yer alan bazı hükümlerin ihlal edildiği durumlar ve diğer pek çok federal suç, "Federal Terörizm Suçu"[24] kapsamına dahil edilmiştir.

---

[24] "Federal Terörizm Suçu *(Federal Crime of Terrorism)*"nun Federal Ceza Kanununun 2332B.nci maddesinde yer alan yasal tanımı şöyledir (Cornell [web], 2012ç):
"(5) 'Federal Terörizm Suçu' terimi bir suç eylemi anlamına gelir ki-
(A) Yıldırmak, zorlamak veya hükümet idaresine misilleme yapmak suretiyle hükümetin davranışlarına tesir etmek veya onu etki altına almak maksadıyla tasarlanır, ve
(B) Aşağıdakilerin bir ihlalidir-..."

Bu düzenleme sonrasında, Federal Ceza Kanununun 1030.ncu maddesinde sayılmış olan aşağıdaki eylemlerin Federal Terörizm Suçu kapsamında değerlendirilmesi de mümkün hale gelmiştir. Bu çerçevede, bahse konu eylemlere ilişkin olarak aşağıda yer verilen hükümler Federal Ceza Kanununun 1030.ncu maddesinden alıntılanmış olmakla birlikte, inceleme, karşılaştırma ve anlayış kolaylığı sağlamak maksadıyla; hem kendi içerisinde yeniden listelenmiş ve numaralandırılmış, hem de orijinal kanun metninde suçluya yönelik olan vurgu, suç eylemi üzerine kaydırılmıştır.

Bu bağlamda ABD Vatanseverlik Yasası'nın 808.nci maddesi ile yapılan düzenlemenin ardından federal terörizm suçunun kapsamı içerisine alınmış olan eylemler şöyle tasnif edilebilirler:

a) Bir bilgisayara bilerek ve yetkisiz olarak veya erişim yetkisini aşarak erişim sağlamak ve bu suretle elde etmiş olduğu; elde edilmeleri durumunda ABD'ye zarar vereceğine veya herhangi yabancı bir millete avantaj sağlayacağına inanılması nedeniyle ulusal savunma, dış ilişkiler veya "Yasak Veri" gerekçeleriyle ABD hükümeti tarafından bir idari emir veya tüzüğe dayanılarak yetkisiz olarak ifşa edilmelerine karşı koruma altına alınmış olan bilgileri, isteyerek;

i) Onları almakla yetkilendirilmemiş herhangi bir kişiye iletmek, göndermek, aktarmak, ya da iletilmesine, gönderilmesine veya aktarılmasına sebep olmak -ya da-,

ii) Onları almakla yetkilendirilmemiş herhangi bir kişiye iletmeye, göndermeye veya aktarmaya kalkışmak ya da böyle bir girişime sebep olmak -ya da-,

iii) Elinde bulundurmak ve onları almakla yetkilendirilmiş ABD çalışanlarına ya da görevlilerine teslim etmeyi kasten ihmal etmek.

b) Korunmuş bir bilgisayara bilerek bir program, bilgi, kod veya komutun iletilmesine neden olmak ve bu davranışının sonucunda

korunmuş bilgisayarda yetkisiz ve kasıtlı olarak "zarar"a[25] sebebiyet vermek suretiyle;

i) Bir veya daha fazla kişinin tıbbi muayene, tanı, tedavi veya bakımında, fiilen veya potansiyel olarak değişiklik ya da bozulmaya neden olmak,

ii) Herhangi bir kişinin fiziksel yaralanmasına neden olmak,

iii) Kamu sağlığına ve güvenliğine yönelik bir tehdite neden olmak,

iv) Ulusal güvenlik, ulusal savunma veya adalet idarelerinin devamlılığını sağlamak üzere ABD hükümeti veya onun bir kurumu tarafından kullanılan bir bilgisayarı etkileyen zarar vermek,

v) Herhangi bir 1 yıllık süre içerisinde 10 veya daha fazla korunmuş bilgisayarı etkileyen zarar vermek.

c) Kasten veya kötü niyetli olarak, iletişim hatlarının, istasyonlarının veya sistemlerinin imhası maksadıyla;

i) ABD tarafından kontrol edilen veya işletilen her türlü telsiz, telgraf, telefon, kablo, hat, istasyon, sistem veya diğer iletişim araçları ile, ABD'nin askeri veya sivil savunma fonksiyonları için kullanılan veya kullanılması amaçlanan inşa edilmiş ya da inşa edilmekte olan her türlü tesis, mülk veya malzemeye zarar vermek veyahut yoketmek,

ii) Bu gibi hatların veya sistemlerin çalışmasına ya da kullanılmasına her ne şekilde olursa olsun müdahale etmek veyahut bu gibi hatlar ya da sistemler üzerinden aktarılan her türlü iletişimin aktarımını engellenmek, yavaşlatmak veya geciktirmek.

---

[25] Zarar *(Damage)* kavramının, Federal Ceza Kanununun 1030.ncu maddesinde yer alan yasal tanımı şöyledir (Cornell [web], 2012b):
"(e) Bu kısımda kullanıldığı hali ile-
(8)"Zarar" terimi; bir program, sistem, bilgi veya verinin kullanılabilirliği ya da bütünlüğündeki herhangi bir bozulma anlamına gelir."

2) "Belirli Terörizm Suçları için Zamanaşımı Olmaması" başlıklı 809.ncu madde kapsamında yapılan düzenlemeler ile;

a) Federal Ceza Kanununda, ölüm cezasını gerektiren suçlar hariç tutulmak üzere, genel olarak öngörülmüş olan 5 yıllık zamanaşımı süresi, ölüm cezasını gerektirenler hariç olmak üzere terörizm suçları için 8 yıla çıkartılmaktadır. Düzenlemeye göre; federal terörizm suçlarının da arasında yer aldığı bazı suçlarda, suçun işlenmesinin ardından geçecek 8 yıl içerisinde suça ilişkin iddianamenin kurulamaması veya "Büyük Jüri (Grand Jury)"[26] yargılaması yapılmamış olması durumunda, bahse konu suça ilişkin olarak kovuşturma, yargılama ve cezalandırma yapılamayacaktır.

b) Federal terörizm kapsamında yer alan suçların işlenmesi sırasında, başka bir kişinin ciddi fiziksel yaralanmasına veya ölümüne neden olunması ya da bariz bir şekilde böyle bir tehlikenin yaratılması durumunda; herhangi bir zaman aşımı süresi olmaksızın, her zaman için suça ilişkin iddianame kurulabilmesine veya Büyük Jüri yargılaması yapılabilmesine olanak sağlanmaktadır.

c) Bu madde kapsamında yapılan değişikliklerin, maddenin yürürlük tarihinden önce veya sonra işlenmiş olan suçlara uygulanmasına imkan tanınmaktadır.

3) "Terörist Komplolar için Cezalar" başlıklı 811.nci madde ile; "federal terörizm suçu" kapsamında yer alan, iletişim hatlarına, istasyonlarına veya sistemlerine zarar verilmesi ya da imhasına yönelik eylemlere ilişkin olarak, daha önceden Federal Ceza Kanununda bulunan *"...kasten ve artniyetli olarak zarar verme veya imha etme girişimi..."* ibaresi çıkartılarak yerine *"...bu gibi maksatlarla girişimde bulunmak veya komplo kurmak..."* ibaresi getirilmiştir. Bu suretle, bahse konu eylemler de "zarar suçu"ndan "tehlike suçu" haline dönüştürülmüş olmaktadır.

---

[26] "Büyük Jüri *(Grand Jury)*"; en az 16, en fazla 23 üyeden meydana gelmektedir(Dayton [web], 2003a). Oluşturulmasına ilişkin prosedür ve şekil yönünden "Dava Jürisi *(Trial Jury)*" ile benzerlikler gösteren "Büyük Jüri", bazı yönlerden ise "Dava Jürisi"nden farklılaşmaktadır. Özellikle çalışma biçimi ve görevleri bakımından ortaya çıkan bu farklılıklar içerisinde en önemli olanı; Büyük Jüri yargılamasının, bir kişinin kendisine isnat edilen suçlardan suçlu olup olmadığına karar verilmesine yönelik olmayıp, kişinin bir suçtan yargılanıp yargılanmaması gerektiğine dair karar verilmesine yönelik olmasıdır(Dayton [web], 2003b).

4) "Teröristlerin Tahliye Sonrası Denetlenmeleri" başlıklı 812.nci madde ile; federal terörizm suçları için öngörülebilecek şartlı tahliye denetim süresinin, bahse konu suç işlenirken başka bir kişinin ciddi fiziksel yaralanmasına veya ölümüne neden olunmasına ya da bariz bir şekilde böyle bir tehlikenin yaratılmış olmasına bağlı olarak tespit edilmesi öngörülmektedir. Bu çerçevede bahse konu denetim sürelerinin, "her hangi bir süre için" veya "ömür boyu" olarak belirlenebilmesine de imkan tanınmıştır.[27]

5) "Terörizm Eylemlerinin Haraç Faaliyeti Kapsamına Alınması" başlıklı 813.ncü madde ile; federal terörizm suçu kapsamındaki eylemler aynı zamanda "haraç/şantaj faaliyetleri"nin[28] de kapsamı içerisine alınmıştır.

Bu madde ile yapılan değişikliğin amacının, çıkar amaçlı suçlar ve bunlardan sağlanan gelirler ile terörizm arasındaki muhtemel finansal bağa vurgu yapılması olduğunu ileri sürmek mümkün ise de, eleştirel bir bakış açısı ile ele alındığı zaman; bu madde ile yapılan değişikliğin asıl amacının, yasaların sağladığı diğer yetkilerin yetersiz kaldığı durumlarda, şüpheli olarak değerlendirilen kişilerin veya eylemlerin takip edilebilmelerini sağlamak maksadıyla, federal terörizm suçu kapsamındaki eylemler ile organize suç eylemlerinin ilişkilendirilmesi için uygun zeminin sağlanması olduğunu da savunmak mümkündür.

6) "Siber Terörizmin Caydırılması ve Önlenmesi" başlıklı 814.ncü madde ile; Federal Ceza kanununda "bilgisayar ile bağlantılı dolandırıcılık ve ilişkili faaliyet" başlığı altında düzenlenmiş olan suçlara

---

[27] "Şartlı Tahliye Sonrası Denetim Süreleri *(Authorized Terms of Supervised Release)*"ne ilişkin olarak, Federal Ceza Kanununun 3583.ncü maddesinde öngörülen düzenleme şöyledir (Cornell [web], 2012e):
*"(b)**Yetkilendirilmiş Denetim Süreleri.** -Aksi belirtilmediği takdirde, yetkilendirilmiş denetim süreleri şöyledir-*
(1)A Sınıfı veya B Sınıfı bir suç (felony) için, beş yıldan çok olmamak üzere;
(2)C Sınıfı veya D Sınıfı bir suç (felony) için, üç yıldan çok olmamak üzere;
(3)E Sınıfı bir suç (felony) veya –bir kabahat haricinde kalan- bir basit suç (Misdemeanor) için, bir yıldan çok olmamak üzere.

[28] "Haraç/Şantaj Faaliyeti *(Racketeering Activity)*"; Federal Ceza Kanununun 96.ncı Bölümü *(United States Code: Title 18 Chapter 96 - Racketeer Influenced and Corrupt Organizations)* 1961.nci maddesinde ayrıntılı bir biçimde tanımlanmış ve bahse konu bölüm altında da oldukça kapsamlı bir biçimde düzenlenmiştir. Bu çerçevede "Racketeering Activity" terimi genellikle, haraç ve şantaj eylemlerinin organize suç kapsamında değerlendirilebilecek biçimleri için kullanılmaktadır. Nitekim tek bir yasal düzenlemeden oluşmamasına rağmen, Federal Ceza Kanununun söz konusu bölümü *"RICO Act"* ya da *"RICO Laws"* olarak da bilinmekte olup, pek çok açıdan bir organize suçlarla mücadele mevzuatı niteliği göstermektedir.

verilecek cezalar ağırlaştırılmış, korunmuş bilgisayarlara yönelik eylemlerin kapsamı netleştirilmiş ve kanunda yer alan tanımlar kısmında bazı değişiklik ve ilaveler yapılmıştır. Bu kapsamda;

a) Korunmuş bilgisayarlara karşı girişilen veya gerçekleştirilen yasadışı eylemlerden doğan zarar ve oluşan kayba ilişkin olarak aşağıdaki şartlar getirilmiştir:

i) Bir veya daha fazla kişinin her hangi bir -1- yıllık süre içerisinde, toplamda en az 5.000 ABD Doları kayba uğraması,

ii) Bir veya daha fazla kişinin tıbbi muayene, tanı, tedavi veya bakımında fiilen veya potansiyel olarak değişiklik ya da bozulmaya neden olunması,

iii) Herhangi bir kişinin fiziksel yaralanmasına neden olunması,

iv) Kamu sağlığına ve güvenliğine yönelik bir tehdide neden olunması,

v) Ulusal güvenlik, ulusal savunma veya adalet idarelerinin devamlılığında ABD hükümeti veya onun bir kurumu tarafından kullanılan bir bilgisayar sistemini etkileyen zarar verilmesi.

b) Para veya başka bir değerin elde edilmesi maksadıyla, korunan bilgisayarlara yönelik olarak iletişim yolu ile işlenilebilecek gasp suçlarının mağdurları arasında sayılan "şirket, kuruluş, eğitim kurumu, finansal kurum, hükümet kurumu veya diğer tüzel kişi" ifadeleri Federal Ceza Kanununun ilgili maddesinden çıkartılmıştır. Bu değişiklik sonrasında kanun metninde yalnızca "kişi *(person)*" ifadesi kalmıştır.

c) Federal Ceza Kanununda yer alan cezalar aşağıdaki şekilde ağırlaştırılmıştır:

i) Ticari avantaj veya mali çıkar sağlamak, bir suçu veya haksız fiili gerçekleştirmek ya da değeri 5.000 ABD Dolarını aşan bilgiyi elde etmek maksadıyla; atıf yapılan kanunlarda belirtilen mali

kurumlardan, herhangi bir federal bakanlık veya kurumdan ya da herhangi korunmuş bir bilgisayardan bilgi almak üzere bir bilgisayara yetkisiz olarak veya yetki aşımı yapılarak erişilmesi durumunda, teşebbüs hali de Federal Ceza Kanunu kapsamında cezalandırılacaktır.

ii) Korunmuş bir bilgisayara bilerek bir program, bilgi, kod veya komutun iletilmesine neden olunduğu ve bu davranışın sonucunda da korunmuş bilgisayarda kasıtlı ve yetkisiz olarak zarara sebebiyet verildiği ya da böyle bir suça teşebbüs edilmesi durumunda; para cezasına, 10 yıldan fazla olmamak üzere hapis cezasına ya da her ikisine birden hükmedilebilecektir.

iii) Korunmuş bir bilgisayara kasıtlı ve yetkisiz olarak erişildiği ve bu davranışın sonucunda da "tedbirsizce" bir zarara sebebiyet verildiği ya da böyle bir suça teşebbüs edildiği durumlarda; para cezasına, 5 yıldan fazla olmamak üzere hapis cezasına ya da her ikisine birden hükmedilebilecektir.

iv) Yukarıda yer alan (ii) ve (iii) alt başlıklarında yer alan suçların işlendiği vakalarda, "bilgisayar ile bağlantılı dolandırıcılık ve ilişkili faaliyet" kapsamında yer alan diğer suçlardan da daha önceden ceza alınmış olması durumunda ise; para cezasına, 20 yıldan fazla olmamak üzere hapis cezasına ya da her ikisine birden hükmedilebilecektir.

c) Federal Ceza Kanununda yer alan, "bilgisayar ile bağlantılı dolandırıcılık ve ilişkili faaliyet"'e ilişkin kavramların tanımlarında aşağıdaki değişiklikler ve ilaveler yapılmıştır.

i) "Korunmuş Bilgisayar *(Protected Computer)*" tanımı içerisinde yer alan; eyaletlerarası veya yurtdışı ticaret ya da iletişimde kullanılan veyahut etkileyen bilgisayarlardan, ABD sınırları dışında bulunanlar da bu tanımın kapsamına dahil edilmişlerdir.

ii) "Zarar *(Damage)*" terimi; *"bir program, sistem, bilgi veya verinin kullanılabilirliği ya da bütünlüğündeki herhangi bir bozulma"* olarak tanımlanmıştır.

iii) "Mahkumiyet *(Conviction)*" terimi; unsurları arasında "bir bilgisayara yetkisiz olarak veya yetki aşımı ile erişimin" de bulunduğu, herhangi bir eyalet hukukuna göre 1 yıldan fazla süreli hapis cezası ile cezalandırılmayı gerektiren suçlardan alınan mahkumiyetleri kapsayacak şekilde tanımlanmıştır.

iv) "Kayıp *(Loss)*" terimi; *"herhangi bir kurban için, suça karşı koyabilmeye, hasar tespiti yaptırmaya ve veri, program, sistem veya bilginin suçun işlenmesinden önceki haline döndürülmesine ilişkin olanların yanısıra, her türlü gelir kaybı ve yapılan -zorunlu- masraflar ile hizmet kesilmesi nedeniyle katlanılmak zorunda kalınan diğer dolaylı zararları da içerecek biçimde, her türlü makul maliyet"* olarak tanımlanmıştır.

v) "Kişi *(Person)*" terimi; *"herhangi bir gerçek kişi, firma, şirket, eğitim kurumu, mali kurum, devlet kurumu, tüzel kişi ya da diğer bir mevcudiyet"* olarak tanımlanmıştır.

d) "Bilgisayar ile bağlantılı dolandırıcılık ve ilişkili faaliyet" kapsamında işlenen suçların sonucunda uğranılan zararların giderilmesi için özel hukuk yoluna başvurulmasına ilişkin olarak ise aşağıdaki şartlar öngörülmüştür:

i) Özel hukuk yoluna ancak, söz konusu davranışın aşağıdaki durumlardan birini içermesi halinde başvurulabilecektir:

(1) Bir veya daha fazla kişinin her hangi bir -1- yıllık süre içerisinde, toplamda en az 5.000 ABD Doları kayba uğraması,

(2) Bir veya daha fazla kişinin tıbbi muayene, tanı, tedavi veya bakımında fiilen veya potansiyel olarak değişiklik ya da bozulmaya neden olunması,

(3) Herhangi bir kişinin fiziksel yaralanmasına neden olunması,

(4) Kamu sağlığına ve güvenliğine yönelik bir tehdite neden olunması,

(5) Ulusal güvenlik, ulusal savunma veya adalet idarelerinin devamlılığında ABD hükümeti veya onun bir kurumu tarafından kullanılan bir bilgisayarı etkileyen zarar verilmesi.

ii) Sadece bir veya daha fazla kişinin her hangi bir -1- yıllık süre içerisinde, toplamda en az 5000 ABD Doları kayba uğradığı durumlarda ise, ancak uğranılan ekonomik -maddi- zararlara ilişkin olarak özel hukuk yoluna başvurulabilecektir.

iii) Bilgisayar donanımının, gömülü yazılımın veya bilgisayar yazılımının tasarım ya da üretimindeki ihmallere ilişkin olarak bu düzenlemelere dayanılarak özel hukuk yoluna başvurulamayacaktır.

e) ABD Ceza Komisyonu[29], "bilgisayar ile bağlantılı dolandırıcılık ve ilişkili faaliyet" suçu kapsamında mahkum olan kişilerin çarptırılmış oldukları hapis cezasının zorunlu asgari süresine bakılmaksızın uygun cezalara tabi tutulabilmeleri için, federal ceza talimatnamelerinde gerekli değişiklikleri yapmak ile görevlendirilmiştir.

7) "Siber Güvenlik Adli Kabiliyetlerinin Geliştirilmesi ve Desteklenmesi" başlıklı 816.ncı madde ile;

a) Adalet Bakanına, mevcut adli bilişim laboratuvarlarını desteklemek ve aşağıdaki kabiliyetlere sahip olmalarını sağlamak üzere, uygun olduğunu değerlendirdiğinde, bölgesel adli bilişim laboratuvarları kurma yetkisi verilmiştir:

> "(1) Suç eylemi (siber terörizm dahil) ile ilişkili olarak ele geçirilmiş veya tespit edilmiş olan 'bilgisayar kanıtı' üzerinde güvenilir adli incelemeler yapmak,

[29] ABD Ceza Komisyonu *(United States Sentencing Commission - USSC)*; 1984 tarihli Kapsamlı Suç Kontrolü Yasası *(Comprehensive Crime Control Act of 1984)*'nın ceza reformu hükümleri çerçevesinde oluşturulmuştur. ABD Hükümetinin hukuk kolundaki bağımsız bir teşkilat olan bahse konu komisyonun; federal mahkemeler için cezalandırma politikaları ve uygulamaları oluşturulması, etkin ve verimli bir suç politikasının geliştirilmesine yardım etmek, federal suç ve cezalar üzerine değerlendirme ve araştırmalar yapmak gibi bir dizi görevi bulunmaktadır (USSC [web], 2012).

(2) Bilgisayar bağlantılı suç (siber terörizm dahil) soruşturmalarına, adli tıp analizlerine ve kovuşturmalarına ilişkin olarak federal, eyalet ve yerel kolluk kuvvetleri personeline ve savcılara eğitim ve öğretim vermek,

(3) Bilgisayar bağlantılı suç ile ilişkili federal, eyalet veya yerel ceza kanunlarının uygulanmasında federal, eyalet ve yerel kolluk kuvvetlerine yardımcı olmak,

(4) Karma görev kuvvetlerinin kullanımı da dahil olmak üzere, bilgisayar bağlantılı suçun soruşturulması, analizi ve kovuşturması hakkındaki federal kolluk bilgisi ve uzmanlığının, eyalet ve yerel kolluk kuvveti personeli ve savcılar ile paylaşılmasını kolaylaştırmak ve teşvik etmek, ve

(5) Adalet Bakanının uygun göreceği diğer faaliyetleri ifa etmek."

b) Bu maddenin gereklerinin yerine getirilebilmesi maksadıyla, her mali yıl için 50 Milyon ABD Dolarlık bir kaynağın tahsis edilmesi uygun görülmüştür.

ğ. Dokuzuncu Bölüm: Geliştirilmiş İstihbarat

ABD Vatanseverlik Yasası'nın dokuzuncu bölümünde yer alan düzenlemeler ile çeşitli kanunlarda değişiklik yapılmak suretiyle; ulusal güvenlik kapsamında değerlendirilen "yabancı ülke istihbarat faaliyetlerinin izlenmesi"ne yönelik istihbarat kapasitesinden ve bahse konu faaliyetlere ilişkin istihbarat bilgilerinden, terörizm ile mücadelede ve ilişkili suç soruşturmalarında da etkin bir biçimde faydalanılması amaçlanmaktadır. Bu çerçevede özellikle Adalet Bakanı ile Merkezi İstihbarat Direktörü[30] arasında yakın ve karşılıklı işbirliği yapılması öngörülmüştür.

Dokuzuncu bölüm içerisinde doğrudan siber güvenlik ile ilişkilendirilebilecek bir düzenleme bulunmamaktadır.

[30] Ulusal İstihbarat Direktörü *(Director of Central Intelligence - DCI)*; 2004 yılında hayata geçirilen İstihbarat Reformu öncesindeki dönemde, ABD İstihbarat Topluluğunun başıdır. Aynı zamanda CIA Başkanı da olan Merkezi İstihbarat Direktörü, İstihbarat Reformu sonrasında yerini Ulusal İstihbarat Direktörü (DNI)'ne bırakmıştır.

h. Onuncu Bölüm: Münferit Düzenlemeler

ABD Vatanseverlik Yasası'nın onuncu bölümünde, esas itibariyle terörle mücadele ile doğrudan ilgili olmadığı değerlendirilerek önceki hiçbir bölüme dahil edilmeyen ya da bu kanun ile alınması öngörülen tedbirlerin uygulanmalarına yönelik programlara ve bunların mali kaynaklarına ilişkin hükümler içeren münferit düzenlemeler yer almaktadır.

Bununla birlikte onuncu bölümün, hem ABD Vatanseverlik Yasası, hem de ABD'deki siber güvenlik algısı ve politikaları bakımından önemi büyüktür. Zira gerek enformasyon devrimine ve bilgi teknolojilerindeki gelişmelere keskin bir vurgunun yapıldığı, gerekse de kritik altyapının korunmasına ilişkin en ciddi düzenlemelerin yer aldığı 1016.ncı madde; ironik bir biçimde, hem onuncu bölümün, hem de ABD Vatanseverlik Yasası'ın son maddesidir.

Onuncu bölüm içerisinde, siber güvenlik ile ilişkilendirilebilecek olan maddeler ve öngördükleri düzenlemeler şöyle sıralanabilirler:

1) "Elektronik Gözetimin Tanımlanması" başlıklı 1003.ncü madde ile; FISA'da, *"ABD'de bulunan bir kişiye gelen veya o kişiden giden telli iletişimin içeriğinin, -ki tespitin ABD topraklarında yapılması durumunda taraflardan herhangi birinin izni gerekmeksizin- elektronik, mekanik veya diğer gözetim cihazları vasıtası ile elde edilmesi"* olarak tanımlanan "elektronik gözetim"[31] teriminin yasal tanımında ve kapsamında değişiklik yapılmıştır. Yeni düzenlemeye göre; Federal Ceza Kanunu gereğince belirli şartların oluşması halinde yasal kabul edilmiş olan, bilgisayar ihlalcisinin yürüttüğü iletişime ilişkin olarak yetki aşımına

[31] "Elektronik Gözetim *(Electronic Surveillance)*"; Federal Kanunlar Külliyatının 50.nci Başlığı *(United States Code: Title 50 – War and National Defense)* 1801.nci maddesinde ayrıntılı bir biçimde tanımlanmıştır. Bahse konu gözetim faaliyetleri esas itibari ile, yabancı istihbarat faaliyetlerinin takip edilmesi *(foreign intelligence surveillance)* kapsamında değerlendirilmektedirler.

dayalı yapılmış tespitler[32] elektronik gözetimin kapsamı dışında yer almaktadır.

2) "İlk Müdahalecilere Destek Yasası" başlıklı 1005.nci madde ile; terör eylemlerinin önlenebilmesi maksadıyla eyalet ve yerel kolluk kuvvetlerine karşılıksız yardım yapılması öngörülmekte ve bu hususta Adalet Bakanı yetkilendirilmektedir. Bahse konu yardımların terörizm ile mücadele projeleri ve programlarının yanı sıra teknoloji ve ekipman tedarikine harcanabilmesi de mümkündür.

3) "Kritik Altyapıların Korunması" başlıklı 1016.ncı madde ile; öncelikle "kritik altyapı koruması *(critical infrastructure protection)*"na ilişkin durum tespitinde bulunulmakta, ardından ABD'nin kritik altyapının korunmasına yönelik politikası ilan edilmekte ve nihai olarak da kritik altyapı güvenliğinin sağlanması maksadıyla analiz faaliyetleri yürütecek olan "Ulusal Altyapı Simülasyon ve Analiz Merkezi (NISAC)"nin kurulması öngörülmektedir. Bu madde aynı zamanda "2001 tarihli Kritik Altyapıların Korunması Yasası (CIPA)" olarak da anılmakta olup; bahse konu madde/kanun kapsamında ABD Kongresi aşağıdaki tespitlerde bulunmuştur:

> "(1) Enformasyon devrimi, ticari davranışları ve hükümetin çalışma biçimlerini olduğu kadar ABD'nin ulusal güvenlik ve savunmasının dayandığı altyapıları da dönüştürmüştür.
>
> (2) Özel teşebbüs, hükümet ve ulusal güvenlik aygıtları artan bir şekilde, aralarında telekomünikasyon, enerji, mali hizmetler, su ve ulaştırma sektörlerinin de bulunduğu, kritik fiziksel ve enformasyon altyapılarının oluşturduğu karşılıklı bağımlı bir ağa dayanmaktadır.
>
> (3) ABD'nin ulusal savunmasının, hükümet devamlılığının, ekonomik refahının ve yaşam kalitesinin muhafaza edilmesi için kritik önemde olan fiziksel ve siber altyapı hizmetlerinin güvenilir bir şekilde verilmesini sağlamak için kesintisiz bir ulusal çaba gereklidir.
>
> (4) Bu ulusal çaba; gerek bahse konu karmaşık ve karşılıklı bağımlı sistemlerin istikrarını temin etmek için gerekli mekanizmaları takdir

[32] "Yetki Aşımı *(Abuse of color of law)*" kapsamında değerlendirilmekte olan bahse konu tespitlerin yasal kabul edilebilmeleri için yerine getirilmesi gereken şartlar, ABD Vatanseverlik Yasası'nın "Bilgisayara Yetkisiz Erişimin Tespiti" başlıklı 217.nci maddesinde düzenlenmiştir.

etmek, gerekse de politika önerilerine destek vermek suretiyle ulusun kritik altyapısına yeterli koruma ve sürekli canlılık sağlamak maksadıyla analitik kabiliyetleri ve kapsamlı modellemeyi gerektirmektedir."

Yine bu madde kapsamında ABD Kongresi tarafından ifade edildiği üzere; ABD'nin kritik altyapının korunmasına yönelik politikası şöyledir:

"(1) ABD kritik altyapısının işleyişindeki herhangi bir fiziksel veya sanal kesilmenin; nadir, kısa, etkisi coğrafi olarak sınırlı, yönetilebilir ve ekonomi, sosyal hizmetler, devlet hizmetleri ve ulusal güvenlik üzerindeki zararlarının asgari seviyede olması.

(2) Yukarıda belirtilen politika hedefine ulaşmak için gerekli faaliyetlerin, tüzel kişilerin ve hükümet dışı örgütlerin de dahil edilmeleri ile, bir kamu-özel sektör ortaklığı çerçevesinde yerine getirilmesi.

(3) Federal hükümetin temel fonksiyonlarının devamlılığını her türlü koşul altında sağlamak için, kapsamlı ve etkili bir programı yürürlükte bulundurmak."

3. İÇ GÜVENLİK YASASI *(HOMELAND SECURITY ACT)*

Çalışmanın bu kısmında ayrıntılı bir şekilde incelenecek olan, tam adı ile "*Homeland Security Act of 2002*" ve yaygın biçimde kullanılan kısaltması ile "HSA" isimli kanun; esas itibariyle, 11 Eylül Saldırıları sonrasında ülke içi asimetrik tehditlerle mücadele ihtiyacını karşılamak üzere kurulan ve bu dönemdeki güvenlik yapılanmasının omurgasını oluşturan ABD İç Güvenlik Bakanlığı *(Department of Homeland Security)*'nın kuruluş ve teşkilat yasası niteliğindedir.

Bu temel niteliğinin yanı sıra siber güvenlik ile yakından ilişkili olan diğer iki yasayı da bünyesinde barındırması nedeniyle çalışmanın bu kısmında ele alınmış olan İç Güvenlik Yasası, şeklen ABD Vatanseverlik Yasası'ndan daha farklı bir biçimde incelenecektir. Zira yukarıda da ifade edildiği üzere bir kuruluş ve teşkilat yasası niteliğinde olması, İç Güvenlik Yasasının bir bütün olarak ele alınmasını, incelenmesini ve anlaşılmasını

oldukça zorlaştırmaktadır. Bu çerçevede İç Güvenlik Yasası içerisinde yer alan "2002 tarihli Siber Güvenliğin Geliştirilmesi Yasası *(Cyber Security Enhancement Act of 2002)*" ve "2002 tarihli Federal Enformasyon Güvenliği Yönetimi Yasası *(Federal Information Security Management Act of 2002)*" ayrıntılı bir biçimde ele alınırken; birçoğu İç Güvenlik Bakanlığının teşkilatlanmasına ilişkin olan diğer hükümlere, yalnızca asimetrik tehdit bağlamında siber güvenlik ile ilişkili olmaları durumunda yer verilecektir.

Bu çalışma kapsamında, ABD Kongre Kütüphanesi resmi internet sitesinden alınmış olan nihai kanun metni kullanılmış ve Cornell Üniversitesi Hukuk Fakültesi Yasal Bilgi Enstitüsü (LII) veritabanındaki Federal Kanunlar Kodifikasyonundan faydalanılmış olup; çalışmanın "İç Güvenlik Yasası Kapsamında Yer Alan Hükümler" isimli altbaşlığı kapsamında yer alan başlıkların isimlendirilmesinde ve sıralanmasında bahse konu yasanın orijinal metnine sadık kalınmıştır.

a. İç Güvenlik Yasası Kapsamında Yer Alan Hükümler

(1) Birinci Bölüm: İç Güvenlik Bakanlığı

İç Güvenlik Yasası'nın birinci bölümünde, İç Güvenlik Bakanlığının görevleri ve üst yönetim yapılanmasına ilişkin düzenlemeler yer almakta olup; bu kapsamda İç Güvenlik Bakanlığının asli görevlerine, "Yönetim Bölümü; Misyon" başlıklı 101.nci maddede yer verilmiştir.

Bu bölüm çerçevesinde yapılmış olan düzenlemelere ilişkin olarak genel bir değerlendirme yapıldığı zaman, aşağıda belirtilen hususlar özellikle dikkati çekmektedir:

- İç Güvenlik Bakanlığına bağlanmış olan kurumların, oluşturulan bu yeni ve devasa yapı içerisinde bir anlamda ezilmemeleri ya da eritilmemeleri gerektiğinin sürekli olarak vurgulanması,

- İç güvenliğin sağlanmasında özel sektör ile stratejik bir işbirliğinin kurulması ve yürütülmesi -ve bir anlamda özel sektörün temsil edilmesi- ile görevlendirilmiş olan, iç güvenlik bakanına bağlı bir "özel asistan" kadrosunun ihdas edilmesi.

İç Güvenlik Yasası'nın birinci bölümü içerisinde, özellikle asimetrik tehdit bağlamında siber güvenlik ile ilişkilendirilebilecek olan madde ve öngördüğü düzenlemeler şöyledir:

"Yönetim Bölümü; Misyon" başlıklı 101.nci madde ile; İç Güvenlik Bakanlığının görevleri aşağıdaki gibi sıralanmaktadır:

> "(A) ABD içerisinde terörist saldırıları önlemek,
>
> (B) ABD'nin terörizme karşı güvenlik açıklarını azaltmak,
>
> (C) ABD içerisinde meydana gelen terörist saldırıların zararlarını asgariye indirmek ve etkilerinin giderilmesine yardımcı olmak,
>
> (D) Doğal ve insanyapısı krizlerin yanı sıra acil durum planlamasına dair bir odak noktası olarak davranmak da dahil olmak üzere, kendisine bağlanan kurumların tüm fonksiyonlarını ifa etmek,
>
> (E) Bakanlık bünyesinde yeralan ve ülke güvenliği ile doğrudan ilişkili olmayan altbölümlerin veya kurumların, özel bir kongre yasasının varlığı haricinde, fonksiyonlarının azaltılmamasını veya ihmal edilmemesini sağlamak,
>
> (F) Ülke güvenliğini temin etmeyi amaçlayan çaba, eylem ve programlar tarafından azaltılmaksızın, ABD'nin ekonomik güvenliğini bir bütün olarak sağlamak, ve
>
> (G) Uyuşturucu kaçakçılığı ile terörizm arasındaki bağlantıları izlemek, bu gibi bağlantıları kesmeye yönelik çabaları koordine etmek ve uyuşturucu kaçakçılığını engellemeye yönelik çabalara farklı biçimlerde de katkıda bulunmak."

Bu kanun ile İç Güvenlik Bakanlığına bağlanmış olan kurumların yetkilerine ilişkin olarak da, yine aynı madde içerisinde yer alan diğer bir hükme göre; *"aksi durum kanunla özel bir şekilde ifade edilmedikçe, terörizm eylemlerinin soruşturulması ve kovuşturulmasında birincil sorumluluk İç Güvenlik Bakanlığında değil, bahse konu eylemlere*

ilişkin olarak yetkili olan federal, eyalet ve yerel kolluk kuvvetlerinde olacaktır."

(2) İkinci Bölüm: Enformasyon Analizi ve Altyapı Koruma

İç Güvenlik Yasası'nın, kritik altyapılara ilişkin bilgilerin güvenliğine ve işlenmesine odaklanmış olan ikinci bölümünde; çalışmanın ilerleyen kısımlarında incelenecek olan "2002 tarihli Siber Güvenliğin Geliştirilmesi Yasası *(Cyber Security Enhancement Act of 2002)*" haricinde, siber güvenlik ile ilişkilendirilebilecek olan maddeler ve öngördükleri düzenlemeler şöyle sıralanabilirler:

1) "Enformasyon Analizi ve Altyapı Koruma Direktörlüğü" başlıklı 201.nci madde ile; başında bir bakan yardımcısının bulunacağı, "Enformasyon Analizi ve Altyapı Koruma Direktörlüğü *(Information Analysis and Infrastructure Protection Directorate)*" kurulmaktadır. Söz konusu madde incelendiğinde bu direktörlüğün en önemli görevinin; terörizm tehdidini tespit etmek ve tanımlamak ile, kritik altyapıdaki güvenlik açıklarını belirlemek üzere kolluk ve istihbarat kurumları ile özel sektörün elindeki bilgilere erişmek, bunları toplamak ve analiz etmek olduğu görülmektedir. ABD'nin kritik altyapısını ve temel kaynaklarını korumak üzere kapsamlı bir ulusal plan geliştirilmesinin de bahse konu direktörlüğün görevleri arasında yer aldığının ifade edildiği aynı madde çerçevesinde; "*güç üretim ve dağıtım sistemleri, enformasyon ve (uydular dahi) iletişim sistemleri, elektronik mali sistemler, acil durum hazırlık iletişim sistemleri ve bu gibi sistemleri destekleyen fiziksel ve teknolojik unsurlar*" kritik altyapı kapsamında değerlendirilmektedirler.

Yine bahse konu madde ile; görevlerini yerine getirebilmesi maksadıyla Dışişleri Bakanlığı, CIA, FBI, NSA, NIMA[33], DIA ve diğer federal kurumlardan personelin direktörlük emrinde görevlendirilmesine

[33] *National Imagery and Mapping Agency* (Ulusal Görüntüleme ve Haritalama Teşkilatı). Sonradan NGA adını almıştır.

imkan tanınırken, aşağıdaki kurumlar da İç Güvenlik Bakanına bağlanmaktadır:

- Ulusal Altyapı Koruma Merkezi (NIPC); önceden FBI'ya bağlıdır.

- Ulusal İletişim Sistem Dairesi (NCS); önceden Savunma Bakanlığına bağlıdır.

- Kritik Altyapı Güvence Dairesi *(Critical Infrastructure Assurance Office)*; önceden Ticaret Bakanlığına bağlıdır.

- Ulusal Altyapı Simülasyon ve Analiz Merkezi (NISAC); önceden Enerji Bakanlığına bağlıdır.

- Federal Bilgisayar Olaylarına Müdahale Merkezi *(Federal Computer Incident Response Center)*; önceden ABD Genel Hizmetler İdaresi (GSA)'ne bağlıdır.

2) İkinci Bölüm içerisindeki 211.nci ve 215.nci maddeler arasında yer alan kısım, kritik altyapılara yönelik ihlallere ilişkin bilgilerin takip edilebilmesi maksadıyla kabul edilen "2002 tarihli Kritik Altyapı Bilgisi Yasası *(Critical Infrastructure Information Act of 2002)*"nı içermektedir.

Bahse konu kanun ile, kritik altyapı sistemlerine veya korunmuş sistemlere ilişkin belirli bazı bilgiler, "kritik altyapı bilgisi (critical infrastructure information)" olarak tanımlanmaktadır. Bu kapsamda;

- Suç niteliğindeki cari ve potansiyel müdahaleler ile müdahale tehditlerine ilişkin bilgiler,

- Sorunlara ve geliştirilen çözümlere ilişkin bilgiler,

- Müdahalelere direnme kabiliyetlerine ilişkin bilgiler, kritik altyapı bilgisi olarak kabul edilmektedir.

Bahse konu yasa kapsamında yer alan diğer düzenlemeler ise, kritik altyapı bilgilerinin toplanması, korunması ve kullanılmasına ilişkin esasları içermektedir.

3) "Federal Olmayan Siber Güvenliğin Geliştirilmesi" başlıklı 223.ncü madde ile; Enformasyon Analizi ve Altyapı Koruma Direktörü, kritik enformasyon sistemlerine sahip olan veya işleten eyalet ve yerel kamu kurumları -ve talep etmeleri durumunda özel sektör kurumları- ile kritik altyapı sistemlerinin güvenlik açıklarının yanı sıra bunlara yönelik tehdit ve saldırılara ilişkin analizleri paylaşmak, uyarılarda bulunmak ve kriz yönetimi desteği sağlamakla yükümlü kılınmaktadır.

4) "NET Guard" başlıklı 224.ncü madde ile; "NET Guard" adı altında, enformasyon sistemlerine ve iletişim ağlarına yapılan saldırılara müdahale etmek ve etkilerini gidermekte yerel halka yardımcı olmak üzere, yerel gönüllülerden oluşan bir "ulusal teknoloji muhafaza *(national technology guard)*" yapılanmasının hayata geçirilmesi hususunda Enformasyon Analizi ve Altyapı Koruma Direktörüne yetki verilmektedir.

5) İkinci bölümün "Bilim ve Teknoloji Dairesi" altbaşlığı altında yeralan, "Dairenin Kurulması; Direktör" başlıklı 231.nci madde ile; Adalet Bakanlığı bünyesinde faaliyet göstermek üzere "Bilim ve Teknoloji Dairesi *(Office of Science and Technology)*" kurulmaktadır. "Dairenin Görevi; Vazifeler" başlıklı 232.nci madde de ise, bahse konu dairenin görevleri ve bu görevlerin ifası sırasında yerine getireceği vazifeler yer almaktadır.

Bu kapsamda, *"kolluk hizmetleri teknolojisi*[34] *üzerine yapılan çalışmalarda ulusal odak noktası olarak hizmet etmek"* ve *"federal, eyalet ve yerel kolluk kuvvetlerine ekipman, eğitim ve teknik destek sağlanmasına yönelik programları yürütmek"* ile görevlendirilen söz konusu dairenin pek çok vazifesi arasında, siber güvenlik ile ilişkilendirilebilecek olanlar şöyledir:

> "(6) ....ilişkin alanlarda geliştirme, deneme, değerlendirme ve fayda-maliyet analizleri yürütmek;...(F) Soruşturmaları ve adli bilişimi de içermek üzere adli tıp çalışmalarını kolaylaştıran araç ve teknikler,

[34] İç Güvenlik Yasası'nın 233.ncü maddesinde yer alan tanımına göre;
"Kolluk Hizmetleri Teknolojisi (Law Enforcement Technology)" terimi, soruşturma ve adli tıp teknolojilerini, ceza teknolojilerini ve yargı sürecini destekleyen teknolojileri içerir.

(11) Siber suçlar ile mücadelede eyalet ve yerel kolluk kuvvetlerine yardımcı olmak üzere, ileri soruşturma analizleri ve adli bilişim araçlarına yönelik bir edinme, araştırma, geliştirme ve yaygınlaştırma programını yönetmek."

(3) Üçüncü Bölüm: İç Güvenliğin Desteklenmesinde Bilim ve Teknoloji

İç güvenliğin sağlanması kapsamında yürütülecek bilimsel ve teknolojik faaliyetleri düzenlemeye yönelik üçüncü bölüm içerisinde, özellikle asimetrik tehdit bağlamında siber güvenlik ile ilişkilendirilebilecek olan madde ve öngördüğü düzenleme şöyledir:

"İç Güvenlik İleri Araştırma Projeleri Kurumu" başlıklı 307.nci madde ile; "iç güvenlik araştırması *(homeland security research)*" terimi aşağıdaki biçimi ile tanımlanmakta ve bu gibi araştırmaları yürütmek üzere "İç Güvenlik İleri Araştırma Projeleri Kurumu *(Homeland Security Advenced Research Projects Agency - HSARPA)"* kurulmaktadır:

"(2) İÇ GÜVENLİK ARAŞTIRMASI.--İç güvenlik araştırması terimi, terör eylemleri başta olmak üzere iç güvenlik tehditlerinin tespit edilmesi, önlenmesi, bu tehditlerden korunulması, müdahale edilmesi ve etkilerinin giderilmesi ile ilgili araştırmalar anlamına gelir."

(4) Sekizinci Bölüm: Federal Olmayan Kuruluşlar ile Koordinasyon, Genel Müfettiş, ABD Gizli Servisi, Sahil Güvenlik, Genel Hükümler

İç Güvenlik Yasası'nın münferit düzenlemeleri içeren sekizinci bölümünde, siber güvenlik ile ilişkilendirilebilecek olan maddeler ve öngördükleri düzenlemeler şöyle sıralanabilirler:

1) "Aktarılan Görevler" başlıklı 821.nci madde ile; ABD Gizli Servisi (USSS), bakanlık içerisinde ayrı bir kurum olarak muhafaza edilmek şartıyla İç Güvenlik Bakanına bağlanmıştır.

Bu kapsamda, önceki dönemlerde sahtecilik ve dolandırıcılık suçlarına odaklanmış olan ABD Gizli Servisinin, ABD Vatanseverlik Yasası ile siber suçlara ilişkin görev ve yetkilerinin arttırılmasının ardından İç Güvenlik Yasası ile de İç Güvenlik Bakanlığına bağlanmış olması basit bir örgütsel değişikliğin ötesindedir. Zira bu durum, siber suçlara ilişkin olarak ABD'deki güvenlik algısında ortaya çıkan ve odak noktasının çıkar amaçlı suçlardan terör suçlarına kaydığı bir değişime de önemli bir örnek teşkil etmektedir.

2) "Askeri Faaliyetler" başlıklı 876.ncı madde ile; İç Güvenlik Yasası içerisinde yer alan hiçbir düzenlemenin savaş, ABD'nin askeri savunması veya diğer askeri faaliyetler bağlamında İç Güvenlik Bakanına herhangi bir yetki vermediği ve bahse konu faaliyetler bağlamında varolan yetkileri sınırlamadığı ifade edilmiştir.

3) "Posse Comitatus Yasası'nın Devam eden Önemi ve Geçerliliğinin Teyidine İlişkin Kongre Görüşü" başlıklı 886.ncı madde ile; "Anayasa veya Kongre tarafından yetkilendirilen durum ve şartlar" haricinde, kolluk hizmetlerini de içerecek biçimde "yasaları uygulamak" üzere Silahlı Kuvvetlerin kullanılmasını yasaklayan "Posse Comitatus Yasası *(Posse Comitatus Act)*"na[35] atıfta bulunulmaktadır. Bu çerçevede bahse konu kanunun geçerliliği ve önemi Kongre tarafından teyit edilmekte

---

[35] 1878 yılında kabul edilmiş olan *"Posse Comitatus Act"*e adını veren ve Latince bir terim olan *Posse Comitatus*; bir yönetim bölgesindeki kamu düzeninin korunmasına yardımcı olmak üzere göreve çağrılan ve o yönetim bölgesindeki fiziken elverişli vatandaşlardan meydana gelen, İlkçağ İngilteresi'ne özgü bir kurumdur (Encyclopedia Britannica Online [web], 2012). Posse Comitatus Act olarak anılan ve Federal Ceza Kanununun "Kara ve Hava Kuvvetlerinin Posse Comitatus Olarak Kullanımı" başlıklı 1385.nci maddesinde yer alan yasal düzenlemeye göre ise (Cornell [web], 2012c);
"Her kim ki, Anayasa veya Kongre tarafından açıkça yetkilendirilmiş vakalar ve şartlar haricinde, isteyerek Kara veya Hava Kuvvetlerinin herhangi kısmını yasaların uygulanması maksadıyla posse comitatus olarak ya da diğer bir şekilde kullanırsa; para cezası veya iki yıldan fazla olmamak üzere hapis cezası ya da her ikisi ile birden cezalandırılır."
Elsea'nın, ABD Kongresine sunduğu raporunda da ifade ettiği üzere; *Posse Comitatus Act*, Kara ve Hava Kuvvetleri haricinde kalan kuvvetlere ilişkin olarak "sessiz"dir. Dolayısı ile, Deniz Kuvvetlerinin, Deniz Piyadelerinin, Sahil Güvenliğin ve -bir milis kuvveti olarak- Ulusal Muhafızların kullanılabileceği durumları doğrudan kapsamamaktadır. Mahkemelerin genellikle, bahse konu kanunun kendiliğinden Deniz Kuvvetlerine ve Deniz Piyadelerine ilişkin olarak uygulanamayacağını kabul ettiklerini ifade eden Elsea; ancak mahkemelerin söz konusu kuvvetlerin sınırlandırıcı mahiyetteki benzeri nitelikteki diğer idari ve yasal düzenlemelerin kapsamı içerisinde yer aldıklarına ilişkin bir görüşü de benimsemiş olduklarına dikkat çekmektedir (Elsea [web], 2005).

ve İç Güvenlik Yasası'nda yer alan hiçbir düzenlemenin söz konusu yasanın geçerliliğini etkileyecek biçimde yorumlanamayacağı ifade edilmektedir.

Bu kapsamda İç Güvenlik Yasası'nın 876.ncı ve 886.ncı maddeleri bir arada değerlendirildikleri zaman; ister iç güvenlik genelinde, isterse de siber güvenlik özelinde olsun, ABD'de silahlı kuvvetler ile kolluk kuvvetleri arasında tam bir görev ayrımına gidildiği net bir biçimde ortaya çıkmaktadır. Bu durumun özellikle siber güvenlik açısından önemi ise; aksine ve geçerli bir yasal bir düzenleme bulunmadıkça, ABD Silahlı Kuvvetlerinin siber savaş ve güvenlik kapasitesinin siber suçlara ya da siber terörizme yönelik olarak kullanılamayacak olması noktasında ortaya çıkmaktadır.

4) "Elektronik, Telli ve Sözlü İletişimden Elde Edilen Bilgileri Paylaşma Yetkisi" başlıklı 896.ncı madde ile; soruşturma, kolluk ve diğer yetkili federal kurum görevlilerinin elektronik, telli ve sözlü iletişimden elde edilen bilgileri yabancı kolluk ve soruşturma makamları ile paylaşmalarına imkan tanınmıştır.

Bu kapsamda Federal Ceza Kanununun ilgili maddesinde yapılan değişikliğe göre, söz konusu bilgi paylaşımının yapılabilmesi için aşağıdaki şartlardan birinin karşılanması gerekmektedir:

- Resmi görevlerin yerine getirilebilmesi için gerekli olmak,
- ABD içinde veya dışında, gerçek veya olası bir saldırının ya da düşmanca hareketin, yurtiçi veya yurtdışı sabotajın, ulusal veya uluslararası terörizmin, yabancı bir gücün ya da ajanının gizli istihbarat faaliyetlerinin önlenmesi veya bunlara müdahale edilmesi ile ilgili olmak.

b. Siber Güvenliğin Geliştirilmesi Yasası *(Cyber Security Enhancement Act)*

Tam adı *"Cyber Security Enhancement Act of 2002"* olan ve tek bir maddeden oluşan "2002 tarihli Siber Güvenliğin Geliştirilmesi Yasası" ile; Federal Ceza Kanununun 1030.ncu maddesinde yer alan "Bilgisayar Dolandırıcılığı ve İstismarı" suçlarından alınan cezalarda caydırıcılık sağlayıcı değişikliklerin yapılması öngörülmektedir.

Aynı zamanda İç Güvenlik Yasası'nın 225.nci maddesini de oluşturan bu kanun çerçevesinde, siber güvenlik ile ilişkilendirilebilecek olan düzenlemeler şöyle sıralanabilirler:

1) Cezalandırma politikaları ve uygulamalarına ilişkin olarak federal düzeyde yönergeler geliştirmek ve yayımlamakla görevli olan ABD Cezalandırma Komisyonu (USSC);

> "Cezalandırma yönergeleri ve politika açıklamalarının, birinci paragrafta[36] ifade edilen ihlallerin ciddiyetini, bu gibi ihlallerin artan sıklığını ve bu gibi ihlallerin önlenmesi için caydırıcı ve uygun cezalara olan ihtiyacı yansıtmasını sağlayacaktır."

Bu çerçevede, bahse konu yönergelerin hazırlanmasında Komisyonun gözönünde bulundurması gereken faktörler şöyle sıralanmaktadır:

> "(i) Suçtan kaynaklanan potansiyel ve gerçek kayıp,
>
> (ii) Suçun planlanma ve karmaşıklık seviyesi,
>
> (iii) Suçun ticari avantaj veya özel mali yarar sağlamak amacıyla işlenip işlenmemesi,
>
> (iv) Davalının suçun işlenmesinde, zarar vermek kastı ile kötü niyetli olarak davranıp davranmadığı,
>
> (v) Suçun, kişilerin özel hayatın gizliliğine ilişkin haklarına zarar verme derecesi,

[36] Bahse konu paragrafta Federal Ceza Kanununun 1030.ncu maddesinde yer alan suçlara atıfta bulunulmaktadır.

(vi) Suçun, ulusal savunma, ulusal güvenlik veya adalet hizmetlerinin sürekliliğinde hükümet tarafından kullanılan bir bilgisayarı içerip içermediği,

(vii) Suç eylemi ile, kritik altyapıda önemli ölçüde bir müdahalenin veya bozulmanın amaçlanıp amaçlanmadığı ya da bu gibi durumların ortaya çıkıp çıkmadığı,

(viii) Suç eylemi ile, kamu sağlığına veya güvenliğine yönelik bir tehdidin yaratılmasının veyahut her hangi bir kişinin yaralanmasının amaçlanıp amaçlanmadığı ya da bu gibi durumların ortaya çıkıp çıkmadığı."

2) ABD Vatanseverlik Yasası'nın 212.nci maddesi ile değiştirilmiş olan Federal Ceza Kanununun "Müşteri İletişim veya Kayıtlarının Gönüllü Açıklanması"na ilişkin kısmında, mevcut düzenlemelerin ruhuna fazlaca dokunmayan bazı küçük değişiklikler yapılmıştır. Bahse konu değişikliklerin yanı sıra, Federal Ceza Kanununun "Müşteri İletişim veya Kayıtlarının Zorunlu Açıklanması"na ve "Telli, Sözlü ve Elektronik İletişimin Tespit ve İfşasının Yasaklanması"na ilişkin kısımlarında ise; mahkeme emri *(court order)* ve mahkeme celbi *(subpoena)* gibi kanuna uygunluk halleri arasına "kanuni yetki *(statutory authorization)*" ibaresi de eklenmiştir. Bahse konu düzenlemeler sonrasında, kişi hak ve hürriyetleri açısından oldukça kritik öneme sahip olan ve münhasıran mahkemelere ait olan bazı yetkilerin, bir anlamda yasamanın belirleyeceği şartlar altında yürütmenin görevlilerine devredilebilmesinin yolu açılmıştır.

3) ABD Vatanseverlik Yasası'nın 814.ncü maddesi ile değiştirilmiş olan Federal Ceza Kanununun 1030.ncu maddesinde yer alan "Bilgisayar Dolandırıcılığı ve İstismarı" suçlarında hükmedilebilecek cezalara ilişkin olarak; korunmuş bilgisayarlara karşı girişilen eylemler istisnai olarak yeniden düzenlenmiş ve bu eylemlere verilebilecek cezalar aşağıdaki biçimde ağırlaştırılmıştır:

"(5)(A) Eğer ki, (a)(5)(A)(i) bendini ihlal eden suçu işlemek suretiyle fail bilerek veya düşüncesizce ciddi fiziksel yaralanmaya neden olur veya böyle bir yaralanmaya neden olacak girişimde bulunur ise, bu madde kapsamında para cezasına veya 20 yıldan fazla olmamak üzere hapis cezasına ya da her ikisine birden hükmedilebilir, ve

(B) Eğer ki, (a)(5)(A)(i) bendini ihlal eden suçu işlemek suretiyle fail bilerek veya düşüncesizce ölüme neden olur veya ölüme neden olacak girişimde bulunur ise, bu madde kapsamında para cezasına, herhangi bir süre ile hapis veya ömür boyu hapis cezasına ya da her ikisine birden hükmedilebilir."

4) Soruşturmacı veya kolluk kuvveti görevlilerinin mahkeme kararı olmaksızın *"Pen Register"* veya *"Trap and Trace"* cihazlarını kullanma yetkisine sahip oldukları acil durumların arasına; *"korunmuş bir bilgisayara karşı devam etmekte olan ve bir yıldan fazla hapis ile cezalandırılabilecek bir suç teşkil eden saldırı durumu"* da dahil edilmiştir.

5) Federal Ceza Kanununun elektronik iletişime ve iletişim bilgilerine yetkisiz ve yasadışı olarak erişim ve müdahaleyi düzenleyen "Saklı İletişime Kanunsuz Erişim" başlığı altında suç sayılan hallerin arasına; *"anayasa ya da herhangi bir ABD veya eyalet kanununu ihlal eden herhangi bir suç eylemi ya da haksız fiilin devam ettirilmesi amacıyla girişilen eylemler"* de dahil edilmiştir. Bu kapsamda:

a) Suçun ticari avantaj sağlama, kötü niyetli yok etme ya da zarar verme, özel ticari kazanç sağlama veya anayasa ya da herhangi bir ABD veya eyalet kanununu ihlal eden herhangi bir suç eyleminin veya haksız fiilin devam ettirilmesi amacıyla işlenmesi durumunda; suçun ilk işlenişinde hükmedilebilecek hapis cezası üst sınırının 1 yıldan 5 yıla, suçun müteakiben işlenmesi durumunda hükmedilebilecek hapis cezası üst sınırının ise 2 yıldan 10 yıla çıkartılması,

b) Suçun yukarıda sayılan amaçlar haricinde işlenmesi durumunda ise; suçun ilk işlenişinde para veya 1 yıldan fazla olmamak üzere hapis cezasının ya da her ikisinin birden verilmesi, suçun müteakiben işlenmesi durumunda ise para veya 5 yıldan fazla olmamak üzere hapis cezasının ya da her ikisinin birden verilmesi öngürülmüştür.

c. Federal Enformasyon Güvenliği Yönetimi Yasası *(Federal Information Security Management Act)*

Tam adı *"Federal Information Security Management Act of 2002"* ve resmi kısaltması "FISMA" olan, "2002 tarihli Federal Enformasyon Güvenliği Yönetimi Yasası" ile; enformasyon güvenliğine ilişkin federal kanunlarda, mevcut güvenlik önlemlerini geliştirici değişiklikler yapılmaktadır. FISMA'ya ilişkin olarak özellikle dikkati çeken bir nokta da; özel sektör kuruluşlarının kamu kurumları ile neredeyse eşitlenen konumudur. Zira FISMA kapsamında özel sektör; hem enformasyon güvenliğini sağlayan temel unsurlardan biri, hem de kamu kurumları ile birlikte enformasyon güvenliği şemsiyesi altında yer alan korunması gereken bir yapı olarak görülmektedir.

İç Güvenlik Yasası'nın 1001.nci ve 1006.ncı maddeleri arasında yer alan altı maddeden oluşmasına rağmen FISMA, tümüyle enformasyon güvenliğine odaklanmış olması nedeniyle, kendi alanında oldukça büyük bir öneme sahiptir. Bununla birlikte, enformasyon güvenliği olgusunun sahip olduğu geniş kapsam nedeniyle; çalışmanın bu kısmında, bahse konu kanun yalnızca siber güvenlik ile ilişkili olan kısımları üzerinden ele alınmıştır. Bu çerçevede, FISMA kapsamında siber güvenlik ile ilişkilendirilebilecek olan madde ve öngörülen düzenlemeler şöyle sıralanabilirler:

1) Sekiz buçuk sayfa uzunluğunda olan "Enformasyon Güvenliği" başlıklı 1001.nci madde ile; "Kamu Yayıncılığı ve Belgeleri"ne ilişkin federal mevzuat içerisinde yer alan "Enformasyon Güvenliği" ile ilişkili mevcut düzenlemeler tümüyle değiştirilmekte ve bir anlamda yeni baştan yazılmaktadır. Bu madde kapsamında, "Enformasyon Güvenliği"ne ilişkin "yeni" federal mevzuatın yapılış amaçları şöyle sıralanmaktadır:

> "(1) Federal faaliyetleri ve unsurları destekleyen enformasyon kaynakları üzerindeki enformasyon güvenliği kontrollerinin etkinliğinin sağlanması için kapsamlı bir çerçeve temin etmek,

(2) Mevcut federal bilgi işlem ortamının yüksek oranda ağa dayalı olan yapısını dikkate alacak ve sivil, ulusal güvenlik ve kolluk camiaları tarafından yürütülen enformasyon güvenliği çabalarının koordinasyonunu da içerek biçimde, tüm federal hükümet çapında etkin bir yönetim ve güvenlik risklerine ilişkin gözetim sağlamak,

(3) Federal enformasyon ve enformasyon sistemlerini korumak için gerekli olan asgari kontrollerin geliştirilmesini ve sürdürülmesini sağlamak,

(4) Federal hükümet teşkilatlarının enformasyon güvenliği programlarının geliştirilmiş bir biçimde gözetimi için bir mekanizma sağlamak,

(5) Ticari amaçlı olarak geliştirilmiş enformasyon güvenliği ürünlerinin; gelişmiş, dinamik, güçlü ve etkili bilgi güvenliği çözümleri sunduklarını, ulusal savunma ve ekonomik güvenlik için önemli olan, özel sektör tarafından dizayn ve inşa edilerek işletilen kritik enformasyon altyapısının korunması için piyasa çözümlerini yansıttıklarını kabul etmek,

(6) Enformasyon güvenliğinde kullanılacak özel teknik donanım ve yazılımlara ilişkin olarak, ticari olarak geliştirilmiş olan ürünler arasından yapılacak seçimin her bir federal kurumun kendisine bırakılması gerektiğini kabul etmek."

Yine aynı madde ile, ilgili yasal mevzuat içerisinde geçen bazı önemli terimlerin yasal tanımlarına açıklık getirilmiştir. Bu çerçevede;

"(1) 'Enformasyon Güvenliği *(Information Security)*' terimi, enformasyonu ve enformasyon sistemlerini yetkisiz erişim, kullanım, ifşa, bozulma, değiştirilme ya da imhadan korumak anlamına gelir..."

(2) 'Ulusal Güvenlik Sistemi *(National Security System)*' terimi, bir federal teşkilat veya bir federal teşkilatın sözleşmeli hizmet sağlayıcısı[37] ya da bir federal teşkilat adına hareket eden diğer bir örgüt tarafından kullanılan veya işletilen herhangi bir enformasyon sistemi (her hangi bir telekomünikasyon sistemini de içerecek biçimde) anlamına gelir ki; işlevleri, işletmesi veya kullanımı-

(A) İstihbarat faaliyetleri ile bağlantılı;

(B) Ulusal güvenlikle ilişkili kriptoloji faaliyetleri ile bağlantılı;

[37] Metinde kullanılan orijinal ifade, "müteahhit" ya da "yüklenici" anlamlarına gelebilen, "*contractor*"dur. İncelenmekte olan kanunun ruhu ile uyumlu olması maksadıyla; enformasyon sektöründeki özel firmalardan alınabilecek hizmetlere atfen, "hizmet sağlayıcı" olarak çevrilmiştir.

(C) askeri kuvvetlerin komuta ve kontrolü ile bağlantılı,

(D) Bir silah veya silah sisteminin ayrılmaz bir parçası olan donanım ile bağlantılı; veya

(E) askeri veya istihbari görevlerin doğrudan yerine getirilmesinde kritik önemdedir. Bu tanım, rutin idari ve ticari uygulamalar (bordro, finans, lojistik ve personel yönetimi uygulamalarını da içerecek biçimde) için kullanılan bir sistemi kapsamaz.

(4) 'Enformasyon Sistemi *(Information System)*' terimi, verinin veya enformasyonun otomatik olarak toplanması, depolanması, yönlendirilmesi, yönetimi, hareketi, kontrolü, görüntülenmesi, değiştirilmesi, değiş tokuşu, aktarılması veya alınmasında kullanılan her türlü ekipman veya ekipman ile bağlantılı sistem ya da ekipmanın alt-sistemleri anlamına gelir ve şunları içerir-

(A) Bilgisayarlar ve bilgisayar ağları;

(B) Yardımcı donanım;

(C) Yazılım, gömülü yazılım ve ilgili prosedürler;

(D) Destek hizmetleri de dahil olmak üzere hizmetler;

(E) İlgili kaynaklar."

Bu madde kapsamında yer alan diğer bir düzenleme ile de; kendi enformasyon güvenliklerini sağlamak noktasında, zorunlu bazı standartları karşılamaları ve bir güvenlik programı başlatmaları şartı ile federal kurumlar serbest bırakılmıştır. Bununla birlikte, her federal kurumun enformasyon güvenliği alanında yürüttüğü faaliyetleri belirlenen resmi kurumlara ve bu kurumlarında yapacakları değerlendirmeleri Kongreye düzenli olarak rapor etmeleri de öngörülmüştür.

2) "Enformasyon Teknolojisinin Yönetimi" başlıklı 1002.nci madde ile; kamu binaları, mülkleri ve tesislerine ilişkin federal mevzuat içerisinde yer alan "Federal Enformasyon Sistemleri Standartlarının Sorumluluğu" ile ilişkili mevcut düzenlemelerde değişiklik yapılmaktadır. Bu kapsamda; Yönetim ve Bütçe Dairesi (OMB) Müdürü, Ulusal Standartlar ve Teknoloji Enstitüsü (NIST) tarafından geliştirilerek önerilecek asgari enformasyon güvenliği standartlarını, İç Güvenlik

Bakanına da danıştıktan sonra yayımlamak ile görevlendirilmiştir. Ulusal güvenlik sistemleri bu genel düzenlemenin kapsamı dışında bırakılmış olup; bu sistemlere ilişkin standartların ve talimatnamelerin geliştirilmesi, yayımlanması, uygulanması ve takip edilmesi hususları, kanun veya ABD Başkanı tarafından ayrıca emredilmiş olma şartına bağlanmıştır.

3) "Ulusal Standartlar ve Teknoloji Enstitüsü" başlıklı 1003.ncü madde ile; Ulusal Standartlar ve Teknoloji Enstitüsü (NIST) Kuruluş Yasasında bazı değişiklikler yapılmaktadır. Bu madde çerçevesinde NIST'in bazı önemli görevleri şöyle sıralanabililer:

"Enstitü-

(1) Enformasyon sistemlerine ilişkin standartların, yönergelerin, ilişkili yöntem ve tekniklerin geliştirilmesi ile görevli olacaktır;

(2) Bir federal teşkilat veya bir federal teşkilatın sözleşmeli hizmet sağlayıcısı ya da bir federal teşkilat adına hareket eden diğer bir örgüt tarafından kullanılan veya işletilen, ulusal güvenlik sistemleri haricindeki enformasyon sistemleri için, asgari gereklilikleri karşılayacak standartları ve yönergeleri geliştirecektir;

(3) Ulusal güvenlik sistemleri için geçerli olmamak kaydı ile, tüm federal kurum faaliyetleri ve unsurları için yeterli bilgi güvenliğini sağlamak üzere, asgari gereklilikleri karşılayacak biçimde standartlar ve yönergeler geliştirecektir."

Aynı madde kapsamında, NIST tarafından belirlenecek standartların ve oluşturulacak yönergelerin niteliklerine ilişkin olarak da birçok düzenleme yer almaktadır. Bahse konu düzenlemeler içerisinde;

a) NIST tarafından belirlenecek standartların ve oluşturulacak yönergelerin, Savunma Bakanlığı, NSA, OMB, GAO, Enerji Bakanlığı ve İç Güvenlik Bakanlığının yanı sıra diğer ilgili kurum ve dairelere de danışılarak geliştirilmelerinin öngörülmüş olması,

b) "Ulusal güvenlik sistemi" olarak nitelendirilmiş olan enformasyon sistemlerine ilişkin standartların ve yönergelerin, kanun hükümleri ve ABD Başkanının emirleri ile uyumlu bir biçimde, NSA ile

koordinasyon içerisinde geliştirilmelerinin öngörülmüş olması özellikle dikkati çekmektedir.

4) "Enformasyon Güvenliği ve Gizliliği Danışma Kurulu" başlıklı 1004.ncü madde ile; NIST Kuruluş Yasasında yer alan ve Ticaret Bakanlığına bağlı olarak faaliyet gösteren "Bilgisayar Sistem Güvenliği ve Gizliliği Danışma Kurulu *(Computer System Security and Privacy Advisory Board)*"na ilişkin mevcut düzenlemelerde bazı değişiklikler yapılmaktadır. Söz konusu değişikliklerin bu çalışma açısından önemi ise; değişikliklerin içeriğinden ziyade, enformasyon sistemlerine yönelik algıdaki değişimi ve genişlemeyi "kavramsal ve terimsel" olarak yansıtmalarından kaynaklanmaktadır. Zira, bu madde ile; daha önceden "bilgisayar ya da telekomünikasyon", "bilgisayar ya da telekomünikasyon teknolojisi", "bilgisayar ya da telekomünikasyon ekipmanı", "bilgisayar sistemleri" ve "bilgisayar sistem güvenliği" terimleri ile ifade edilen olgular "enformasyon" çatısı altında birleştirilerek, "enformasyon teknolojisi", "enformasyon sistemi" ve "enformasyon güvenliği" terimleri ile karşılanmaya başlanmışlardır. Nitekim bu kapsamda, "Bilgisayar Sistem Güvenliği ve Gizliliği Danışma Kurulu"nun ismi de, "Enformasyon Güvenliği ve Gizliliği Danışma Kurulu *(Information Security and Privacy Advisory Board)*" olarak değiştirilmiştir.

DÖRDÜNCÜ BÖLÜM

SİBER GÜVENLİĞİN SAĞLANMASINA YÖNELİK YÜRÜTME FAALİYETLERİ

1. FEDERAL HÜKÜMET POLİTİKALARI

11 Eylül 2001 tarihinden günümüze kadar geçen dönem içerisinde ABD Hükümeti tarafından geliştirilen gerek ulusal güvenlik, gerekse de siber güvenlik politikaları, elbette ki söz konusu dönemde yönetimde bulunan başkanlar olarak, George W. Bush (2001-2009) ve Barrack Obama (2009-Günümüz) ile onların kadrolarının birer eseridir. Farklı partilere mensup olan bu iki başkandan; gerek görev süresinin uzunluğu, gerekse de saldırıların hemen sonrasındaki dönemde pek çok politikayı, stratejiyi ve örgütlenmeyi şekillendiren hayati tercihleri yapmış olması nedeniyle, George W. Bush'un güvenlik politikaları üzerindeki etkisinin çok daha fazla olduğunu ileri sürmek yanlış olmayacaktır.

Başkan Bush'un, özellikle 11 Eylül Saldırıları sonrası dönemde yapmış olduğu kritik tercihleri ve geliştirdiği yaklaşımı değerlendiren Krieger'e göre (Dobrowolsky ve diğerleri, 2009: 21);

> "ABD dış politikasında, 50 yıldan fazladır stratejik kısıt nedeniyle görmezden gelinmiş olan bir şey, saldırgan mahiyetteki "Ulusal Güvenlik Stratejisi"nin 2002 yılı Eylül'ünde ortaya konulması ile güç kazanarak değişmiştir. Bu belge, dış ilişkilere Bush'un damgasını vurmuş ve kendine özgü bir doktrinin esaslarını sistemleştirmiştir. Söz konusu strateji, Bush Doktrinini oldukça canlı bir şekilde resmeden ve Amerika'nın daha saldırgan, tek taraflı ve jeopolitik yeni stratejisine ilişkin neyin doğru veya yanlış olduğunu simgeleştiren Irak'ın İşgali ile birlikte hakim paradigma haline gelmiştir."

Ancak bu noktada şunu da ifade etmek gerekir ki; her iki başkan döneminde de, kitle imha silahlarının kullanıldığı muhtemel terörist

saldırılar, birincil güvenlik tehdidi olarak kabul edilmiştir. Nitekim Priest ve Arkin'in de aktardığı üzere (2011: 120-121); Bush Yönetimi döneminde, "ABD içerisinde Kitle İmha Silahlarının kullanıldığı, eşzamanlı ve yıkıcı" mahiyette 3 ila 6 saldırının yapılabileceği değerlendirilirken; nükleer silahların kullanıldığı bir terörist saldırı tehdidi Başkan Obama tarafından "Amerikan halkının karşı karşıya olduğu en vahim tehlike" olarak nitelendirilmiştir.

ABD'nin siber tehditlere ilişkin güvenlik algısının tarihsel süreç içerisinde geçirdiği değişimin net bir biçimde ortaya konulabilmesi noktasında; M. Dunn Cavelty'nin *"Cyber Security and Threat Politics"* isimli eseri oldukça kapsamlı ve anlaşılır bir çerçeve sunmaktadır. Bahse konu tarihsel süreç, Dunn Cavelty'nin çizdiği kavramsal ve kuramsal çerçeve üzerinden genel bir değerlendirmeye tabi tutulduğu zaman; üç dönem şeklinde tasnif edilmesi mümkün görünmektedir. Net ve kesin bir şekilde birbirlerinden ayırt edilmeleri mümkün olmayan söz konusu dönemler içerisinde; üzerine odaklanılan her yeni tehdit, kendisinden önce varolan tehditleri ortadan kaldırmaksızın onlar ile birlikte var olmuş ve böylelikle de siber tehditlerin ve siber güvenliğin kapsamı sürekli olarak genişlemiştir. Bu çerçevede, bilgisayar ve veri güvenliğinin sağlanmasına yönelik ilk düzenlemelerin ortaya çıktığı ve bugünkü anlamı ile "siber güvenlik" kavramının somutlaşmaya başladığı Başkan Reagan döneminde; bilgisayar suçlarına ve verilere yönelik casusluk eylemlerine odaklanmış bir tehdit algılaması mevcuttur (Dunn Cavelty, 2008: 59-65). Soğuk savaş sonrası dönemde ise enformasyon teknolojisinde ortaya çıkan hızlı gelişmelere de paralel olarak; bilgisayarlar ve internet, "enformasyon savaşı" olgusu kapsamında asimetrik birer silah olarak görülmeye başlanmış ve siber güvenliğin askeri boyutu önplana çıkmıştır (Dunn Cavelty, 2008: 66-90). 11 Eylül 2001 tarihinden sonra ise, kritik altyapının korunmasına ve iç güvenliğe ağırlık veren, terörizm merkezli ve asimetrik nitelikli bir siber tehdit algısı hızla yaygınlık kazanmış olup; bahse konu son dönem büyük oranda Başkan Bush tarafından şekillendirilmiştir (Dunn Cavelty, 2008: 91-121).

Bu kapsamda, neredeyse 30 yıllık bir süreci referans alan her üç dönemin de birbirlerini yumuşak bir şekilde takip etmelerine ve her yeni

döneme damgasını vurmuş olan "tehdit" algısının aslında bir önceki dönem içerisinde önceden ifade edilmeye başlanmış olmasına bağlı olarak; siber tehditlerin ve dolayısı ile de siber güvenliğin teknolojik, politik ve sosyal değişimlerden etkilenen evrimsel bir süreç içerisinde bulunduğunu ileri sürmek mümkündür. Nitekim bu süreç neticesinde; siber suç, siber savaş ve siber terörizm olguları hem siber güvenliğin ortak, temel ve asli kaygıları haline gelmiş, hem de siber güvenliğe yönelik farklı bakış açılarını yansıtan birer prizma niteliği kazanmışlardır.

Yaptıkları çalışma ile ABD'nin günümüzdeki ulusal güvenlik profilini çıkartmış olan Priest ve Arkin'in de ifade etiği üzere (2011: 118);

> "ABD'nin elektronik hayat damarlarının ulusal seviyede korunması, DHS'nin ve 2009 yılında faaliyete geçen, Fort Meade, Maryland'da bulunan ordu -4 yıldız- seviyesindeki Siber Komutanlığın sorumluluğundadır. Bu komutanlık askeri elektronik savunma tedbirlerinin tümünü kontrol eder ve ABD varlıklarını etkileyen her hangi bir siber savaşta mücedele eder. ABD içerisinde ise siber güvenlikten sorumlu olan FBI'dır."

Yasal mevzuat açısından bakıldığı zaman ise, tüm federal kurumların kendi sistemlerinin siber güvenliğini sağlamakla yükümlü olduklarına ve görev alanlarına girmesi durumunda da kritik altyapının korunmasına ilişkin ilave sorumluluklar yüklendiklerine dikkat çeken Fischer'e göre (2011: 4); *"birden fazla kurumu ilgilendiren yükümlülükler karmaşıktır."*

Federal hükümetin 11 Eylül Saldırılarına yönelik ilk tepkisinin siber güvenlik boyutunun; kritik altyapının korunmasına odaklanan ve bu alandaki mevcut yapılanmayı yeni baştan inşa eden EO 13228 ve EO 13231 sayılı Başkanlık İdari Emirleri ile somutlaştığını ifade eden Dunn Cavelty (2008: 104); bu yeni durumu şöyle tasvir etmektedir:

> "'İç Güvenlik Dairesinin ve İç Güvenlik Konseyinin Kurulması' başlıklı ve 08 Ekim 2001 tarihli EO 13228 ile Bush, yeni İç Güvenlik Dairesi *(Office of Homeland Security)*'nin bir parçası olmak üzere, Beyaz Saray bünyesinde bir Siber Savunma Ofisi *(Office of Cyberdefense)* kurdu...

'Enformasyon Çağında Kritik Altyapının Korunması' başlıklı ikinci İdari Emir, EO 13231, kritik altyapı için enformasyon sistemlerini korumak üzere siyasal tavsiyelerde bulunmak ve programları koordine etmek ile sorumlu olan Başkanlık Kritik Altyapının Korunması Kurulu *(the President's Critical Infrastructure Protection Board)*'nu ihdas etti."

Terörle mücadele ve asimetrik tehditler bağlamında ise, ABD hükümetinin stratejik seviyedeki tepkisini içeren ilk "Ulusal Güvenlik Stratejisi (NSS)"nin 2002 yılında, ilk "Terörle Mücadele Ulusal Stratejisi (NSCT)"nin ise 2003 yılında yayımlandığını ifade eden Forest; söz konusu belgelerin stratejik çerçeve içerisindeki merkezi rollerine şöyle dikkat çekmektedir (2007: 3-4);

"NSS, NSCT için stratejik bir çerçeve sağlarken, her ikisi de - İç Güvenlik Ulusal Stratejisi (Temmuz 2002'de yayımlandı), Kitle İmha Silahları Ulusal Stratejisi (Aralık 2002), Güvenli Siber Uzay Ulusal Stratejisi (Şubat 2003), Kritik Altyapı ve Önemli Varlıkların Fiziksel Korunması Ulusal Stratejisi (Aralık 2003) Ulusal Uyuşturucu Kontrol Stratejisi (Şubat 2002) ve Deniz Güvenliği Ulusal Stratejisi (Eylül 2005) gibi- ilave stratejik belgeler ile desteklenmişlerdi.

Yakın zamanda, bu belgelerde ele alınan konuların birçoğu NSS ve NSCT'nin yeni 2006 versiyonlarında desteklenmiş ve genişletilmiştir."

Yakın dönemde siber güvenlik kapsamında yürütülen en önemli federal hükümet faaliyeti ise, Fischer'e göre; Başkan Bush tarafından 2008 yılında yayımlanan NSPD-54/HSPD-23 sayılı Başkanlık Direktifleri ile hayata geçirilmiş olan "Kapsamlı Ulusal Siber Güvenlik Girişimi (CNCI)" olmuştur (2011: 3):

"Bu belgeler 'Gizli'dir, ancak Obama Yönetimi bunlara ilişkin bir tanımlamanın 2010 yılı Mart ayında yayımlanmasına izin vermiştir. Bahse konu tanımlamada yer alan 12 alt girişimin hedefleri; federal sistemlere harici erişim noktalarının birleştirilmesini; bu sistemlerin bünyelerine, saldırı tespit ve önleme sistemleri yerleştirilmesini; araştırma koordinasyonu ve önceliklendirmelerinin iyileştirilmesi ve "yeni nesil" teknolojinin, bilgi paylaşımının, siber güvenlik eğitimi ve farkındalığının geliştirilmesini; enformasyon teknolojilerine ilişkin küresel tedarik zincirinden kaynaklanan risklerin azaltılmasını; ve kritik altyapının korunmasında federal rolün açıklığa kavuşturulmasını içermektedir."

Hükümet kurumlarının siber güvenlik alanındaki yetki ve sorumluluklarını bir bütün olarak ele alan Fischer; Priest ve Arkin ile benzer ancak çok daha kapsamlı bir biçimde, federal kurumları siber güvenlik alanındaki sorumlulukları üzerinden şöyle tasnif etmektedir (2011: 4):

> "Genel olarak, Beyaz Saray kurumlarının rollerine ilaveten, DHS sivil-sektörde asli siber güvenlik teşkilatıdır. Ticaret Bakanlığına bağlı olan NIST, OMB tarafından yayımlanan siber güvenlik standartlarını ve yönergelerini geliştirirken, siber güvenlik ile ilişkili yasaların uygulanmasından büyük ölçüde Adalet Bakanlığı sorumludur. NSF, NIST ve DHS birlikte siber güvenlik ile ilişkili araştırma ve geliştirme falliyetlerini yerine getiriler. NSA, her ne kadar diğer kurumlar da önemli roller oynamakta iseler de, ulusal güvenlik sektöründe asli siber güvenlik teşkilatıdır. Yeni kurulan ve Savunma Bakanlığına bağlı ABD Stratejik Komutanlığının bir parçası olan ABD Siber Komutanlığı ise askeri siber uzay operasyonlarından öncelikle sorumludur."

ABD Silahlı Kuvvetlerinin, enformasyon teknolojisindeki gelişmelere ve yeni asimetrik tehdit algılamalarına paralel olarak, "enformasyon savaşı" olgusunun da merkezinde yer aldığı bir dönüşüm sürecine girdiğini ve bahse konu bu değişimin 2001 yılından itibaren daha da açık bir şekilde görülmeye başlandığını ifade eden Dunn Cavelty (2008: 110-111); dönemin ABD Savunma Bakanı Donald Rumsfeld'in 11 Eylül Saldırılarından kısa bir süre önce, NATO'ya yönelik gelecek dönem tehditleri arasında siber saldırılarında yer aldığına ilişkin açıklamalarına, ittifak politikaları kapsamında özellikle dikkati çekmektedir (2008: 111):

> "Rumsfeld müttefiklere sadece ABD'nin değil, aynı zamanda diğer NATO ülkelerinin ve buna bağlı olarak da bir bütün olarak ittifakın, siber uzaydan gelen saldırılar tarafından tehdit edildiğini anlattı. Rumsfeld, NATO'ya yönelik 'gelecekteki meydan okumalar' arasında sadece geleneksel terörizmi, ileri teknoloji silahları ve Kitle İmha Silahları ile donatılmış füzeleri değil, aynı zamanda siber saldırıları da saydı."

2001 yılı sonrasında bahse konu dönüşüm sürecine hâkim olduğunu savunduğu ve "Rumsfeld Doktrini" olarak da isimlendirilen anlayışı, Rumsfeld'in *Foreign Affairs* Dergisinde 2002 yılında yayımlanmış

olan *"Transforming the Military"* başlıklı makalesine atfen tanımlayan Dunn Cavelty'e göre (2008: 112);

> "Rumsfeld Doktrini, teknolojik olarak gelişmiş bir ordunun, 'Hareket *(Mobility)*', 'Görünmezlik *(Stealth)*' ve 'Teknoloji *(Technology)*' esaslarına dayanmak suretiyle, göreceli olarak az sayıdaki asker ile dünyanın herhangi bir yerindeki savaşları kolaylıkla kazanacağını vaad ediyordu."

Bahse konu doktrinin hayata geçirilmesine yönelik atılmış somut bir adım olarak, Bakan Rumsfeld tarafından onaylanarak 30 Ekim 2003 tarihinde yayımlanmış olan "Enformasyon Operasyonları Yol Haritası" isimli belgeye dikkat çeken Dunn Cavelty'e göre (2008: 111);

> "Belge, 'Enformasyon Operasyonları (IO)'nın beş önemli alanında sahip olduğu kapasiteyi arttırması için Savunma Bakanlığına çağrıda bulunuyordu: Eektronik Savaş (EW), Psikolojik Operasyonlar (PSYOPS), Operasyon Güvenliği (OPSEC), Askeri Aldatma ve Bilgisayar Ağı Operasyonları (CNO). Çok daha grafiksel bir biçimde, belgede; 'Ağ'da savaşmalıyız', 'Psikolojik Operasyonu geliştirmeliyiz', 'Ağ ve Elektromanyetik Saldırı Kapasitesini geliştirmeliyiz' gibi ifadeler yer alıyordu."

Her ne kadar ABD Silahlı Kuvvetlerinin içerisinden geçtiği değişim süreci ile 11 Eylül Saldırıları arasında doğrudan ya da dolaylı olarak ilişki kurulabilmesi mümkün ise de, bahse konu değişim sürecine hakim olan anlayışın temellerinin 11 Eylül Saldırıları öncesindeki dönemde ve enformasyon teknolojilerinde yaşanılan hızlı değişimde aranması yanlış olmayacaktır. Daha önceden de vurgulandığı üzere bu çalışmanın konu ve kapsamı çerçevesinde, 11 Eylül Saldırılarına ABD hükümeti tarafından verilen asıl tepki; ABD'deki istihbarat ve güvenlik aygıtının asimetrik tehditler bağlamında yeniden yapılandırılması ve gerekli görülen yerlerde yeni kurumlar ile takviye edilmesi olmuştur.

Obama Yönetiminin de söz konusu örgütlenme eğilimini devam ettirdiğine ve 2009 yılında 39, 2010 yılında ise 24 yeni kuruluşu terörle mücadele kapsamında oluşturduğuna dikkat çeken Priest ve Arkin (2011: 276); bu kuruluşlardan bir tanesinin de, Deniz Kuvvetleri Siber Savaş, İstismar ve Enformasyon Hakimiyeti Laboratuvarı (CWEID) olduğunu ifade etmektedirler.

Bu kapsamda, istihbarat ve güvenlik yapılanmasının asimetrik tehditler ile mücadele çerçevesinde güçlendirilmesine ve ABD Silahlı Kuvvetlerinin enformasyon savaşı konsepti çerçevesinde dönüştürülmesine yönelik adımların Başkan Obama döneminde de atılmaya devam edildiğini ileri sürmek mümkündür.

Enformasyon Savaşı olgusunun silahlı kuvvetleri dönüştürdüğü, siber savaş ve siber terörizm tartışmalarının her geçen gün daha fazla yapıldığı bu ortamda aykırı bir ses olarak, Obama Yönetiminin siber güvenlikten sorumlu en yetkili ismi olan Beyaz Saray Siber Güvenlik Koordinatörü Howard Schmidt özellikle dikkati çekmektedir. Schmidt'e göre (Wired [web], 2010); *"ortada bir siber savaş bulunmamaktadır."* Hükümetin siber güvenlik çabalarını esas itibariyle internet suçları ve casusluk ile mücadeleye odaklaması gerektiğini savunan Schmidt; siber savaş odaklı mevcut siber güvenlik algılamasını, *"korkunç bir metafor ve korkunç bir konsept"* olarak nitelendirmektedir. Bu kapsamda, *"böyle bir ortamda hiç kimsenin kazanması mümkün değildir"* tespitinde bulunan Schmidt, çok daha önemli ve belki de kritik bir tespiti de -biraz da kinayeli bir biçimde- mevcut istihbarat ve güvenlik yapılanmasının içerisinde bulunduğu kurumlar arası güç mücadelesine ilişkin olarak yapmaktadır (Wired [web], 2010):

> "Son yıllarda, siber güvenliğin sağlanmasında başrolü (orduyu temsil eden) NSA'nın mı yoksa (sivil tarafta yer alan) DHS'nin mi alacağına ilişkin olarak başkentte yürütülen güç mücadelesinde oldukça fazla mürekkep[38] dökülmüştür."

Her ne kadar Schmidt'in, kurumlar arası güç mücadelesine ilişkin olarak yukarıda yapmış olduğu tespitin merkezinde yer almakta iseler de; elbette ki NSA ve İç Güvenlik Bakanlığı (DHS) arasındaki ilişkilerin rekabet boyutu olduğu kadar işbirliği boyutu da bulunmaktadır.

[38] Schmidt, kullanmış olduğu *"Turf Battle"* ve *"Ink"* kelimeleri ile; sokak çeteleri arasında oldukça kanlı geçen bölgesel güç mücadelelerine bir göndermede bulunarak, bu mücadelede "kan yerine dökülen mürekkep" üzerinden mevcut istihbarat ve güvenlik yapılanması içerisindeki kurumlar arası mücadelenin şiddetini kinayeli bir biçimde vurgulamaktadır.

2. FEDERAL KURUMLAR ARASINDA İŞBİRLİĞİ

Diğer pek çok ülkede olduğu gibi ABD'de de, hükümet politikalarının hayata geçirilmesi ve ilan edilen stratejilerin uygulanması maksadıyla, hükümetin birer parçası olan farklı bakanlıklar ve onlara bağlı farklı kurumlar arasında, işbirliği esaslarını belirlemek ve söz konusu işbirliğini kurumsallaştırmak üzere mutabakat zaptları imzalanmaktadır.

Bu çerçevede, sıklıkla siber saldırılara maruz kalması nedeniyle siber güvenlik konusunda oldukça "tecrübeli" olarak kabul edilebilecek olan Savunma Bakanlığı ile görece daha "genç" olan İç Güvenlik Bakanlığı arasında 24 Eylül 2010 tarihinde imzalanmış olan "İç Güvenlik Bakanlığı ile Savunma Bakanlığı Arasında Siber Güvenliğe ilişkin Mutabakat Zaptı"[39] isimli belge, çalışmanın bu kısmında ele alınmıştır.

İç Güvenlik ve Savunma Bakanlıkları bünyesinde karşılıklı olarak görevlendirilecek personelin görevlerine ve yapılacak işbirliğinin kapsamına ilişkin söz konusu belgenin bu çalışma kapsamında incelenmek üzere seçilmesinin nedeni; gerek ABD'deki istihbarat ve güvenlik yapılanmasına ilişkin güncel bir belge olması, gerekse de NSA'nın istisnai konum ve çalışma biçimine ilişkin oldukça net fikirler verebilmesidir.

Bakanlıklararası bahse konu işbirliğinin amacı ise, mutabakat zaptında şöyle ifade edilmektedir (DHS [web], 2010a):

> "Bu anlaşmanın amacı, ulusun siber güvenliği için stratejik planlamada bakanlıklararası işbirliğini arttırmak, siber güvenlik yeteneklerinin geliştirilmesi için karşılıklı destek ve mevcut operasyonel siber güvenlik faaliyetlerinin eşgüdümünü sağlamak üzere İç Güvenllik ve Savunma Bakanlıkları tarafından temin edilecek personel, ekipman ve tesislere ilişkin esesları ortaya koymaktır. Bu anlaşmanın uygulanılmasında, bir bütün olarak genel kapasitenin arttırılmasının yanı sıra gerek İç Güvenlik Bakanlığının iç güvenliğe yönelik, gerekse de Savunma Bakanlığının

[39] Söz konusu mutabakat zaptının orijinal ve tam adı; *"Memorandum of Agreement Between the Department of Homeland Security and the Department of Defense Regarding Cybersecurity"*dir.

ulusal güvenliğe yönelik görevlerindeki yeteneklerini arttırmak üzere ulusal siber güvenlik çabalarına odaklanılacaktır..."

Yukarıda belirtilen işbirliği amaçları çerçevesinde hazırlanmış olan söz konusu mutabakat zaptı kapsamında;

1) Savunma Bakanlığına bağlı olan NSA bünyesinde çalışmak üzere, İç Güvenlik Bakanlığı personeli içerisinden bir "DHS Siber Güvenlik Koordinasyon Direktörü"nün görevlendirilmesi ve bahse konu personelin aynı zamanda ABD Siber Komutanlığı nezdinde de "DHS Kıdemli Siber Güvenlik Temsilcisi" olarak görev yapması öngörülmüştür. Bu çerçevede (DHS [web], 2010a);

"(7) DHS Siber Güvenlik Koordinasyon Direktörü.

f. Siber uzaydaki iç güvenlik ve ulusal güvenlik faaliyetlerine yönelik bir saldırı, müdahale, uzlaşma veya yetersizlik durumunun önlenmesi, tespit edilmesi, azaltılması ve/veya etkilerinin giderilmesinde yardımcı olmak üzere siber güvenlik tehdit bilgisinin kamu ve özel sektör arasında paylaşılmasını geliştirmeye yönelik Savunma Bakanlığı ve İç Güvenlik Bakanlığı çabalarının koordinasyonunda yardımcı olur."

2) "Müşterek Koordinasyon Unsuru *(Joint Coordination Element)*" adı altında, *"müşterek operasyon planlaması, koordinasyon, eşgüdüm, gerekli yabancı dil çeviri desteği ve siber güvenlik bağlamında iç güvenliğin sağlanması için iç güvenlik bakanlığının diğer görevlerine görev desteği sağlama işlevlerini yerine getirmek"* üzere, NSA bünyesinde görev yapacak bir koordinasyon birimi oluşturulmaktadır. Bu çerçevede, yeni oluşturulan bu birim içerisinde her iki bakanlığın personelinin de müştereken faaliyet göstermeleri öngörülmüştür.

3) *"Müşterek operasyon planlaması, koordinasyon, eşgüdüm, gerekli yabancı dil çeviri desteği ve siber güvenlik bağlamında iç güvenliğin sağlanması için iç güvenlik bakanlığının diğer görevlerine görev desteği sağlanması"* hususlarında mevcut işbirliği seviyesini yükseltmek üzere, uygun görülmesi halinde, "NSA/CCS Tehdit Harekat Merkezi (NTOC)"nde İç Güvenlik Bakanlığı personeli görevlendirilmesine izin verilmektedir.

4) Teknoloji geliştirme ve ortak satınalma faaliyetleri için, NSA Satınalma Direktörlüğünde, İç Güvenlik Bakanlığı personeli görevlendirilmesine izin verilmektedir.

5) Gerek İç Güvenlik Bakanlığı tarafından yürütülen siber güvenlik operasyonları, gerekse de "Ulusal Siber Olaylara Müdahale Planı (NCIRP)" ile operasyonel eşgüdümü sağlamak ve bunları desteklemek üzere; İç Güvenlik Bakanlığı bünyesinde bulunan NCCIC'ye, NSA tarafından bir "Kriptolojik Hizmet Grubu *(Cryptologic Services Group)*"nun, ABD Siber Komutanlığı tarafından ise bir "Siber Destek Unsuru *(Cyber Support Element)*"nun yerleştirilmesine İç Güvenlik Bakanlığı tarafından izin verilmektedir.

6) Gerek İç Güvenlik Bakanlığının Savunma Bakanlığından gelen, gerekse de NSA ve ABD Siber Komutanlığının İç Güvenlik Bakanlığından gelen siber güvenlik destek taleplerini kabul etmesi öngörülmüştür. Bu çerçevede bahse konu taleplerin yürürlükteki yasal mevzuat, yetki ve görev gerekleri ile uyumlu olması durumunda, ilgili bakanlığın gereksinimleri operasyon planlaması ve görev koordinasyonunda dikkate alınacaklardır.

7) Savunma Bakanlığı bünyesinde kurulması önerilen "Bütünleşik Siber Merkez (ICC)" ile İç Güvenlik Bakanlığı bünyesindeki NCCIC arasındaki işbirliği her iki bakanlığın da müşterek sorumluluğunda olacaktır.

Bu kapsamda, İç Güvenlik Bakanlığı ile Savunma Bakanlığı arasındaki işbirliğinin fiilen NSA üzerinden yürütüleceği bir yapıyı oluşturan söz konusu mutabakat zaptı ile; ABD'nin ulusal güvenliğinden -NSA-, ulusal savunmasından -Savunma Bakanlığı- ve iç güvenliğinden -İç Güvenlik Bakanlığı- öncelikli olarak sorumlu olan federal kurumlar, siber güvenliğin ulusal çapta sağlanması amacıyla bir araya gelmekte ve siber güvenlik çabalarını koordineli bir şekilde yürütme iradesini ortaya koymaktadırlar.

3. KOLLUK KUVVETLERİNİN GÜÇLENDİRİLMESİ

Çalışmanın önceki kısımlarında da ortaya konulduğu üzere, 11 Eylül Saldırıları sonrasında özellikle asimetrik tehditler bağlamındaki ve iç güvenlik alanındaki tehdit algılamalarında ciddi bir artış meydana gelmiştir. ABD'deki istihbarat ve güvenlik aygıtının da yeniden yapılandırılmasına yol açan bu durumun diğer bir etkisi de federal, eyalet ve yerel seviyedeki kolluk kuvvetleri üzerinde ortaya çıkmıştır. Bu kapsamda ABD Vatanseverlik Yasası örneğinde de olduğu gibi, güvenlik tehditleri ile mücadelede kendisine dayanılan yasal mevzuat -ağırlıklı olarak- istihbarat ve güvenlik kaygıları üzerinden federal kurumlar ve görevliler lehine değişikliğe uğrarken; güvenlik tehditleri ile "suç" boyutunda da mücadele edilmesine yönelik olarak ortaya çıkan temel eğilimin, kolluk kuvvetlerinin sahip oldukları suçla mücadele kapasitesinin özellikle teknik ve mali açıdan iyileştirilmesine odaklanmış olması dikkat çekmektedir.

Bu kapsamda 11 Eylül Saldırıları sonrasında federal, eyalet ve yerel kolluk kuvvetlerinin geçirmiş oldukları değişim, Lois M. Davis ve çalışma arkadaşları tarafından 2010 yılında hazırlanmış olan RAND raporu ile oldukça geniş bir perspektiften incelenmiş olup; bahse konu rapora göre söz konusu dönem içerisinde kolluk kuvvetleri ciddi bir değişim geçirmişlerdir (Davis ve diğerleri, 2010: xix):

> **"Kolluk Kuvvetlerinin Terörle Mücadeleye Yönelik İşlevleri Geliştirilmiştir**
>
> 11 Eylül Saldırıları öncesinde, kolluk kuvvetlerinin suç istihbaratı faaliyetlerinin odağı örgütlü suç, beyaz yaka suçları veya çeteler gibi belirli suç tiplerinin üzerindeydi. 11 Eylül Saldırıları sonrasında kolluk kuvvetlerinin odağı, aynı zamanda terörist tehditleri de içerecek biçimde geliştirilmiştir."

Karşı karşıya olunan durumu *"kültürel ya da paradigmal bir kayma"* olarak nitelendiren Davis ve çalışma arkadaşları, yaşanılan değişimin örgütlenme üzerindeki etkilerine de vurgu yapmaktadırlar.

Bu kapsamda özellikle terörle mücadele ve iç güvenlik ile ilişkili faaliyetlerde bulunmak üzere neredeyse her seviyede birçok birimin kurulduğunu ifade eden Davis ve çalışma arkadaşları (2010: xxii); bahse konu faaliyetlerin koordinasyonundan, bilgi paylaşımından ve istihbaratın işlenmesinden sorumlu olan füzyon merkezlerinin oluşturulmasına ve güçlendirilmesine yönelik eğilime ise özellikle dikkat çekmektedirler.

11 Eylül Saldırıları sonrasında terörle mücadele ve iç güvenlik faaliyetlerinin artan önemine bağlı olarak kolluk kuvvetlerinin sağladıkları kazanımlara örnek olarak, kriz yönetimi kapasitesinin artmasını, eğitim ve farkındalık programlarının başlatılmasını, Özel Taktik Müdahale Birimlerinin oluşturulmasını, mali yardımların yönetiminde verimliliğin arttırılmasını, füzyon merkezleri oluşturulmasını, teçhizat ve teknoloji alımlarına daha fazla kaynak ayrılmasını gösteren Davis ve çalışma arkadaşlarına göre (2010: xxxi):

> "Terörle mücadele ve iç güvenlik üzerindeki uzun süreli odaklanma yerel, eyalet ve federal seviyedeki kolluk kuvvetleri arasında çok daha geniş kapsamlı bir işbirliğine yönelik kültürel veya paradigmal bir kaymayı gösterir. Ki bu kayma, istihbarat bilgilerinin paylaşımında daha fazla açıklık ile sonuçlanmıştır."

Davis ve çalışma arkadaşları tarafından hazırlanmış olan bahse konu rapor bir bütün olarak değerlendirildiğinde; 11 Eylül Saldırıları sonrasında alınmış olan güvenlik tedbirlerine dayalı olarak gerek örgütlenme boyutunda, gerekse de teknik ve mali boyutta kolluk kuvvetlerinin ciddi kazanımlar sağladıkları görülmektedir. Bu kapsamda istihbarat ve güvenlik endişelerine dayalı olarak kazanılmış olan bu kapasitenin, terörizmin yanı sıra diğer suçlarla mücadele kapsamında da kullanılması gerektiğine ilişkin görüşlerin varlığı ise özellikle dikkati çekmektedir.

BEŞİNCİ BÖLÜM

SONUÇ, DEĞERLENDİRME VE ÖNERİLER

Asli kaygısı, herhangi bir teoriye veya hipoteze dayanmaksızın, bir durum tespiti yapmak ve objektif bir çerçeve çizmek olan böyle bir çalışmada, çalışma kapsamında konuya ilişkin olarak yapılmış olan her tespit esas itibariyle bir sonuç niteliği taşımaktadır. Bu çerçevede özellikle tehdit algısındaki kayma, istihbarat ve güvenlik aygıtının geçirdiği değişim ve yasal mevzuat üzerinden 11 Eylül Saldırıları ile ABD'deki -asimetrik- siber tehdit algısı ve güvenlik politikaları arasında kurulan ilişki, tez çalışmasının konu, kapsam ve bağlam açısından geçerliliğini sağlamaktadır.

Bununla birlikte, 11 Eylül Saldırıları sonrasında asimetrik tehditler ile siber güvenlik arasında kurulan ilişkinin genellikle "dolaylı" nitelikte olması, çalışmanın anlaşılırlığı üzerinde de etkili olmaktadır. Bu nedenle, çalışma kapsamında yapılmış olan bazı tespitlerin aşağıdaki biçimde, birarada ve bir bütün oluşturacak şekilde yeniden ele alınmaları; olgular, kavramlar ve terimler arasında var olduğu iddia edilen ilişkilerin ve etkileşimlerin daha net bir biçimde ortaya konulması bakımından faydalı olacaktır.

- "Savaş" olgusu sosyal, siyasal ve teknolojik nitelikli çeşitli faktörlerin etkisi altında değişime uğramaktadır. Bu kapsamda, -var olduğu iddia edilen- "Siber Savaş" ile "Konvansiyonel Savaş"ın eşit değer ve statüde kabul edilmeleri; teori, doktrin, eğitim ve hepsinden önemlisi hukuk boyutlarında benzer derinlikte tanımlanmış ve benimsenmiş olmalarını gerektirecektir. Dolayısı ile, bahse konu boyutlarda tam ve net bir şekilde tanımlanana ve benimsenene kadar, "Siber Savaş" olgusunun bir örtülü operasyon biçimi veya aracı olarak kabul edilmesi doğru olacaktır.

- Siber tehditlere ilişkin algılamalar; 11 Eylül Saldırıları öncesi dönemde ağırlıklı olarak -çıkar amaçlı- siber suçlar odaklı iken, 11 Eylül

Saldırıları sonrasındaki dönemde, özellikle "kritik altyapı tesisleri"nin korunmasını esas alan "iç güvenlik" anlayışının ağırlık kazanmasına paralel olarak karakteristik bir değişime uğramıştır.

- Tehdit algılamalarına ilişkin olarak yaşanılan söz konusu karakteristik değişiklik; güvenlik tehdidini yaratan muhtemel eylem biçimi üzerinden "asimetrik tehdit" ve "terörizm" kavramlarını, tehdit edilen cihaz ve bilgilerin nitelikleri üzerinden ise "enformasyon savaşı" ve "siber güvenlik" kavramlarını ön plana çıkartmaktadır.

- ABD'nin, 11 Eylül Saldırıları sonrasındaki dönemde geliştirdiği güvenlik politikaları kapsamında sıklıkla kullandığı "Savaş" söylemi; belirli teorik, askeri, politik ve hukuksal sonuçların elde edilmesini sağlamak maksadıyla yapılmış olan bilinçli bir tercihi yansıtmaktadır.

- 11 Eylül Saldırıları, gerek tehdit çerçevesinin çizilmesindeki ve somutlaştırılmasındaki rolü, gerekse de yeni hukuksal düzenlemelerin ve güvenlik politikalarının hayata geçirilmesi için açtığı "Fırsat Penceresi" ile ABD'deki -ve dünyanın geri kalan büyük bir kısmında ki- güvenlik politikaları için bir milat olmuştur.

- "Asimetri", "Terörizm" ve "Siber" gibi kavramlar güvenlik gündeminde ve tartışmalarında kendilerine artan bir şekilde yer bulmaktadırlar.

- Asimetrik tehditlerin nicel olarak arttığı ve nitel olarak çeşitlendiği küreselleşen bir dünyada terörizm, hem devletleri birbirleri ile işbirliği yapmaya zorlamakta hem de ulusal güvenliği sürekli ön planda tutmak suretiyle ulusal hükümetleri güvenlik boyutunda kuvvetlendirmektedir.

- 11 Eylül Saldırıları sonrasında ABD'de alınan terörle mücadele tedbirleri, federal hükümet lehine ciddi bir güç ve yetki artışına işaret etmektedirler.

- 11 Eylül Saldırıları sonrasında uygulamaya geçirilen güvenlik politikalarının ve alınan terörle mücadele tedbirlerinin özünde, "İç Tehdit"

algısı yer almaktadır. Bu çerçevede, Oklahoma Saldırısı yarattığı farkındalık açısından, 11 Eylül Saldırıları ise etkilerinin derinliği ve doğurduğu somut sonuçlar açısından önplana çıkmaktadır.

- 11 Eylül Saldırıları sonrasındaki dönemde ABD'de alınan terörle mücadele tedbirleri, özellikle kişi hak ve hürriyetlerini ihlal etmeleri noktasında eleştirilmektedir.

- Siber güvenliğe yönelik herhangi bir çerçeve yasanın bulunmadığı ABD'de, siber güvenlik politikaları üzerinde en büyük etkiye sahip olan yasal düzenlemeler; ABD Vatanseverlik Yasası ve İç Güvenlik Yasası'dır.

- ABD Vatanseverlik Yasası, tümüyle 11 Eylül Saldırıları sonrasında ortaya çıkmış olan travmatik algıları ya da tepkisel politikaları yansıtmaktan ziyade, önceki dönemlerde yaşanmış çok çeşitli ve çok sayıdaki terörizm tecrübesinden izler de taşıyan çok yönlü ve kapsamlı bir asimetrik tehdit algısını ve güvenlik yaklaşımını içermektedir.

- ABD'nin 11 Eylül Saldırıları sonrasında asimetrik tehditler bağlamındaki siber tehdit algısının özü ve alınan tedbirlerin niteliği; ABD Vatanseverlik Yasası'nın 1016.ncı maddesinde ABD Kongresi tarafından oldukça açık ve net bir şekilde ortaya konulmuştur.

- Enformasyon teknolojilerinin sürekli gelişmeye vurgu yapan karakteri ve çeşitli nedenlerle insanlar üzerinde yarattıkları bağımlılık olgusu gözönünde bulundurulduğunda, bu teknolojilere dayalı olarak gerçeklik kazanan somut veya soyut varlıkların güvenliklerinin sağlanması ihtiyacı, ister "Siber Güvenlik", isterse de "Enformasyon Güvenliği" olarak isimlendirilsin, yeni bir güvenlik sektörünün ortaya çıkmasına neden olmaktadır.

- "Siber Güvenlik" geniş bir perspektiften ele alındığında; çok daha kapsamlı bütünleri oluşturan "Ulusal Güvenlik" ve "Enformasyon Güvenliği" olgularının bir alt dalı olarak kendisini göstermektedir. Bu çerçevede, ulusal güvenliğinin sağlanması amaçlanan bir toplumun bilgisayar sistemleri ve ağlar ile bütünleşme seviyesi, ihtiyacını duyduğu

siber güvenliğin karakterini ve enformasyon güvenliği içerisindeki önemini de derinden etkileyecektir.

- Siber uzayın ve onunla bağlantılı olguların hukuksal statülerine ilişkin olarak "yeni bir hukukun oluşturulması" veya "varolan hukukun yeniden yorumlanması" arasında yapılacak olan tercih, siber uzay ve onunla bağlantılı olgular açısından hayati bir önem taşımaktadır.

- Siber güvenlik, siber uzaya ait olan sanal güvenlik boyutunun yanı sıra; "Kritik Altyapı Tesisleri"nin güvenliği üzerinden fiziki güvenlik, "Elektronik Savaş" ve "Tempest Radyasyonu" gibi olgular üzerinden ise cihaz güvenliği boyutlarına da sahiptir.

- ABD'deki siber tehdit algısı, çıkar amaçlı ve bireysel nitelikli "Siber Suçlar"dan, kritik altyapıya yönelik "Siber Sabotaj" odaklı bir "Siber Terörizm" anlayışına doğru kaymaktadır.

- Günümüz itibariyle, siber güvenlik alanında var olan hassasiyet ve zaafiyetlerin birincil kaynağı; "Ağ"lara duyulan bağımlılıktır.

- Kritik altyapı tesislerinde kullanılan -özellikle ağ bağlantılı- "SCADA Sistemleri", asimetrik nitelikli siber tehditlerin birincil hedefleridir.

- 1878 Tarihli Posse Comitatus Act, ABD Silahlı Kuvvetlerinin kanunların uygulanması maksadıyla ülke içerisinde kullanılmasını yasaklamaktadır.

- ABD'nin ulusal güvenliğini sağlamaya yönelik istihbarat ve güvenlik aygıtı, -siber tehditler de dahil olmak üzere- asimetrik tehditleri ABD içerisinde de karşılayacak biçimde, 11 Eylül Saldırıları sonrasındaki dönemde yeniden yapılandırılmıştır.

- Gerek yetki, gerekse de imkan ve kabiliyetler bağlamında ABD'nin siber tehditlere -ve büyük bir oranda da asimetrik tehditlere- yönelik mücadele kapasitesini; İç Güvenlik Bakanlığı (DHS), FBI, NSA ve ABD Siber Komutanlığı (USCYBERCOM) oluşturmaktadır. Bahse konu kurumlar içerisinde ise, gerek yetki ve sorumlulukları, gerekse de imkan ve kabiliyetleri bakımından NSA önplana çıkmaktadır.

- ABD'nin en kritik siber kabiliyetleri ve siber güvenlik kapasitesinin çok büyük bir kısmı; NSA Başkanının şahsında biraraya gelmektedir.

Aynı zamanda bu çalışmanın içerdiği araştırma sorularına verilen birer yanıt olma özelliği de gösteren yukarıdaki nesnel ve olgusal tespitler, "tehdit" ve "güvenlik" bağlamında ele alındıkları zaman ise; aşağıdakilere benzer bir dizi değerlendirmede bulunulması mümkündür.

Bu kapsamda, değişik görünümlere sahip olan -"gerilla savaşı", "gayri nizami harp" ya da "düşük yoğunluklu çatışma" olarak da adlandırılan- "asimetrik savaş" ve politik şiddetin en sık rastlanılan yansıması olan "terörizm" olgusu üzerinden somutlaşan "asimetrik tehditler"; küreselleşmenin devlet dışı aktörlere sağladığı avantajların ve postmodernitenin -devlet merkezli- düzeni sorgulayıcı yaklaşımının da itici etkisiyle, özellikle 11 Eylül 2001 tarihinden sonra, ulus devletlerin güvenlik gündemlerinde öncekinden çok daha merkezi bir yer işgal etmeye başlamışlardır. Bunun yanı sıra küreselleşmenin dolaylı bir sonucu olarak özellikle bilişim ve iletişim teknolojilerinin kullanımının küresel çapta yaygınlaşmasına paralel olarak anlam kazanan "siber uzay" olgusu, içerisinde yaşanılan fiziksel dünyaya paralel ve güvenlik açısından düzenlenmesi kaçınılmaz olan "sanal" bir gerçeklik yaratmıştır.

Böyle bir ortam içerisinde, ister enformasyon teknolojilerine dayalı ve teknoloji odaklı, isterse de çatışma taktiklerine dayalı ve insan odaklı olsun, "Savaş", "Tehdit" ve "Güvenlik" olgularının "Dördüncü Nesil Savaş" kavramı üzerinden açıklanabilecek bir değişim geçirmekte olduklarının ve bu değişim süreci içerisinde de, "asimetrik" niteliklerin ön plana çıkacağı bir biçimde evrildiklerinin ileri sürülmesi mümkündür. Söz konusu sürecin çok daha önemli bir diğer sonucu ise; ulusal güvenliğin sağlanması noktasında, organize suçlar ile mücadele üzerinden kolluk kuvvetlerini, belirsizliğin giderilmesi üzerinden istihbarat teşkilatlarını, kararlılık ve güvenlik kapasitesi üzerinden ise silahlı kuvvetleri müştereken çalışmaya ve yakınlaşmaya mecbur bırakmasıdır. Tehditlerin nicel ve nitel çeşitliliğine dayalı olarak, tedbirlerin de nicel ve nitel çeşitliliğini yaratacak olan böyle bir yakınlaşma; hayatın neredeyse her alanında çok yönlü ve

disiplinlerarası yaklaşımların gerekliliği yansıtan bir anekdot olan "körlerin bir fili tarif etmesi" örneğindeki gülünç durumun benzerlerinin, çok daha kritik ve olumsuz sonuçlar doğurabilecekleri "ulusal güvenlik" alanında da ortaya çıkmalarını engelleyecek olması açısından da son derece önemlidir. Elbette ki, varolduğu iddia edilen böyle bir değişimin ne kadar gerçek ve başarılı olduğunu ise; 1939 yılında Polonya'nın işgali örneğinde olduğu gibi, eski ve yeni model "güç"lerin karşı karşıya geldikleri -ironik bir biçimde asimetrik nitelikli olan- çatışma ortamları ortaya koyacaktır.

ABD örneği üzerinden değerlendirildiği zaman ise, ister intihar saldırısı yapmak, ister internet sitesi çökertmek, isterse de içeriden bilgi sızdırmak üzere, herhangi bir bireyin tek başına veya diğerleri ile biraraya gelerek ve örgütlenerek asimetrik tehdit üretebilme kapasitesine sahip olabileceği günümüz dünyasında; silahlı mücadele karakteri ön plana çıkan, "haklı" olması kadar "kutsal" olmasına da vurgu yapılan küresel boyuttta girişilmiş bir "Teröre Karşı Savaş"ın başarıya ulaşabilmesi için, başarı kriterlerinin akılcı ve net bir şekilde tanımlanmış olmasının gerekliliği açıktır.

Bu kapsamda, özellikle "asimetrik savaş" olgusunu tanımlayan kavramsal çerçeveye ve onun içerisinde yorumlandığı kuramsal yaklaşımlara ilişkin tartışmalar büyük önem kazanmaktadır. Zira gerek asimetrik tehditler, gerekse de onlarla mücadele kapsamında alınan güvenlik tedbirleri, hem kişilerin fiziki varlıklarını, hem de hak ve özgürlüklerini oldukça somut bir biçimde etkilemektedirler. Bu çerçevede, tam ve kesin olarak ne zaman sona ereceği belli olmayan bir mücadele kapsamında kendilerinden vazgeçilen "hak ve özgürlükler"in karşılığında mutlak bir güvenlik durumuna ulaşılabilmesinin de şüpheli olması, durumu çok daha karmaşık bir hale getirmektedir.

Hem devlet, hem de vatandaş açısından ideal olan şartlar altında; asimetrik tehditler bağlamında tehdit çerçevelerinin, güvenlik politika ve stratejilerinin belirlenmesinde "tehdit" ve "güvenlik" olguları olabildiğince geniş bir kapsamda ele alınarak yorumlanırken, uygulamalar ve sınırlayıcı hukuksal düzenlemeler boyutunda ise aynı olguların olabildiğince dar bir kapsamda ele alınmaları beklenilecektir. Böylelikle, azamileştirilen

"güvenlik" üretiminin kişiler üzerindeki olumsuz etkileri de asgari seviyede tutulacaktır. Günümüzün "önleyici müdahale" ya da "proaktif güvenlik" yaklaşımlarını bir anlamda işlevsizleştiren bu "ütopik" durumun da ortaya koyduğu gibi; tüm asimetrik tehditlerin yarattığı ortak ve en büyük tehlike, asimetrik tehditlerle mücadele sürecinin devlet ile vatandaşı karşı karşıya getiren "sıfır toplamlı oyun *(zero sum game)*" niteliği kazanma ihtimalidir.

Nitekim bu kapsamda, ABD'nin "Kurucu Babalar"ından Benjamin Franklin, *"Geçici güvenliklerini sağlamak için temel özgürlüklerinden vazgeçenler, ne özgürlüğü ne de güvenliği hakederler."* sözü ile, "Güvenlik" ve "Özgürlük" arasında bir tercih yapılmak zorunda kalınmasına ilişkin olarak -ABD açısından da oldukça ironik- bir tespitte bulunmaktadır. Amerikan İdealizminin, hak ve özgürlüklerin esas itibari ile ancak güvenliğin sağlanması durumunda anlam kazanacaklarını savunan "karşı grup" ile çatışmasının kaçınılmaz olduğu böyle bir noktada, asimetrik tehditlerle mücadelenin ABD için "politik ve ahlaki açıdan" sıfır toplamlı bir oyun halini alması da son derece doğaldır.

Yorucu, yıpratıcı, yüksek maliyetli ve uzun sürmesi kaçınılmaz olan "asimetrik tehditler ile mücadele" sürecinde, kullandığı aracın ismi ve niteliği ne olursa olsun, "güçlü" olanın -devlet- "güçsüz" olan -birey- lehine fedakârlıkta bulunarak uzun vadeli ve stratejik tercihler de bulunması; çoğu zaman için mücadelenin merkezinde yer alan kitlelerin "kalplerinin ve beyinlerinin kazanılması" noktasında oldukça önemli politik ve stratejik kazanımlar sağlayabileceği gibi, moral ve etik "doğruluk" iddiaları için de güçlü bir dayanak oluşturacaktır.

Bu tartışmaların güvenlik yönetimi açısından öneminin ortaya çıktığı nokta ise; güvenlik karar alıcısının, "tehdidi ortadan kaldırmak" üzere içerisinde yer aldığı politik, stratejik veya operasyonel karar alma süreçlerinin her hangi bir aşamasında "tehdidin varlığına ve ciddiyetine" ilişkin olarak yaptığı bir hatanın sonucu olarak, alınan güvenlik tedbirlerinin başarısız olmaları ve buna bağlı olarak da tehdidin ciddiyet kazanmasıdır. Bu kapsamda, girişilen başarısız müdahaleye bağlı olarak doğal akışından çıkan tehdidin öncekinden çok daha karmaşık bir hal alması ve kaotik bir ortam yaratması, söz konusu müdahale öncesinde var olan tehlikeyi daha

da büyütebilecektir. Toplumsal düzene ve ulusal güvenliğe yönelik olarak ortaya çıkabilecek bu olumsuz durumun yanı sıra -eğer varsa- güvenlik adına sınırlandırılmış olan kişi hak ve hürriyetlerine ilişkin olarak katlanılmış olan mahrumiyet ve yapılmış olan fedakarlıklar da tümüyle anlamsızlaşacaklardır.

Gerek bireysel, gerekse de örgütsel kaynaklı olarak neredeyse sınırsız sayıda asimetrik tehdidin yaratılabileceği ve somutlaşabileceği günümüz dünyasında, güvenlik yönetimindeki karar alma süreçleri ekonomi biliminin temel kavram ve kanunlarından olan "Alternatif Maliyet"[40] kavramı ve "Azalan Verim Kanunu"[41] üzerinden "fayda" ve "verimlilik" bağlamında ele alındıkları zaman; ulaşılabilir hedefler tespit etmek ve karar alma süreçlerinde rasyonellik sağlamak suretiyle asgari maliyet-karar sayısı ile asgari zamanda azami güvenliğin sağlanabileceği sonucuna ulaşılabilmesi mümkündür. Soyut olguların nicel ölçülebilirliği, "asgari" ve "azami" olanı tanımlayacak olan "başarı" nın görecelliliği, sosyal süreçlerde nesnelliğin mümkün olup olmadığı veya olması gerekip gerekmediği gibi pek çok noktada eleştiriye açık olan bu yaklaşım elbetteki idealize edilmiş bir karar alma sürecini yansıtmaktadır.

Dünyanın farklı yerlerinde farklı gelişmişlik seviyesinde toplumlar bulunduğu gibi aynı toplum içerisinde de farklı gelişmişlik seviyesinde insan grupları bulunabilmektedir. Dolayısı ile, gelişmiş olarak nitelenen toplum veya gruplar için tespit edilen yeni bir olgunun veya durumun geri kalmış olarak nitelendirilebilecek diğer bir toplum veya gruba ilişkin olarak tespit edilememiş olması, bahse konu "yeni" olgunun varlığının evrensel

---

[40] Prof.Dr. Erol Manisalı'ya göre (1996: 13);
"İnsanoğlunun gereksinmeleri sonsuz, buna karşılık, gereksinmeleri karşılayacak olanaklar sınırlı olduğuna göre, eldeki olanakların en uygun biçimde kullanılması, değerlendirilmesi zorunluğu ortaya çıkar.
Eldeki olanakları değerlendirirken gerek birey, gerek firma, gerekse devlet olarak seçim (tercih) yapmak durumu söz konusudur. Birey, şu veya bu işi tutmak veya (A) ya da (B) malını almak alternatifleri ile karşı karşıya bulunduğu zaman bir seçim de ortaya çıkar. Bu bakımdan iktisat bilimini seçim yapma, tercihte bulunma diye tanımlayan iktisatçılara da rastlanır.
Değişik almaşıklar arasında seçim yapmak demek, seçimi yapan birim (birey, firma, devlet) açısından kaynakların veya olanakların 'en iyi kullanılması' anlamına da gelir."

[41] Prof.Dr. Erol Manisalı'ya göre (1996: 39-40);
"İktisatta azalan verim kanununun anlamı şudur; belirli varsayımlar altında, üretim faktörlerinden biri arttırılırken diğeri 'sabit' tutulur ise, ürün (hasıla) artışı, belirli bir noktadan sonra, 'azalarak artan bir seyir' gösterir. Hatta söz konusu üretim faktörlerindeki artış devam eder ise, ürün artışı yerine, azalma durumu ortaya çıkar.
Azalan verim kanununun esası şuna dayanmaktadır. Herhangi bir malın üretimi için kullanılan üretim faktörlerinin 'en uygun' ya da "optimal" bir birleşim oranı, kompozisyonu vardır."

olarak inkar edilmesini gerektirmediği gibi, "eski" olguların sonsuza kadar varolacaklarının kabul edilmesini de gerektirmemektedir. Bu çerçevede "siber uzay ve onun güvenliğinin sağlanması" sorunu da inkâr edilemeyecek bir gerçeklik olarak ortaya çıkmaktadır.

Nihai olarak, bu çalışmanın bütününe yönelik genel bir değerlendirme yapılması durumunda ise, -indirgemeci bir yaklaşımı içermekle birlikte- aşağıdaki sonuca ulaşılabilmesi mümkündür.

Küreselleşen ve hızla enformasyon teknolojilerine bağımlı hale gelen günümüz dünyasına "dördüncü nesil savaş" konseptine dayanan bir güvenlik perspektifinden bakılması, olağanüstü tedbirleri gerektiren asimetrik tehditleri neredeyse olağanlaştırmaktadır. Böyle bir ortam içerisinde, dengesizlik, düzensizlik ve teknoloji temelinde ciddi bir değişim geçiren ve asla ortadan kalkmayacak olan "Güvenlik" ihtiyacının karşılanabilmesi için ise, bazı hak ve özgürlüklerden "Hukuk" ile tespit edilmiş olan şekil ve esaslar çerçevesinde fedakârlık edilmesi kaçınılmazdır. Bu kapsamda, gerek güvenliğin -gerçek anlamda- azamileştirilebilmesi, gerekse de kişi hak ve özgürlükleri üzerindeki olumsuz etkilerin asgarileştirilebilmesi için, güvenlik politika ve stratejilerine yönelik beklentilerin gerçekçi ve net olması bir gerekliliktir. Bu çerçevede karşı karşıya kalınan asıl ve kritik sorun ise; temel haklar istisnasız bir biçimde korunurken güvenliğin azamileştirildiği ve özgürlük kaybının asgarileştirildiği bir denge durumunun amaçlanıp amaçlanmadığı ve güvenlik ihtiyacı üzerinden meşrulaştırılan gözetleyici ve kısıtlayıcı düzenlemelerin bazı "örtülü" politik amaçlar için istismar edilip edilmediğidir.

Her ne kadar, ABD Kongresinin asimetrik tehdit ve siber güvenlik tartışmaları içerisindeki rolü, ABD Kongresi tarafından oluşturulan "ABD'ye Yapılan Terörist Saldırılara İlişkin Ulusal Komisyon" ya da siber güvenliğe yönelik uluslararası işbirliği ve hukuksal düzenleme girişimleri gibi başlıkların bu çalışma kapsamında ihmal edildiklerinin ileri sürülmesi mümkün ise de; bahse konu başlıklar, ayrı çalışmalara konu olması ve derinlemesine incelenmesi gereken oldukça geniş kapsamları nedeniyle bilinçli olarak çalışma kapsamı dışında bırakılmışlardır. Benzeri bir

biçimde, 11 Eylül Saldırıları sonrasında yürürlüğe konulan yasal düzenlemelere ilişkin yargı kararları da "olay incelemesi" biçiminde ele alınmayı zorunlu kılmaları nedeniyle çalışmanın kapsamı dışında tutulmuşlardır. Dolayısı ile, gerek ABD Kongresi ve 9/11 Komisyonu, gerekse de yasal düzenlemelere ilişkin yargı kararları ile ilgili olarak yapılacak akademik çalışmaların, hem bu çalışma için tamamlayıcı nitelikte olacakları, hem de önemli bir araştırma boşluğunu dolduracakları değerlendirilmektedir.

KAYNAKÇA

AKTÜRK, Uğur. **Amerika Birleşik Devletleri'nin Öldürücü Olmayan Silah/Silah Sistemleri Politikaları** (Yüksek Lisans Tezi), Sakarya, Sakarya Üniversitesi Sosyal Bilimler Enstitüsü, 2006.

ANDERSON, Sean K. ve Stephen SLOAN. **Historical Dictionary of Terrorism,** Lanham, Scarecrow Press, 2009.

Atomic Energy Act of 1954, Aug. 30, 1954, Public Law 83-703, 68 Stat. 919.

BARKER, Jonathan. **The No-Nonsense Guide to Terrorism,** Oxford, New Internationalist Publications, 2003.

BIDGOLI, Hossein (Ed). **The Internet Encyclopedia, Volume: 2,** New Jersey, John Wiley & Sons, 2004.

BIRKLAND, Thomas A. **An Introduction to the Policy Process:Theories, Concepts, and Models of Public Policy Making,** New York, M.E.Sharpe Inc., 2010.

BOEREE, C. George. "Abraham Maslow, 1908-1970", **Shippensburg Üniversitesi Resmi İnternet Sitesi,** 2006, <http://webspace.ship.edu/cgboer/maslow.html>, 02.03.2012.

BUZAN, Barry, Ole WAEVER ve Jaap De WILDE. **Security: A New Framework for Analysis,** Colorado, Lynne Rienner Publishers, 1998.

CASTELLS, Manuel. **The Rise of the Network Society: The Information Age: Economy, Society, and Culture Volume I,** West Sussex, Wiley-Blackwell, 2010.

CCRC İnternet Sitesi. "Cyberterrorism: The Real Risk", 2002, <http://www.crime-research.org/library/Robert1.htm>, 16.04.2012.

CLARKE Richard A. ve Robert K. KNAKE. **Siber Savaş: Ulusal Güvenliğe Yönelik Yeni Tehdit,** (Çev. Murat ERDURAN), İstanbul, İstanbul Kültür Üniversitesi, 2011.

Cornell Üniversitesi Hukuk Fakültesi Resmi İnternet Sitesi. "18 USC § 1029 – Fraud and Related Activity in Connection with Access Devices", 2012a, <http://www.law.cornell.edu/uscode/text/18/1029>, 11.04.2012.

Cornell Üniversitesi Hukuk Fakültesi Resmi İnternet Sitesi. "18 USC § 1030 – Fraud and Related Activity in Connection with Computers", 2012b, <http://www.law.cornell.edu/uscode/text/18/1030>, 11.04.2012.

Cornell Üniversitesi Hukuk Fakültesi Resmi İnternet Sitesi. "18 USC § 1385 – Use of Army and Air Force as Posse Comitatus", 2012c, <http://www.law.cornell.edu/uscode/text/18/1385>, 16.04.2012.

Cornell Üniversitesi Hukuk Fakültesi Resmi İnternet Sitesi. "18 USC § 2332B – Acts of Terrorism Transcending National Boundaries", 2012ç, <http://www.law.cornell.edu/uscode/text/18/2332b>, 20.04.2012.

Cornell Üniversitesi Hukuk Fakültesi Resmi İnternet Sitesi. "18 USC § 3127 - Definitions for Chapter", 2012d, <http://www.law.cornell.edu/uscode/text/18/3127>, 20.04.2012.

Cornell Üniversitesi Hukuk Fakültesi Resmi İnternet Sitesi. "18 USC § 3583 – Inclusion of a Term of Supervised Release After Imprisonment", 2012e, <http://www.law.cornell.edu/uscode/text/18/3583>, 11.04.2012.

Cornell Üniversitesi Hukuk Fakültesi Resmi İnternet Sitesi. "44 USC § 3502 – Definitions", 2012f, <http://www.law.cornell.edu/uscode/text/44/3502>, 16.04.2012.

CORNISH, Paul, David LIVINGSTONE, Dave CLEMENTE ve Claire YORKE. **On Cyber Warfare: A Chatham House Report,** London, Royal Institute of International Affairs, 2010.

DAVIS, Lois M, Michael POLLARD, Kevin WARD, Jeremy M. WILSON, Danielle M. VARDA, Lydia HANSELL ve Paul STEINBERG. **Long-Term Effects of Law Enforcement's Post-9/11 Focus on Counterterrorism and Homeland Security,** Santa Monica, RAND Corporation, 2010.

Dayton Üniversitesi Resmi İnternet Sitesi. "Federal Grand Juries", 2003a, <http://campus.udayton.edu/~grandjur/fedj/fedj.htm> 16.04.2012.

Dayton Üniversitesi Resmi İnternet Sitesi. "What is a Grand Jury?", 2003b, <http://campus.udayton.edu/~grandjur/faq/faq1.htm> 16.04.2012.

Department of the Army. **U.S. Army Guerrilla Warfare Handbook,** New York, Skyhorse Publishing, 2009.

Dictionary of Sociology. "Post-modernism", Oxford, Oxford University Press, 2009, 585.

Department of Homeland Security (DHS). **National Infrastructure Protection Plan: Partnering to Enhance Protection and Resiliency,** Washington, DC, DHS, 2009.

DHS Resmi İnternet Sitesi. "About the National Protection and Programs Directorate", 2011a, <http://www.dhs.gov/xabout/structure/editorial_0794.shtm> 08.04.2012.

DHS Resmi İnternet Sitesi. "Memorandum of Agreement Between The Department of Homeland Security and The Department of Defense Regarding Cybersecurity", 2010a, <http://www.dhs.gov/xlibrary/assets/20101013-dod-dhs-cyber-moa.pdf>, 09.04.2012.

DHS Resmi İnternet Sitesi. "National Cybersecurity and Communications Integration Center", 2011b, <http://www.dhs.gov/files/programs/nccic.shtm> 08.04.2012.

DHS Resmi İnternet Sitesi. "National Cyber Security Division", 2010b, <http://www.dhs.gov/xabout/structure/editorial_0839.shtm>, 08.04.2012.

DHS Resmi İnternet Sitesi. "Who Became Part of the Department?", 2012, <http://www.dhs.gov/xabout/history/editorial_0133.shtm>, 02.03.2012.

DOBROWOLSKY, Alexandra, Sandra ROLLINGS-MAGNUSSON ve Marc G. DOUCET. **"Security, Insecurity, and Human Rights: Contextualizing Post-9/11",** Sandra ROLLINGS-MAGNUSSON (Ed.), Anti-Terrorism: Security and Insecurity after 9/11, Nova Scotia, Fernwood Publishing, 2009, 13-31.

DOLNIK, Adam. **Understanding Terrorist Innovation: Technology, Tactics and Global Trends,** Oxon, Routledge, 2009.

DREYFUS, Hubert L. **On the Internet,** Oxon, Routledge, 2008.

DUNN CAVELTY, Myriam. **Cyber-Security and Threat Politics: US Efforts to Secure the Information Age,** Oxon, Routledge, 2008.

ECHEVARRIA II, Antulio J. **Fourth-Generation War and Other Myths,** Carlisle, Strategic Studies Institute, 2005.

ELSEA, Jennifer. "The Posse Comitatus Act and Related Matters: A Sketch", **Naval History & Heritage Command (United States Navy) Resmi İnternet Sitesi,** 21.02.2006, <http://www.history.navy.mil/library/online/posse%20comit.htm>, 16.04.2012.

Encyclopedia Britannica Online. "Posse Comitatus", **Encyclopedia Brittannica,** 2012, <http://www.britannica.com/EBchecked/topic/471943/posse-comitatus>, 16.04.2012.

EUSTIS, Joanne D. **Agenda-Setting: The Universal Service Case** (Doktora Tezi), Blacksburg, Virginia Polytechnic Institute and State University, 2000.

FAHRENKRUG, David T. "Cyberspace Defined", **Air University (United States Air Force) Resmi İnternet Sitesi,** 2007, <http://www.au.af.mil/au/awc/awcgate/wrightstuff/cyberspace_defined_wri ghtstuff_17may07.htm>, 01.03.2012.

FARER, Tom J. "The Interplay of Domestic Politics, Human Rights, and U.S. Foreign Policy", Thomas G. WEISS, Margaret E. CRAHAN ve John GOERING (Eds.), **Wars on Terrorism and Iraq: Human Rights, Unilateralism, and U.S. Foreign Policy,** New York, Routledge, 2004.

FBI Resmi İnternet Sitesi. "Color of Law Abuses", <http://www.fbi.gov/about-us/investigate/civilrights/color_of_law>, 11.04.2012.

FISCHER, Eric A. **Federal Laws Relating to Cybersecurity: Discussion of Proposed Revisions,** Washington, DC, Congressional Research Service, 2011.

FLORIDI, Luciano. **Philosophy and Computing: An Introduction,** London, Routledge, 1999.

FOREST, James J.F (Ed.). **Countering Terrorism and Insurgency in the 21st Century: International Perspectives,** Westport, Praeger Security International, 2007.

FrameWorks Institute İnternet Sitesi. "The FrameWorks Perspective: Strategic Frame Analysis", 2012, <http://www.frameworksinstitute.org/perspective.html>, 24.03.2012.

GIDDENS, Anthony. **Ulus-Devlet ve Şiddet,** (Çev. Cumhur ATAY), İstanbul, Devin Yayınları, 2005.

GOPALAKRISHNAN, Kasthurirangan ve Srinivas PEETA. **Sustainable and Resilient Critical Infrastructure Systems: Simulation, Modeling, and Intelligent Engineering,** Berlin-Heidelberg, Springer-Verlag, 2010.

HELD, David ve Anthony McGREW. **Globalization/Anti-Globalization: Beyond the Great Divide,** Cambridge, Polity Press, 2007.

HELD, Virginia. **How Terrorism Is Wrong: Morality and Political Violance,** New York, Oxford University Press, 2008.

HOFFMAN, Frank G. **Conflict in the 21st Century: The Rise of Hybrid Wars,** Arlington, Potomac Institute for Policy Studies, 2007a.

HOFFMAN, Frank G. "4GW as a Model of Future Conflict", **Boyd 2007 Conference,** 13 July 2007, Warfare Since Boyd Panel Presentation, 2007b, <http://smallwarsjournal.com/blog/4gw-as-a-model-of-future-conflict >, 01.03.2012.

Homeland Security Act of 2002, H.R. 5005, Nov. 25, 2002, Public Law 107-296, 116 Stat. 2135-2321.

IC Resmi İnternet Sitesi. "Seventeen Agencies and Organizations United Under One Goal", 2012, <http://www.intelligence.gov/about-the-intelligence-community/>, 02.03.2012.

JANCZEWSKI, Lech J. ve Andrew M. COLARIK. **Managerial Guide for Handling Cyber-Terrorism and Information Warfare,** Hershey, Idea Group Publishing, 2005.

JOHNSTON, Hank ve John A. NOAKES. **Frames of Protest: Social Movements and the Framing Perspective,** Lanham, Rowman and Littlefield Publishers, 2005.

KAMIENSKI, Lukasz. "Electromagnetic Pulse (EMP)", Christopher H. Sterling (Ed.), **Military Communications: From Ancient Times to the 21st Century,** Santa Barbara, ABC-CLIO, 2008, 136-137.

Kaspersky Lab. İnternet Sitesi. "Kaspersky Lab and ITU Research Reveals New Advanced Cyber Threat", 2012, <http://www.kaspersky.com/about/news/virus/2012/Kaspersky_Lab_and_ITU_Research_Reveals_New_Advanced_Cyber_Threat>, 28.05.2012.

KOVACICH, Gerald L. ve Edward P. HALIBOZEK. **The Manager's Handbook for Corporate Security: Establishing and Managing a Successful Assets Protection Program,** Boston, Butterworth-Heinemann, 2003.

KUHN, Markus G. ve Ross J. ANDERSON. "Soft Tempest: Hidden Data Transmission Using Electromagnetic Emanations", David AUCSMITH (Ed.), **Information Hiding: Second International Workshop, IH'98 Portland, Oregon, USA, April 14–17, 1998 Proceedings,** Berlin-Heidelberg, Springer-Verlag, 1998, 124-142.

KUSHNER, Harvey W. **Encyclopedia of Terrorism,** Thousand Oaks, Sage Publications, 2003.

LaROUCHE, Jr., Lyndon H. "A Strategic View of European History Today: Globalization, The New Imperialism", **Executive Intelligence Review,** Volume: 32, Issue: 42, 28 October 2005, 4-35, <http://www.larouchepub.com/eiw/public/2005/2005_40-49/2005_40-49/2005-43/pdf/04-35_42_feat.pdf>, 02.03.2012.

LAWSON, Tony. **Sociology For A Level: A Skills-Based Approach,** London, Collins Educational, 1993.

LERNER, K. Lee ve Brenda WILMOTH LERNER (Eds.). **Encyclopedia of Espionage, Intelligence, and Security, Volume: 1,** Farmington Hills, Gale, 2004a.

LERNER, K. Lee ve Brenda WILMOTH LERNER (Eds.). **Encyclopedia of Espionage, Intelligence, and Security, Volume: 3,** Farmington Hills, Gale, 2004b.

LESSER, Ian O, Bruce HOFFMAN, John ARQUILLA, David RONFELDT ve Michele ZANINI. **Countering the New Terrorism,** Santa Monica, RAND Corporation, 1999.

LEWIS, James A. **Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats,** Washington, DC, Center for Strategic and International Studies, 2002.

MACIONIS, John J. **Sociology,** New Jersey, Prentice-Hall, 1997.

MANİSALI, Erol. **İktisada Giriş,** İstanbul, Der Yayınevi, 1996.

MARSH, Ian, John COCHRANE ve Gaynor MELVILLE. **Criminal Justice: An Introduction to Philosophies, Theories and Practice,** London, Routledge, 2004.

McCRIE, Robert D. **Security Operations Management,** Boston, Butterworth-Heinemann, 2001.

MIRABELLO, Mark. **Handbook for Rebels and Outlaws: Resisting Tyrants, Hangmen, and Priests,** Oxford, Mark MIRABELLO, 2009.

MOGHADDAM, Fathali M. **How Globalization Spurs Terrorism: The Lopsided Benefits of "One World" and Why That Fuels Violence,** Westport, Praeger Security International, 2008.

MORLEY, Deborah ve Charles S. PARKER. **Understanding Computers: Today and Tomorrow,** Boston, Cengage Learning, 2010.

MOSS, Robert. **"Urban Guerrilla Warfare"**, Sarkesian, Sam C. (Ed.), Revolutionary Guerrilla Warfare: Theories, Doctrines and Contexts, New Brunswick, Transaction Publishers, 2010, 475-506.

NCTC Resmi İnternet Sitesi. "About the National Counterterrorism Center", 2012, <http://www.nctc.gov/about_us/about_nctc.html>, 03.04.2012.

NSA/CSS Resmi İnternet Sitesi. "Central Security Service (CSS)", 2011a, <http://www.nsa.gov/about/central_security_service/index.shtml>, 08.04.2012.

NSA/CSS Resmi İnternet Sitesi. "Frequently Asked Questions About NSA - 10. What are the Differences between NSA/CSS' and U.S. Cyber Command's Roles?", 2011b, <http://www.nsa.gov/about/faqs/about_nsa.shtml#about10>, 08.04.2012.

New York Times Gazetesi İnternet Sitesi. "Pentagon to Consider Cyberattacks Acts of War", 31.05.2011, <http://www.nytimes.com/2011/06/01/us/politics/01cyber.html>, 02.01.2012.

New York Times Gazetesi İnternet Sitesi. "Obama Order Sped Up Wave of Cyberattacks Against Iran", 01.06.2012, <http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?_r=2&hp>, 02.06.2012.

NEWMAN, Edward. **A Crisis of Global Institutions: Multilateralism and International Security,** Oxon, Routledge, 2007.

ODNI Resmi İnternet Sitesi. "About the ODNI", 2011, <http://www.dni.gov/who.htm>, 08.04.2012.

ÖZÇELİK, Murat. **Elektronik Harp ve Sinyal Karıştırması** (Yüksek Lisans Tezi), Ankara, Gazi Üniversitesi Fen Bilimleri Enstitüsü, 2006.

Ponemon Institute. **Second Annual Cost of Cyber Crime Study: Benchmark Study of U.S. Companies,** Michigan, Ponemon Institute, 2011.

POMPER, Stephen D. **Asymmetric: Myth in United States Military Doctrine** (Yüksek Lisans Tezi), Fort Leavenworth, Kansas, Faculity of the US Army Command and General Staff Collage, 2004.

POSNER, Richard A. **Preventing Surprise Attacks: Intelligence Reform in the Wake of 9/11,** Lanham, Rowman and Littlefield Publishers, 2005.

PRADOS, John. "Covert Operations", Alexander DeConde, Richard Dean Burns ve Fredrik Logevall (Eds.), **Encyclopedia of American Foreign Policy, Volume: 1,** New York, Charles Scribner's Son, 2002, 387-396.

PRIEST, Dana ve William M. ARKIN. **Top Secret America: The Rise of the New American Security State,** New York, Little Brown and Company, 2011.

PUŞCAŞ, Vasile. "Management of Post-Crisis Global Interdependencies", **International Economics Congress on An Interdisciplinary Analysis of the Roles of Global Politics & Civil Society in International Economics,** Berlin, 04-07 February 2010, 2010 <http://www.culturaldiplomacy.org/academy/content/articles/biec/speakers/speakers-pages/files/Managing_the_Post_Crisis_Global_Economic_Interdependence_-_Dr._Puscas.pdf>, 04.03.2012.

RODIN, David. **"The Ethics of Asymmetric War",** Richard SORABJI ve David RODIN (Eds.). The Ethics of War: Shared Problems in Different Traditions, Aldershot, Ashgate Publishing, 2006, 153-168.

ROLLINGS-MAGNUSSON, Sandra. **"Security, Human Rights, and Social Justice: Where Do We Go From Here?",** Sandra ROLLINGS-MAGNUSSON (Ed.), Anti-Terrorism: Security and Insecurity after 9/11, Nova Scotia, Fernwood Publishing, 2009, 214-221.

RYAN, Charlotte. **Prime Time Activism: Media Strategies for Grassroots Organizing,** Boston, South End Press, 1991.

SAMUELS, Richard J. (Ed.). **Encyclopedia of United States National Security, Volume: 1,** Thousand Oaks, Sage Publications, 2006.

SCHAEFER, Richard T. **Sociology,** New York, McGraw-Hill Higher Education, 2005.

SEARLE, John R. **Speech Acts: An Essay in the Philosophy of Language,** Cambridge, Cambridge University Press, 1999.

SHEPPARD, Ben. **The Psychology of Strategic Terrorism: Public and Government Responses to Attack,** Oxon, Routledge, 2008.

SKIBELL, Reid. "Cybercrimes and Misdemeanors: A Reevaluation of the Computer Fraud and Abuse Act", **Berkeley Technology Law Journal,** Volume: 18, Issue: 3, 2003, 909-944.

TANWAR, S.P. **Information, Media and National Security** (Kurs Bitirme Tezi), New Delhi, National Defence College, 2005.

TEEPLE, Gary. **"Towards a Theory of Terrorism",** Sandra ROLLINGS-MAGNUSSON (Ed.), Anti-Terrorism: Security and Insecurity after 9/11, Black Point, Nova Scotia, Fernwood Publishing, 2009, 32-58.

TOWNSON, Michael. **Mother-Tongue and Fatherland: Language and Poliics in German,** Manchester, Manchester University Press, 1992.

TREGLIA, Philip. **Emerging Threat to America: Non-State Entities Fighting Fourth Generation Warfare in Mexico** (Yüksek Lisans Tezi), Monterey, Naval Postgraduate School, 2010.

TURNER, Michael A. **Historical Dictionary of United States Intelligence,** Lanham, Scarecrow Press, 2006.

Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) Act of 2001, H.R. 3162, Oct. 26, 2001, Public Law 107-56, 115 Stat. 272-402.

US-CERT Resmi İnternet Sitesi. "About Us", 2012a, <http://www.us-cert.gov/about-us/>, 08.04.2012.

US-CERT Resmi İnternet Sitesi. "Control Systems Security Program (CSSP) - Industrial Control Systems Cyber Emergency Response Team", 2012b, <http://www.us-cert.gov/control_systems/ics-cert/>, 08.04.2012.

USSC Resmi İnternet Sitesi. "About the Commission – Overview of the United States Sentencing Commission", 2012, "<http://www.ussc.gov/About_the_Commission/Overview_of_the_USSC/USSC_Overview.pdf> 19.04.2012.

USSS Resmi İnternet Sitesi. "About the U.S. Secret Service Electronic Crimes Task Forces", 2010a, <http://www.secretservice.gov/ectf_about.shtml>, 08.04.2012.

USSS Resmi İnternet Sitesi. "Criminal Investigations", 2010b, <http://www.secretservice.gov/criminal.shtml>, 08.04.2012.

USSS Resmi İnternet Sitesi. "ECTF Legislation", 2010c, <http://www.secretservice.gov/ectf_legislation.shtml>, 08.04.2012.

Van BERGEN, Jennifer. "The USA PATRIOT Act Was Planned Before 9/11", 20.05.2002, <http://www.globalissues.org/article/342/the-usa-PATRIOT-act-was-planned-before-911>, 16.04.2012.

Washington Post Gazetesi İnternet Sitesi. "Iran Acknowledges That Flame Virus Has Infected Computers Nationwide", 30.05.2012, <http://www.washingtonpost.com/world/national-security/iran-acknowledges-that-flame-virus-has-infected-computers-nationwide/2012/05/29/gJQAzlEF0U_story.html>, 30.05.2012.

WATERS, Gary, Desmond BALL ve Ian DUDGEON. **Australia and Cyber-Warfare,** Canberra, ANU E Press, 2008.

WEINER, Tim. **Legacy of Ashes: The History of the CIA,** New York, Doubleday, 2007.

Wired Dergisi İnternet Sitesi. "White House Cyber Czar: There Is No Cyberwar", 04.03.2010,

<http://www.wired.com/threatlevel/2010/03/schmidt-cyberwar/>, 24.03.2012.

WIKIPEDIA İnternet Sitesi. "Governance, Risk Management and Compliance(GRC)", 2012a, <http://en.wikipedia.org/wiki/Governance,_Risk_Management,_and_Compliance>, 26.03.2012.

WIKIPEDIA İnternet Sitesi, "New World Order (Politics)", 2012b, <http://en.wikipedia.org/wiki/New_world_order_(politics)>, 02.03.2012.

WIKIPEDIA İnternet Sitesi. "Pen Register", 2011a, <http://en.wikipedia.org/wiki/Pen_register>, 11.04.2012.

WIKIPEDIA İnternet Sitesi. "Security Information and Event Management(SIEM)", 2012c, <http://en.wikipedia.org/wiki/Security_information_and_event_management>, 26.03.2012.

WIKIPEDIA İnternet Sitesi. "Sunset Provision", 2012ç, <http://en.wikipedia.org/wiki/Sunset_provision>, 11.04.2012.

WIKIPEDIA İnternet Sitesi. "TEMPEST", 2012d, <http://en.wikipedia.org/wiki/TEMPEST>, 23.03.2012.

WIKIPEDIA İnternet Sitesi. "Trap and Trace Device", 2011b, <http://en.wikipedia.org/wiki/Trap_and_trace_device>, 11.04.2012.

WIKIPEDIA İnternet Sitesi. "Waco Siege", 2011c, <http://en.wikipedia.org/wiki/Waco_siege>, 06.03.2012.

WILKINSON, Paul. "The Role of the Military in Combatting Terrorism in a Democratic Society", **Terrorism and Political Violance,** Volume: 8, Issue: 3, 1996, 1-11, <http://www.tandfonline.com/doi/pdf/10.1080/09546559608427360>, 03.04.2012.

YALDA, Christine ve Jonathan WHITE. **"New Rules for a New Game: The Challenge of Preserving Human Dignity in a Shadow War",** Sandra ROLLINGS-MAGNUSSON (Ed.), Anti-Terrorism: Security and Insecurity after 9/11, Black Point, Nova Scotia, Fernwood Publishing, 2009, 59-82.

YAYCI, Esra. **Bilişim Suçları** (Yüksek Lisans Tezi), Ankara, Gazi Üniversitesi Sosyal Bilimler Enstitüsü, 2007.

ZALMAN, Amy. "The History of Terrorism", **About.Com İnternet Sitesi,** 2012, <http://terrorism.about.com/od/whatisterroris1/p/Terrorism.htm.>, 18.06.2012.