



**SİBER SALDIRILARA CEVAP OLARAK MEŞRU
SAVUNMA VE GÜÇ KULLANMANIN MEŞRUIYETİ:
YUMUŞAK HUKUKUN GRİ ALANINDA GEZİNMEK**

Yüksek Lisans Tezi

Büşra Ayşe Durkan

Eskişehir 2024

**SİBER SALDIRILARA CEVAP OLARAK MEŞRU SAVUNMA VE
GÜÇ KULLANMANIN MEŞRUIYETİ: YUMUŞAK HUKUKUN
GRİ ALANINDA GEZİNMEK**

Büşra Ayşe DURKAN

Yüksek Lisans Tezi

Uluslararası İlişkiler Anabilim Dalı

Danışman: Prof.Dr. Cenap Çakmak

Eskişehir

Anadolu Üniversitesi

Lisansüstü Eğitim Enstitüsü

Temmuz 2024

JÜRİ VE ENSTİTÜ ONAYI

Büşra Ayşe DURKAN'ın "Siber Saldırılara Cevap Olarak Meşru Savunma ve Güç Kullanmanın Meşruiyeti: Yumuşak Hukukun Gri Alanında Gezinmek" başlıklı tezi **12 Temmuz 2024** tarihinde, aşağıdaki jüri tarafından Lisansüstü Eğitim-Öğretim ve Sınav Yönetmeliğinin ilgili maddeleri uyarınca **Uluslararası İlişkiler Anabilim Dalı Uluslararası İlişkiler programında, yüksek lisans tezi** olarak değerlendirilerek kabul edilmiştir.

İmza

Üye (Tez Danışmanı) : Prof. Dr. Cenap ÇAKMAK

.....

Üye :Doç. Dr. Erhan AKDEMİR

.....

Üye :Doç. Dr. Mustafa Cüneyt ÖZŞAHİN

.....

Prof. Dr. Saime ÖNCE
Anadolu Üniversitesi
Lisansüstü Eğitim Enstitüsü Müdürü

ÖZET

SİBER SALDIRILARA CEVAP OLARAK MEŞRU SAVUNMA VE GÜÇ KULLANMANIN MEŞRUIYETİ: YUMUŞAK HUKUKUN GRİ ALANINDA GEZİNMEK

Büşra Ayşe DURKAN

Uluslararası İlişkiler Anabilim Dalı

Anadolu Üniversitesi, Lisansüstü Eğitim Enstitüsü, Temmuz 2024

Danışman: Prof.Dr. Cenap Çakmak

Siber savaş günümüzde gelişen teknolojiler ile ortaya çıkan geleneksel savaşın yerini alan bir çatışma türüdür. Siber silahların geleneksel silahlardan farklı olması ve devletlerin kritik altyapılarına saldırı yapabilme kapasitesine sahip olması nedeniyle kontrol altında tutulması önem arz etmektedir. Siber saldırıların devletler açısından büyük etkiler yaratması nedeniyle silahlı saldırı olarak kabul edilip edilmemesi konusu büyük tartışma yaratmaktadır. Bu durum hem ulusal hem de uluslararası alanda siber saldırılar ile ilgili hukuk kuralı koyma anlamında büyük değişimleri beraberinde getirmiştir. Tallinn Manual ve Budapeşte Sözleşmesi uluslararası alanda yapılan sözleşmeler iken NIS Directive (Network and Information Security Directive veya Ağ ve Bilgi Güvenliği Yönergesi) ve Cyber Act (Siber Güvenlik Yasası) Avrupa Birliği sınırları içinde oluşmuş hukuk kurallarını içermektedir. Siber alan ile ilgili bu sözleşmeler yumuşak hukukun bir parçası olmuştur. Devletler siber saldırıların uluslararası hukuktaki yerini sert hukuk kapsamında değerlendirmekte zorlanabilmektedir. Fakat yumuşak hukuk uygulamalarının sert hukuka evrilebildiği örnekler uluslararası ilişkilerde yer almaktadır. Bu çalışmanın amacı, devletlerin bir siber saldırıyla karşılaştığı zaman Birleşmiş Milletler Sözleşmesi'nin 51.maddesine dayanarak meşru müdafaa ve kuvvet kullanma hakkının olup olmadığını ve yumuşak hukuk kurallarının siber saldırılarda mevzuat oluşturma konusunda etkili olup olmadığını nitel yöntem kullanarak incelemektir.

Anahtar Sözcükler: Siber saldırılar, Meşru Müdafaa ve Kuvvet Kullanma, Tallinn Manual, Yumuşak ve Sert Hukuk

ABSTRACT

LEGITIMATE DEFENSE AND THE LEGITIMACY OF THE USE OF FORCE IN RESPONSE TO CYBER ATTACKS: NAVIGATING THE GRAY AREA OF SOFT LAW

Büşra Ayşe Durkan

Department of International Relations

Anadolu University, Institute of Postgraduate Education, July 2024

Advisor: Prof. Dr. Cenap Çakmak

Cyber warfare is a type of conflict that replaces traditional warfare, which has emerged with developing technologies today. It is important to keep cyber weapons under control because they are different from traditional weapons and have the capacity to attack the critical infrastructures of states. Since cyber attacks have great effects on states, the issue of whether they should be considered as armed attacks or not creates great debate. This situation has brought about major changes in terms of establishing legal rules regarding cyber attacks both nationally and internationally. While the Tallinn Manual and the Budapest Convention are international agreements, the NIS Directive (Network and Information Security Directive) and the Cyber Act include the legal rules formed within the borders of the European Union. These agreements regarding cyberspace have become part of soft law. Cyber attacks have a place in international relations. States may have difficulty evaluating this issue within the scope of hard law. However, there are examples in international relations where soft law practices can evolve into hard law. The purpose of this study is to examine whether states have the right to self-defense and use force based on Article 51 of the United Nations Charter when faced with a cyber attack, and whether soft law rules are effective in creating legislation on cyber attacks, using a qualitative method.

Key Words: Cyber attacks, Self-Defense and Use of Force, Tallinn Manual, Soft and Hard Law

TEŞEKKÜR

Yüksek lisansın ders döneminde uluslararası hukuk dersinde yapacağım meşru müdafaa ve kuvvet kullanma adında bir sunumun tez konum için bana fikir vereceğini ve bu konu hakkında tez yazacağımı bilmiyordum. Uluslararası hukuk dersini anlatan Prof.Dr. Elif Uzun’a tez konum hakkında destekleri için çok teşekkür ediyorum.

Tez danışmanım Prof. Dr. Cenap Çakmak’a, tez sürecindeki yönlendirmeleri, destekleri ve sabrı için sonsuz teşekkür ediyorum. Kendisinin bilgi ve deneyimleri, tezimin bu noktaya gelmesinde önemli bir rol oynamıştır. Ayrıca tez jürim olan Doç.Dr. Erhan Akdemir ve Doç.Dr. Mustafa Cüneyt Özşahin hocalarıma verdikleri tavsiye ve yönlendirmeler için teşekkür ediyorum.

Tez yazma sürecim boyunca desteklerini esirgemeyen ve her zaman arkamda olmaları benim için mutluluk kaynağı olan aileme sonsuz teşekkür ediyorum. Bu süreç boyunca desteklerini her zaman üzerimde hissettiğim arkadaşlarıma minnettarım.

ETİK İLKE VE KURALLARA UYGUNLUK BEYANNAMESİ

Bu tezin Anadolu Üniversitesi Bilimsel Araştırma ve Yayın Etiği Yönergesi hükümlerine göre hazırlandığını; bana ait, özgün bir çalışma olduğunu; çalışmamın hazırlık, veri toplama, analiz ve bilgilerin sunumu olmak üzere tüm aşamalarında bilimsel etik ilke ve kurallara uygun davrandığımı; bu çalışma kapsamında elde edilen tüm veri ve bilgiler için kaynak gösterdiğimi ve bu kaynaklara kaynakçada yer verdiğimi; bu çalışmanın Anadolu Üniversitesi tarafından kullanılan “bilimsel intihal tespit programı”yla tarandığını ve hiçbir şekilde “intihal içermediğini” beyan ederim. Herhangi bir zamanda, çalışmamla ilgili yaptığım bu beyana aykırı bir durumun saptanması durumunda, ortaya çıkacak tüm ahlaki ve hukuki sonuçları kabul ettiğimi bildiririm.

Büşra Ayşe DURKAN

İÇİNDEKİLER

ÖZET	iii
ABSTRACT	iv
TEŞEKKÜR	v
ETİK İLKE VE KURALLARA UYGUNLUK BEYANNAMESİ	vi
İÇİNDEKİLER	vii
TABLOLAR DİZİNİ	x
KISALTMALAR DİZİNİ	xi
GİRİŞ	1
BİRİNCİ BÖLÜM	3
YUMUŞAK HUKUK	3
1.1. Yumuşak Hukuk Kavramının Tanımı ve Evrim Süreci	3
1.2. Uluslararası Hukukta Yumuşak Hukukun İşlevi	5
1.3. Yumuşak Hukuk ve Küresel Yönetişim	6
1.4. Yumuşak Hukuk ve Sert Hukuk: Farklılıklar ve Etkileşimler	7
İKİNCİ BÖLÜM	9
KUVVET KULLANIMI VE MEŞRU MÜDAFAA	9
2.1. Kuvvet Kullanımı ve Meşru Müdafanın Tanımı ve Değişen İçeriği	9
2.2. Ön Alıcı Meşru Müdafaa (Preemptive) ve Önleyici Meşru Müdafaa (Preventive) Kavramları	12
2.3. Meşru Müdafanın Varsayılan Koşulları	13
2.3.1. Aciliyet ilkesi	14
2.3.2. Orantılılık ilkesi	14
2.3.3. Gereklilik ilkesi	15
2.4. Meşru Müdafaa Hakkının Kullanımına İlişkin Örnekler	15
2.4.1. Falkland adası harekâtı	15
2.4.2. Arap-İsrail savaşları	16
2.4.3. Amerika'nın Irak'ı işgali	18
2.4.4. Rusya'nın Ukrayna'yı işgali	19

2.4.5. Rusya'nın Gürcistan'ı işgali.....	21
ÜÇÜNCÜ BÖLÜM	24
SİBER SALDIRI TÜRLERİ VE SİBER SALDIRILARDA MEŞRU MÜDAFAA VE KUVVET KULLANIMI	24
3.1. Siber Savaş Kavramının İncelenmesi	24
3.2. Siber Saldırı Türleri	25
3.2.1. Hizmet engelleme saldırıları (DDos saldırıları).....	26
3.2.2. Kimlik avı (Phishing)	26
3.2.3.Yemleme kancası (Spear phishing).....	26
3.2.4. Ortadaki adam (Man in the middle attack).....	27
3.2.5. Fidyeye yazılımı (Ransomware).....	27
3.2.6. Kripto hırsızlığı (Cryptojacking).....	27
3.2.7. Kötü amaçlı yazılım (Malware)	28
3.2.7.1. Virüs.....	28
3.2.7.2. Solucan (Worm)	28
3.2.7.3. Truva atı (Trojan horse)	29
3.2.7.4. Mantık bombası (Logic bomb)	29
3.2.7.5. Arka kapı (Backdoor).....	29
3.2.7.6. Rootkit.....	30
3.3.Siber Saldırılarda Meşru Müdafaa ve Kuvvet Kullanımı	31
DÖRDÜNCÜ BÖLÜM	34
SİBER SALDIRILARA UYGULANACAK OLAN HUKUK	34
4.1. Tallinn Manual ve Siber Saldırıların Uygulanacak Olan Hukuk	34
4.1.1. Devletin gerçekleştirdiği siber saldırılar	35
4.1.2. Denizde yapılan siber saldırıların durumu	37
4.1.3. Hava sahalarında gerçekleştirilen siber saldırıların durumu	40
4.1.4. Uzayda gerçekleştirilen siber saldırıların durumu	41
4.1.5. Uluslararası hukuka göre dokunulmazlıktan yararlanan konumları hedefleyen saldırılar	42
4.1.6. Önleyici savaş kavramının siber saldırılarda geçerlilik durumu	43
4.1.7. Diplomatik ve konsolosluk hukuku temsilcileri tarafından gerçekleştirilen siber saldırılar	44
4.1.8. İnsan hakları hukukuna aykırı yapılan siber saldırılar	44

4.2. Avrupa Konseyi Siber Suçlar Sözleşmesi	44
4.3. Siber Suçlar Üzerine BM Genel Kurul Kararları.....	46
4.3.1. 57/239 numaralı karar	47
4.3.2. 58/199 numaralı karar	47
4.3.3. 55/63 numaralı karar	48
4.3.4. 74/247 numaralı karar	49
4.3.5. 73/27 numaralı karar	49
4.4. Avrupa Birliği ve Siber Güvenlik Kararları	50
4.4.1. Avrupa Birliği siber güvenlik yasası (Cyber act)	51
4.4.2. Avrupa Birliği siber dayanıklılık yasası (Cyber resilience act)	52
4.4.3. Avrupa Birliği siber güvenlik stratejisi (Cyber security strategy)	53
4.4.4. Ağ ve bilgi sistemleri direktifi (NIS directive)	53
4.5. Uluslararası İnsancıl Hukuk ve Siber Saldırıları.....	54
4.6. Uluslararası Ceza Mahkemesinin Siber Saldırı Kararları.....	55
BEŞİNCİ BÖLÜM	57
SİBER SALDIRILARA ÖRNEKLER.....	57
5.1. Stuxnet Saldırısı	57
5.2. Titan Rain	60
5.3. Estonya Saldırısı.....	64
5.4. Duqu Saldırısı.....	67
SONUÇ.....	69
KAYNAKÇA	72

TABLÖLAR DİZİNİ

Tablo 3.1. Kötü Amaçlı Yazılımların Bilgisayarlara Bulaş Oranı.....30

Tablo 4.1.2005'ten 2022'e Kadar Devlet Destekli Olduğundan Şüphelenilen Siber Operasyonların Sayısı, Seçilmiş Ülkeler.....36

Tablo 5.1. Çinlilerin İzinsiz Girişleri ile İlgili Raporlama.....62



KISALTMALAR DİZİNİ

BM: Birleşmiş Milletler

NATO: North Atlantic Treaty Organization

UAD: Uluslararası Adalet Divanı

NIEO: New International Economic Order

OECD: Organisation for Economic Co-Operation and Development

G-8: Group of Eight

PISA: Programme for International Student Assessment

AB: Avrupa Birliği

DTÖ: Dünya Ticaret Örgütü

GATT: General Agreement on Tariffs and Trade

BMGK: Birleşmiş Milletler Genel Kurulu

CIA: Central Intelligence Agency

UCM: Uluslararası Ceza Mahkemesi

CCDCOE: Cooperative Cyber Defence Centre of Excellence

MEB: Münhasır Ekonomik Bölge

ENISA: European Network and Information Security Agency

ICTC: International Criminal Tribunal for Cyberspace

GİRİŞ

Modern zamanların en iyi icadı olan bilgisayar ve ardından gelen internetin icadı, insanların hayatını kolaylaştırırsa da birtakım zorlukları beraberinde getirmiştir. Bilgisayar sistemlerinin gelişmesi ve bilgisayarlar arası saldırıların yapılması siber alan kavramını ortaya çıkarmıştır. Siber alanda saldırılar yapılmaya başlanmış ve bu saldırılar bireysel olmaktan çıkıp devletlerarası saldırılar olarak da gerçekleşmeye başlamıştır. Siber saldırı kavramları üçe ayrılır bunlar; siber suç (cyber crime), siber saldırı (cyber attack) ve siber çatışma (cyber warfare) olarak adlandırılır. Siber suç bilgisayar ortamında işlenen herhangi bir suç olarak tanımlanır. Siber saldırı ise politik bir amacı olup bilgisayar üzerinden işlenen suçların genel adıdır. Siber çatışma ise siber saldırıların silahlı saldırı boyutuna ulaşmış hali anlamına gelmektedir. Siber saldırı ve siber çatışma konuları politik konuları içerdiği için uluslararası ilişkilerde bu konulara daha çok değinilmektedir.

Devletler bu saldırıların önlenmesi aşamasında hem iç hukuk hem de uluslararası hukuk sistemlerini kullanarak mevzuat oluşturma girişimine başlamış ve devam ettirmektedirler. Siber saldırılar için mevzuat oluşturmak devletlerarası gerçekleşebilecek olan saldırılarda meşru müdafaa ve kuvvet kullanımının hangi koşullarda sağlanabileceği üzerine bir çerçeve oluşturmak oldukça önemlidir. İlk olarak var olan mevzuatta neler yazdığını belirtmek önem taşımaktadır. Birleşmiş Milletler Şartı 2/4 maddesinde, devletlerin kuvvet kullanması yasaklanmıştır ve siber saldırıları da bu maddenin içine dahil etmek mümkündür. Bu maddenin istisnası olan 51.maddede devletlerin meşru savunma hakkının olduğundan bahsedilmektedir. Silahlı saldırıya varan siber saldırılarda meşru müdafaa hakkı gereklilik, orantılılık ve aciliyet kriterlerine dayandığı sürece yapılabilmektedir (Hathaway, Crootoof, Levitz, Nix, Nowlan, Perdue ve Spiegel, 2012, s.838-841).

Siber saldırıların önlenmesi için konulan kurallar genellikle yumuşak hukuk kurallarına dayanmakta olup, siber saldırılar ile ilgili herhangi bir sert hukuk girişi bulunmamaktadır. Geleneksel saldırıların azaldığı ve siber saldırıların da arttığı bu

dönemde siber alanın düzenlenebilmesi için belirli kurallara ihtiyaç vardır. Bu ihtiyacın karşılanması için NATO iş birliğine dayalı Siber Savunma Mükemmeliyet Merkezi'nin 2010 yılında oluşturduğu, Uluslararası Uzmanlar Grubu tarafından 95 kuraldan oluşan Tallinn Manual oluşturulmuştur. Her ülkeden uzmanların katılımıyla oluşturulan bu belge uluslararası nitelik taşımaktadır (Lotrionte, 2018, s.76-78). 2016 yılı haziran ayında ise Tallinn Manual 2.0 yayınlanmış ve ilk yayınlanan belgeye göre bazı değişimler olmuştur. Örneğin, ilk yayınlanan belgeye göre Tallinn Manual'i yazan uzmanlar grubu çeşitliliği artmış ve Batılı uzmanlar yanında Doğulu (Çin, Belarus, Japonya) gibi yerlerden uzmanlarda katılmıştır. İlk versiyonuna göre Tallinn Manual'in içeriği genişletilmiştir ve uluslararası hukuktaki özel rejimlerde siber saldırılar durumunda nasıl bir yol izleneceği konusu detaylıca incelenmiştir (Jensen, 2017, s.737-739). Siber alan ile ilgili uluslararası nitelik taşıyan bir başka belge, 2007 yılında yürürlüğe giren, Avrupa Siber Suçlar Sözleşmesi diğer adıyla Budapeşte Sözleşmesidir. Bu belgeler siber hukukun oluşması için emsal niteliği taşıyabilecek belgeler olarak tanımlanabilir. Bu belgeler sert hukuk niteliği taşımadığı için devletler tarafından henüz davranış kuralları olarak yerleşmemiştir. (McGhee, 2014, s.30).

Bu tez çalışmasında, birinci bölümde yumuşak hukukun tanımı ve sert hukuk ile ayırdımı, ikinci bölümde kuvvet kullanma tanımı ve kuvvet kullanmaya örnekler, üçüncü bölümde siber saldırı türlerinin incelenmesi, dördüncü bölümde siber saldırılara uygulanacak olan hukukların incelenmesi ve beşinci bölümde siber saldırılarda örnek olayların incelenmesine değinilecektir.

BİRİNCİ BÖLÜM

YUMUŞAK HUKUK

1.1. Yumuşak Hukuk Kavramının Tanımı ve Evrim Süreci

Uluslararası hukuk, devletlerin otorite yokluğunda düzeni kurmak üzere yetki vererek oluşturduğu kurallar zinciridir. Devletler uluslararası bir üst otoritenin kurulması için yetki vermekte oldukça çekingen davranabilmektedir. Devletler otoritenin düzenlediği kurallara tâbii olmak isterler fakat diğer yandan bu kurallar devletlerin rahat hareket edememesine neden olduğu için kuralların varlığından rahatsız olmaktadır (Westerman, Hage, Kirste ve Mackor, 2018, s.245). Devletlerin tâbii olduğu kuralların oluşturulmasında uluslararası hukukun kaynakları önemlidir. Uluslararası hukukun kaynaklarına BM'nin yargı organı olan Uluslararası Adalet Divanı Tüzüğü'nün 38. maddesinde değinilmiştir. 38.maddede uluslararası hukukun kaynaklarının bağlayıcı kaynaklar ve yardımcı kaynaklar olarak ikiye ayrılmasından bahsedilmektedir. Bağlayıcı kaynaklar, uluslararası antlaşmalar, hukukun genel ilkeleri ve yapılageliş kuralları olarak belirtilmektedir. Yardımcı kaynaklar ise mahkeme kararları ve uzmanların görüşleri olarak ikiye ayrılmaktadır (Uluslararası Adalet Divanı Statüsü, 1945).

Birleşmiş Milletler gibi uluslararası kuruluşlar hem bağlayıcı hem de bağlayıcılığı olmayan kurallar oluşturabilmektedir. Birleşmiş Milletler Güvenlik Konseyi'nin aldığı kararlar bağlayıcı nitelik taşımaktadır. Birleşmiş Milletler tarafından yayınlanan 1948 İnsan Hakları Evrensel Bildirgesi, UAD Tüzüğü'nün 38.maddesine göre kanun olarak sayılmamaktadır. Diğer bir deyişle bildirge bağlayıcı nitelik taşımamaktadır. Fakat insan hakları alanında devletlerin kanun gibi önem verdiği ve uyguladığı bir belge olarak tarihe geçmiştir. Başka bir anlaşma olan 1970 tarihli "Dostça İlişkiler ve İşbirliğine İlişkin Uluslararası Hukuk İlkeleri Bildirgesi" de insan hakları bildirgesi gibi bağlayıcı olmayan fakat devletler arasında kanun gibi yer edinen belgeler arasında yer almaktadır (Westerman, Hage, Kirste ve Mackor, 2018, s.247-249).

Bağlayıcılığı olmayıp devletlerin davranışlarını düzenleyen kurallar yumuşak hukukun alanına girmektedir. Yumuşak hukukun tanımı konusunda belirsizlikler bulunsa da en açıklayıcı tanımı şudur; yasal açıdan herhangi bir güce bağlanmayan fakat diğer yandan yasal etki meydana getirebilecek davranış kurallarına yumuşak hukuk denmektedir (Senden, 2004, s.111-113). Yumuşak hukuk kavramı olduğu gibi sert hukuk kavramı da literatürde yer almaktadır. Sert hukuk ile belirli bir otoritenin dayattığı katı kurallar ifade edilmekte olup bu kurallara uyulmadığında yaptırım ile karşılaşılacağı kastedilmektedir. Yumuşak hukuk ve sert hukuk birbirlerini tamamlayan iki unsur olarak düşünülebilir. Yumuşak hukukun kapsadığı belgeler şunlardır; konferanslarda sunulan bildiriler, uluslararası olan örgütlerin kararları (BM Şartı 25.maddede Güvenlik Konseyi'nin aldığı bağlayıcılığı olan kararlar hariç), uluslararası sözleşmeler, yönergeler, konferans kararları ve planlar. Başlangıçta yumuşak hukuk enstrümanları dikkate alınmazken, zamanla yumuşak hukukunda sert hukuk kadar etkili olabildiği görüldüğünde yumuşak hukuk alanlarında da çekince kullanılmaya başlanmıştır. Amerika'nın Rio Deklarasyonundaki 7.maddeye çekince koyması bu duruma verilebilecek en iyi örnektir. Amerika çevre alanında herhangi bir sorumluluk almak ve iş birliği içinde olmak istemediği için bu maddeye çekince koydurmuştur. Bu açıdan bakıldığında artık bağlayıcı belgelerin verdiği zorunlu sorumluluk, bağlayıcı olmayan belgelerin verdiği isteğe bağlı sorumluluk ile eş değer hale gelmiştir (Bailliet, 2012, s.202-205).

Yumuşak hukuk kavramı yeni ve esnek bir kavram olduğu için devletler tarafından kötüye kullanılabilme olasılığı yüksektir. Fakat Rio Deklarasyonu veya İnsan Hakları Bildirgesi örneğinde olduğu gibi bazı durumlarda da yumuşak hukuk sert hukuk kadar ciddiye alınabilecek durumlar yaratabilir. BM tarafından kabul edilen 1972 Stockholm Deklarasyonu da yumuşak hukuka örnek olarak verilebilmektedir. Bu deklarasyon sayesinde devletler hem ulusal hem de uluslararası alanda çevrenin kirletilmesini önleme ve koruma çalışmalarını beraberlik içerisinde sürdürme kararını almışlardır. Uluslararası Hukuk Enstitüsü tarafından 1961 Uluslararası Deniz Kullanımına İlişkin Kanun, 1979 Nehirlerin ve Göllerin Kirlenmesi ve Uluslararası Hukuka İlişkin Kanun ve 1987 Uluslararası Korumaya İlişkin Kanun ile çevresel alanda yumuşak hukukun uygulanması yaygınlaştırılmıştır. Ticari alanda esnek yasallaştırmaya örnek vermek gerekirse “Yeni Uluslararası Ekonomik Düzen (NIEO)” verilebilir. Amerika tarafından yayınlanan belge bağlayıcılığı olmayan belge niteliği taşımaktadır buradaki kurallar

devletler tarafından zamanla içselleştirilerek esnek yasallaştırmaya zemin hazırlamıştır. Bu örneklere bakıldığında yumuşak hukukun güç ve etkisinin yadsınamaz olduğu görülmektedir (Handl, Reisman, Simma, Dupuy ve Chinkin, 1988, s.371-393).

1.2. Uluslararası Hukukta Yumuşak Hukukun İşlevi

Yumuşak hukuk, uluslararası hukukun önemli bir parçası haline gelmiştir. Birleşmiş Milletler ve G8 gibi kuruluşlarda yumuşak hukukun kullanım alanları giderek yaygınlaşmıştır. Yumuşak hukukun esnek yasallaşması sayesinde konulan kuralların teamül hukukuna evrilmesinin sağlanabilmesi uluslararası örgütlerin dikkatini çekmiştir. Yumuşak hukuka devletler tarafından uyulmaması durumunda, sert hukuka nazaran ağır bir yaptırımla karşılaşılmamaktadır. Ayrıca yumuşak hukuk ile ilgili herhangi bir dava açılıp Uluslararası Adalet Divanı'nın önüne getirilmemektedir. Örneğin, OECD tarafından üç senede bir yapılan PISA anketi, 15 yaşındaki çocukların eğitiminin ölçme ve değerlendirilmesi üzerine yapılan bir ankettir. Bu anketin devletler üzerinde herhangi bir zorlama ve otoritesi yoktur fakat devletler bu ankette sıralamalarını değiştirebilmek için eğitim alanında yeni düzenlemeler yapabilmektedir. Farklı bir deyişle, örf ve âdet hukukuna karşı gelindiğinde uygulanan yaptırım toplum tarafından dışlanma veya ayıplanma oluyor ise devletler tarafından örf ve âdet hukukuna karşı gelmek devletler tarafından küçümsenmek gibi anlamlara gelebilmektedir. Örf ve âdetin kurduğu bu soyut otorite sayesinde devletler yumuşak hukukta bile olsa kendilerini diğer devletler tarafından baskı altında hissedebilmektedir (Goldmann, 2012, s.335-339).

Yumuşak hukukun esnek bir hukuk türü olmasından dolayı devletler tarafından göz ardı edilme olasılığı yüksektir. Fakat her yumuşak hukuk enstrümanı farklı önem ve derecelere sahiptir. Genellikle yumuşak hukuk uluslararası hukukta kullanılsa da iç hukukta da kullanıldığına dair örnekler bulunmaktadır. Yumuşak hukukun uluslararası hukuktaki örnekleri 1970'lerde başlamış ve zamanla artmaya devam etmiştir. Örneğin, çevre alanında yapılan ilk yumuşak hukuk belgesi olarak Stocholm Deklarasyonu gösterilebilir. Hukuk literatürüne bakıldığında genelde yumuşak hukukun çevre alanında kullanıldığı görülse de başka alanlarda da yumuşak hukukun kullanıldığı görülebilir. Yumuşak hukuk sayesinde devletler kararları kolay ve maliyetsiz alabilmektedir (Ahmed ve Mustofa, 2016, s.1-14).

1.3. Yumuşak Hukuk ve Küresel Yönetişim

Yönetişim, ulusal hükümetlerin geniş bir alana yayılarak uluslararası alanda bir yönetim sağlaması anlamına gelmektedir. Yönetişim kavramı yumuşak hukukun uygulanabilirliği açısından oldukça önemli bir kavramdır. Yönetişim ve yumuşak hukuk bu nedenle birbirinden ayrılamayan ve birbirini tamamlayan iki parça olarak görülebilir. Yumuşak hukuk sayesinde küresel yönetişimin sürdürülmesinin sağlanması için yeni aktörler devreye girmektedir (Elia Antonio, Aho ve Stefan, 2021, s.22-24). 1970 yılında Herman Haken tarafından ortaya atılan sinerji teorisi işbirlikçi yönetim tarzının öneminden bahsetmektedir. Teoride yönetişimde önemli olan aktörlerin devlet, kolluk kuvvetleri, sosyal kuruluşlar, şirketler ve bireyler olduğu belirtilir. Bu aktörlerden en aktif olanların ise şirketler ve devletler olduğuna dikkat çekilmektedir (The Communist Party of China News, 2015)

James Rosenau'ya göre, küresel yönetim kavramı aileden başlayıp uluslararası kurum ve kuruluşları kapsamaktadır. Aktörlerin arasındaki etkileşimin devamlı ve sürdürebilir olması uluslarüstü bir yönetişimin kurulmasında oldukça önemlidir. Fakat uluslararası aktörlerin etkileşiminde ve normların aktörler için etkili olmadığı durumlarda küresel yönetişimin etki alanı sınırlanmış olur.

Küresel yönetişimde uluslararası kurum ve kuruluşların önemi yadsınamaz bir gerçektir. Uluslararası örgütler yönetişimin sağlanması üzerine hem yumuşak hukuk hem de sert hukuktan faydalanmaktadır. Örneğin, Avrupa Birliği tarafından 2000 yılında düzenlenen bir zirvede Lizbon Stratejisi adı verilen bir plan kabul edilmiş ve bu plan AB ülkelerine ekonomi, hizmet ve çevre konularında yeniden yapılandırma getirmiştir. Lizbon stratejisi adı verilen plan, açık koordinasyon yöntemi (Open method of coordination) kullanılarak yapılmıştır. Açık koordinasyon yönteminin amacı, AB üyesi devletlerin ekonomi, hizmet ve çevre konularında ne kadar aşama kaydettiğinin izlenmesi ve bu alanlarda gelişim gösteren devletlerin paylaşılarak diğer devletlere örnek olmasının sağlanmasıdır. Bu metot sayesinde AB, üyelerinin belirli alanlarda neler yaptıklarını rahatlıkla izleyebilecek ve üye devletler ise kendi aralarında yaptıkları çalışmalar ile öne çıkmak isteyeceklerdir. Daha önce PISA anketi örneğini ele almıştık ve burada da benzer nitelikte bir durum yer almaktadır. Çünkü PISA anketi de devletlerin özgür iradelerine dayalı olmakta ve herhangi bir yaptırım bulunmamaktadır.

Fakat devletlerarası bir rekabete sebep olmasından dolayı, devletler baskı altında hissedebilir ve eğitim alanında yeniden yapılandırma için çaba gösterebilirler (Filipovic ve Buncic, 2015, s.103-s.114).

1.4. Yumuşak Hukuk ve Sert Hukuk: Farklılıklar ve Etkileşimler

Yumuşak hukuk bağlayıcı olmayan hukuk anlamına geldiği gibi sert hukuk ise bağlayıcılığı olan ve uygulanmadığında cezai yaptırımı olan hukuk türü anlamına gelmektedir. Uluslararası alanda otorite sahipleri genellikle sert hukukun uygulanmasını yumuşak hukuka göre daha çok tercih ederler. Sert hukukun taahhütlere bağlı güvenilir bir dayanak olması ve aktörlerin eylemlerini bazen de egemenliklerini kısıtlayabilecek durumda olması sert hukuku otoriteler tarafından tercih edilebilir kılmaktadır. Fakat yumuşak hukuk devletlere fazla sorumluluk yüklediğinden dolayı devletlerin daha ılımlı baktığı bir hukuk türüdür.

Yumuşak hukukun yapısı itibariyle esnek olması çoğu zaman eleştirilmiş ve bu sistemin yaygınlaştırılması halinde hukukun istikrarını kaybedebileceği düşünülmektedir. Fakat sert hukuka ulaşılması yolunda yumuşak hukuk bir basamak olarak kullanılabilir. Yumuşak hukuk yolu kullanılarak uluslararası aktörlerin üzerinde otorite kurduktan sonra yumuşak hukuku sert hukuka dönüştürebilmek daha kolay olabilir. Sert hukukta otoritenin etkin bir biçimde yer alması ve yetki paylaşımı olduğu için aktörler yetkilerini devretmek konusunda isteksiz davranabilmektedir. Yumuşak hukukun sert hukuka dönüşme evresi esnek yasallaşma olarak adlandırılabilir. Esnek yasallaştırmanın sözleşme maliyeti, sert hukukun yasallaştırılmasına göre daha düşüktür. Örneğin, Uluslararası Çalışma Örgütü sözleşme maliyetlerinin düşük olması nedeniyle artık bağlayıcı olmayan anlaşmaların ortaya atılmasına önem vermiştir. Başka bir örnek ise Dünya Ticaret Örgütü'nün hazırladığı sert taslak hukuk yerine GATT gibi daha yumuşak hukuka dayalı bir anlaşma kabul edilip GATT'ın giderek geliştirilmesidir (Abbott ve Snidal, 2000, s.421-436).

Sert hukuk araçları devletlerin iç hukukuna transforme edildiğinde etki alanı oldukça genişlemektedir. Hem uluslararası alanda hem de ulusal alanda sert hukuk uygulandığında caydırıcılığın etkisi yüksektir. Bu etki sayesinde devletler otoriteye karşı olsa da sert hukukun güvenilir bir liman olduğunu düşünmektedirler. Fakat sert

hukuk araçlarının egemenliği sınırlandırması konusu hassas alanları da içerebildiği için devletlerin taahhütlerinin alınması zorlaşabilir. Bu süreç hem maliyetli hem de uzun olabilmektedir. Günümüzde koşulların hızlıca değişiklik göstermesi ile sert hukuk enstrümanlarının bu koşullara ayak uydurabilmesi güç olabilmektedir. Sert hukuka dayalı bir anlaşma değişikliğe uğradığı düşünüldüğünde bu anlaşmanın yeniden düzenlenmesi ve devletlerden taahhütlerin yeniden alınması gerekebilir.

Rasyonalist ve inşacı akademisyenler yumuşak hukukun farklı noktalarına odaklanmaktadır. Rasyonalist akademisyenler yumuşak hukukun sözleşme maliyetlerini azaltmasına odaklanırken, inşacı akademisyenler yumuşak hukuk sayesinde devletlerin sosyalleşme, tartışma ve ikna etme aşamalarını kolaylaştırdığını söylemektedir. Ayrıca rasyonalistler de yapılandırmacılar gibi yumuşak hukukun ortak bir girişimcilik ruhu yarattığını belirtmektedir. Sert ve yumuşak hukuk araçlarının her ikisinin de devletlere yararı bulunabilir. Fakat yumuşak hukukun sert hukuka dönüşme süreci devletler için az maliyetli ve devletlerin hür iradesine bağlı olduğu için devletlerde daha özgür ve otorite olmadan kuralları bağlı olma eğilimi gösterebilmektedir (Shaffer ve Pollack, 2010, s.717-721).

İKİNCİ BÖLÜM

KUVVET KULLANIMI VE MEŞRU MÜDAFAA

2.1. Kuvvet Kullanımı ve Meşru Müdafanın Tanımı ve Değişen İçeriği

Kuvvet kullanma kavramı silahın kullanılmasıyla oluşan zorlama halini içermektedir. Devletler tarih boyunca savaşmış ve savaşmanın gereği olarak gördükleri kuvvet kullanımına ihtiyaç duymuşlardır. Fakat kuvvet kullanımı yasağı kavramının uluslararası hukukta yer alması, Birinci Dünya Savaşı sonrası Wilson Prensiplerine dayalı olarak kurulan Milletler Cemiyeti Misakı ile olmuştur (Bozkurt, 2003, s.6). Misak'taki 2, 13 ve 15. maddeler, devletlerarası barışın sağlanması, uyuşmazlıkların çözümü ve yetki sınırlandırması konularına değinmektedir. Kuvvet kullanma konusuna ise Misak'ın 16.maddesinde değinilmekte olup, kuvvet kullanan Cemiyet üyesi devletlere uygulanacak olan yaptırımlardan bahsedilmektedir. 12, 13 ve 15. Maddelerde bir uyuşmazlık durumunda ilk önce hakem kararına başvurulması gerektiği ve bu başvuru süreci içerisinde savaşa girmenin mümkün olmadığı, hakemin verdiği karara uyan devlete karşı herhangi bir saldırıda bulunulmaması gerektiği ve uyuşmazlığın boyutunun hakem kararını aştığı zaman ise durumun Genel Sekreter aracılığı ile Meclis'e taşınması gerektiğini söylemektedir. 17.maddede Cemiyet'e üyeliği bulunmayan ülkelerin aralarında yaşadığı sorunlarda ise bu sorunların çözümünde Misak'taki kurallara başvurmaları üzerine yol gösterilecek olup, kendilerine yol gösterilmesini isteyen devletlerin Misak'ta geçen kurallara tabii olabileceğinden bahsetmektedir. Ayrıca maddede Cemiyet'e üye olmayıp anlaşmazlık karşısında Cemiyet'ten yol göstermesini beklemeyen devletlere karşı Konsey'in önlem alabileceğinden söz etmektedir (Milletler Cemiyeti Misakı, 1935).

Daha sonra kuvvet kullanmanın sınırlandırılması üzerine adını ABD Dışişleri Bakanı Frank B. Kellogg ve Fransa Dışişleri Bakanı Aristide Briand'tan alan, Briand-Kellogg Paketi ortaya çıkmış ve antlaşma 24 Temmuz 1929 da yürürlüğe girmiştir

(Lesaffer,2011, s.1-2). Bu antlaşma iki dünya savaşı arasında çatışmanın olmamasını ve barışın istikrarlı bir şekilde devam etmesini sağlamıştır. Hem Misak'ta hem de Briand-Kellogg Paktında savaş kelimesine rastlanmamıştır. Briand-Kellogg Paktı savaşın önlenmesi ve barışın sağlanması konusunda Birleşmiş Milletler Antlaşması'nın temelini oluşturmuştur (Williams,1935, s.346-348). Fakat bu barış süreci İkinci Dünya Savaşı ile tekrardan bozulmuş ve antlaşma önemini yitirmiştir. İkinci Dünya Savaşı'nın sonunda Birleşmiş Milletler kurulmuş ve Milletler Cemiyeti'nin Misakına karşılık "Birleşmiş Milletler Antlaşması" adı altında kurallar oluşturulmuştur. BM Antlaşması da Misak da yer verildiği gibi kuvvet kullanımına değinmiştir. BM Antlaşmasının 2/4 maddesine göre BM üyelerinin bir başka devletin iç işlerine karışmaması ve o devlete karşı kuvvet kullanmaması gerektiği belirtilmiştir. Bu maddenin istisnası olarak BM Antlaşması 51.madde göz önünde bulundurulmaktadır (Ruys, 2010, s.53-58). 51.maddeye göre devletlerin herhangi bir silahlı saldırıya maruz kalması durumunda, maruz kalan devlet bireysel veya ortak savunma hakkına sahiptir (Keskin, 1998, s.22-35).

Kuvvet kullanma kavramının Milletler Cemiyet'i ile ortaya çıktığı görülse de bu kavramın kullanılması antik çağlara dayanmaktadır. Antik Roma'da kuvvet kullanımı konusu "haklı savaş" kavramıyla öne çıkmaktadır. Haklı savaş kavramının mimarları Thomas Aquinas ve Saint Augustine'dir (Elshtain, 1992, s.8-10). Haklı savaş kavramında, adından da anlaşılacağı üzere, haklı bir sebebe sahip olmak savaşın tek ve geçerli sebebi sayılırdı. Modern ulus devletlerin ortaya meydana çıkmasıyla birlikte haklı savaş diye bir kavram geçerliliğini yitirmiş ve devletler herhangi bir sebep olmadan kuvvet kullanmaya başlamışlardır (Lango, 2014, s.3-5). 16.yy. ve 20.yy. arasında devletler özgürlük içinde kuvvet kullanmaya devam etmiştir. 1899-1907 La Haye Sözleşmeleri'nde kuvvet kullanma nedeniyle ortaya çıkan ağır kayıpların engellenmesi için önlem alınmıştır fakat kuvvet kullanmaya sınırlama getirilmemiştir. Drago-Porter Doktrini ile birlikte kuvvet kullanma tekrardan sınırlandırılmaya başlanmış bir devletin diğer devletten alacağı varsa ve bu ödenmediyse kuvvet kullanmanın sınırlandırılması kararı getirilmiştir. Milletler Cemiyeti'nin kurulmasına kadar kuvvet kullanma konusunda belirli bir istikrar görülme de Milletler Cemiyeti'yle birlikte kuvvet kullanma belirli durumlar hariç tamamıyla sınırlandırılmıştır (Tosun, 2009, s.89-93).

Kuvvet kullanma yasağının istisnası olarak koruma sorumluluğu kavramı, uluslararası hukukta yeni bir kavram olarak literatüre girmiştir. Koruma sorumluluğu kavramı, bir devletin kendi halkını iç sorunlardan koruması anlamına gelmektedir. Eğer devlet halkını iç sorunlardan koruyamaz ise başka devlet veya devletlerin bu durumu uluslararası toplumun sorunu olarak görerek o devlete yardım etmesi insani müdahalenin alanına girmektedir. Koruma sorumluluğu kavramı, ilk olarak 15 Eylül 2005'te yapılan Dünya Zirvesi Sonuç Belgesi'nde yayımlandı. Ardından ise Güvenlik Konseyi'nin Silahlı Çatışmalarda Sivillerin Korunmasına Dair kararında koruma sorumluluğu kavramına yer verildi. Koruma sorumluluğu kavramı teoride bu şekilde yasallaştırıldı. Pratikte ise Libya Krizi ile yasallaştırılıp önemli hale geldi (Hilpold, 2014, s.1-3). Libya Krizi aracılığıyla koruma sorumluluğu kavramının yasallaştırılması konusu sadece bu belgelere dayanmayıp, BM Antlaşması 41 ve 42.maddeleri ve BMGK'nın 1970 ve 1973 kararını içermektedir (Şentuna, 2019, s.215-239). BM Şartı'nın 41.maddesinde Güvenlik Konseyi'nin kararlaştırdığı üzere silahlı bir müdahale olmadan Konsey, üyelerini bazı önlemler almaya davet edebildiği ve diplomasi yoluyla ilişkilerin kesilmesi, hava, deniz, kara yollarını kullanarak faaliyetlerde bulunulmasından bahsedilmektedir. BM Şartı'nın 42.maddesinde ise 41.maddede alınan önlemlerin zayıf kaldığı durumlarda uluslararası alanda barışın yeniden sağlanabilmesi için hava, deniz ve kara kuvvetleri aracılığıyla her türlü operasyonun yapılabileceğine değinilmektedir (Birleşmiş Milletler, 1945, s.14).

Ruanda ve Kosova'da yaşanan etnik çatışmalar koruma sorumluluğu kavramının üzerinde durulması için dönüm noktaları olmuştur. İki tarafta da yaşanan çatışmalardan ders alınarak BM Genel Sekreteri Kofi Annan'ın önerisiyle "Uluslararası Müdahale ve Devlet Egemenliği Komisyonu" kurulmuştur. Bu komisyon tarafından yayınlanan ilk raporda devletin sorumlulukları, olaylara hangi şartlarda müdahale edebileceği ve eğer müdahale edilmezse uluslararası toplumun devreye girebileceği açıkça belirtilmiştir (Glanville, 2012, s.9-10).

2018 yılında Myanmar'da yapılan soykırımı Rohingya halkı üzerine etnik temizlik yapıldı. Soykırım yapılırken Facebook uygulamasından grupların kurulduğu ve bu grupların kışkırtmaya yol açtığı Facebook tarafından açıklandı. Başka bir örnek olan Ruanda Soykırımında, radyolarda soykırımı destek mesajlarının yayınlanması ve soykırımla ilgili talimatların verilmesi ile kötü noktalara ulaştı. İki örnekte de iletişim

teknolojilerinin yarattığı en acımasız sonuçlar karşımıza çıkmaktadır. Fakat siber saldırılar iyi amaçlar için kullanıldığı zaman bu gibi eylemlerin ortaya çıkmasını önleyebilme kapasitesine sahiptir. Devletler koruma sorumluluğu kapsamında siber alandan yardım alabilirse koruma sorumluluğunu en iyi şekilde yerine getirebilirler (Switzer ve Park, s.113-127).

2.2. Ön Alıcı Meşru Müdafaa (Preemptive) ve Önleyici Meşru Müdafaa (Preventive) Kavramları

Meşru müdafaa kavramı, BM Antlaşması'nın 51. maddesinde belirtilmiş olup, maddede devletler meşru müdafaa hakkına sahip oldukları zaman ne gibi uygulamaları takip etmesi gerektiğinin açıklaması yapılmıştır. Meşru müdafaa kavramı ikiye ayrılmaktadır: 1) Ön alıcı meşru müdafaa 2) Önleyici meşru müdafaa (Dönmez, 2017, s.8-15). Ön alıcı meşru müdafaa bir saldırının gerçekleşmesi gerekir ve saldırıya maruz kalan taraf meşru müdafaa hakkını kullanır (Bunn, 2003, s.3). Önleyici meşru müdafaa ise potansiyel tehditlere karşı bu tehditleri önlemek üzere saldırının gerçekleştirilmesi demektir. Ön alıcı savaş kavramı uluslararası hukukta meşru kabul edilirken, önleyici savaş kavramının meşruluğu halen tartışılmaktadır. Önleyici savaş kavramı Bush Doktrini ile gündeme gelmiştir. Bush Doktrini, Osmanlı ile İtilaf Devletleri arasında imzalanan Mondros Ateşkes Antlaşmasına benzemektedir. Ateşkes antlaşmasının 7.maddesinde İtilaf Devletlerinin kendilerine tehdit olarak gördükleri yerleri işgal etme maddesi yer almaktadır. Bu madde önleyici savaş kavramına uyan bir örnektir. Önleyici savaş kavramının tanımlanması aslen Bush Doktrini'nin yayınlanmasıyla gerçekleşmiştir (Erkul, 2018, s.643-654).

Bush Doktrini, George W. Bush tarafından 2002 yılında yayınlanan dış politika tanımlayıcı bir belgedir. ABD işgal ettiği bölgelerde işgalini haklı bir sebebe ve yasal bir zemine dayandırmak için bu belgeyi oluşturmuştur (Luban,2004, s.207-209). 11 Eylül sonrası Amerika'nın dış politikası teröre karşı savaş açmak olmuştur. Bu düşünce itibarıyla ilk önce Afganistan'ın işgali ve ardından Irak'ın işgali meydana gelmiştir. Bu devletler, Doktrin'de "haydut devletler" olarak anılmakta ve bu haydut devletlerin uluslararası alanda bir tehlike yaratabileceği belirtilmiştir. Belgede haydut devletlerin kimyasal silahları olabileceği ve bu silahların ABD'yi hedef alabileceği de belirtilmiştir.

Bu ise Bush Doktrin'in "önleyici savaş" stratejisi bağlamında tehdit altında olduğunu belirten bir ifadedir. Bush Doktrininde bahsedilen önleyici savaşın gerekliliklerine göre ABD'nin tehdit altında gördüğü yerlere kuvvet kullanması meşru müdafaaya hâlel bir durum getirmeyecektir (Dündar, 2018, s.53-55).

Önleyici savaş için kayda değer örneklerden biri Arap-İsrail Savaşıdır. İsrail, kendisine silahlı saldırıda bulunmasını öngördüğü Mısır'ın bu saldırıya yeltenmemesi için Suriye, Ürdün, Mısır topraklarına sahip oldu. 242 sayılı karara dayanarak Konsey İsrail'in son çatışmada işgal edilen topraklardan çekilmesini talep etmiştir. Son çatışmada işgal edilen topraklardan çekilme kararı aynı zamanda önceki işgal ettiği toprakları onaylar niteliktedir. Saldırganlığın Tanımına İlişkin BM Kararı da bir devletin başka bir devletin topraklarında kuvvet kullanarak hak iddia etmesinin yanlış olduğunu vurgulamaktadır. Ayrıca İsrail'e yönelik herhangi bir kararın Birleşmiş Milletler Güvenlik Konseyi'nden çıkmasına ABD'nin veto verebilme ihtimali de unutulmamalıdır. Fakat aynı durumu Azerbaycan kendi topraklarını işgal eden Ermenistan için kullansa, Konsey Azerbaycan'ı kınayabilirdi (Aral, 1999, s.31).

Ön alıcı savaş ise bir devlet diğer bir devlete saldırdığı zaman saldırıya maruz kalan devletin o zamanda meşru müdafa hakkını kullanıp geri saldırı düzenlemesi anlamına gelmektedir. Bu kavrama örnek olarak Pearl Harbor saldırısı verilebilir. Japonya'nın 1941 yılında ABD'nin limanlarına saldırı düzenlemesi ABD için meşru müdafa hakkını oluşturmuştur. ABD ise 1945 yılında Japonya'ya karşı saldırı düzenlemiştir. Fakat BM'nin daha kurulmamış olması ve meşru müdafa kavramında aciliyet ilkesi diye bir kavramın henüz literatürde olmamasından dolayı ABD'nin bu saldırısı meşru sayılabilir (Hoover Institution, 2017).

2.3. Meşru Müdafaanın Varsayılan Koşulları

Devletlerin meşru müdafaaya başvurması gerektiğinde uyması gereken bazı ilkeler bulunmaktadır. Aciliyet, orantılılık ve gereklilik ilkeleri meşru müdafaanın gerçekleştirilebilmesinin şartları arasındadır. Aciliyet kavramı, meşru müdafaada tanımlanması zor olan bir ilkedir. Bir saldırı karşısında saldırıya ne zaman karşılık verileceği tartışma konusudur. Gereklilik ilkesi ise bütün barışçıl yollar denenmiş fakat sonuç alınamamışsa bu aşamada meşru müdafaanın gerekli olduğu anlamına

gelmektedir. Orantılılık kavramında ise yapılan bir saldırıya karşı meşru müdafaa yapılırken karşılık verme durumunun eşit oranda olmasıdır. Meşru müdafaa'nın varsayılan koşullarını detaylıca irdelemek, konunun anlaşılması ve istisnaların anlaşılması açısından oldukça önemlidir. Siber alanda hukuk kurallarının oluşturulma aşamasında önemli bir kaynak olan Tallinn Manual'deki Schmitt Kriterleri'nde de aciliyet kriterinden bahsedilmektedir. Yapılan siber saldırılarda saldırı boyutunun aşılp aşılmadığını belirlemek için hazırlanan Schmitt kriterlerinden biri aciliyet ilkesidir. Siber saldırılarda da geleneksel saldırılar gibi meşru müdafaa hakkının kullanılabilmesi için zaman önemli olabilmektedir. Bu konu detaylıca başka bir başlık altında örnekler ile beraber incelenecektir. (Akande ve Liefänder, 2013, s.563-568).

2.3.1. Aciliyet ilkesi

Herhangi bir silahlı saldırıda devletin meşru müdafaa hakkını kullanabilmesi için aciliyet ilkesini gerçekleştirmesi gereklidir. Aciliyet kavramında kastedilen durum silahlı saldırının yapıldığı zamanda meşru müdafaa hakkının kullanılması gerekliliğidir. Devletlerin karar alma süreçleri bireylerden farklı olduğu için bireylere göre devletler daha yavaş karar almaktadır. Eğer saldırı yapan devlet, saldırıya maruz kalan devlet ile sorunlarını çözme yoluna başvurmuşsa, bu süreç olumsuz olsa bile devletin meşru müdafaa hakkı korunmaktadır. Aciliyet ilkesini açıklayabilmek için en önemli örnek Arjantin'in Falkland Adalarını işgal etmesidir. İngiltere yapılan işgale geç cevap vermiştir. İngiltere'nin bu işgale geç cevap vermesinin sebebi Falkland Adasının İngiltere'ye uzak olması olmuştur. Bu gibi durumlar aciliyet ilkesi için sorun teşkil etmemektedir (Aral, 1999, s.28).

2.3.2. Orantılılık ilkesi

Meşru müdafaa hakkının kullanılmasında gerekli olan diğer ilkelere göre biri orantılılıktır. Bir saldırı durumunda saldırıya maruz kalan devlet meşru müdafaa hakkını kullanırken orantılılık ilkesini göz önünde bulundurmalıdır. Orantılılık ilkesi dehşet dengesi denen durumun ortaya çıkmasını engellemede önemli bir rol oynamaktadır. Dehşet dengesi ile bahsettiğimiz durum bir devletin diğer bir devlete saldırmasında orantılılık ilkesine uymamasıdır. Örneğin: İkinci Dünya Savaşı'nda Japonya'nın Pearl

Harbor Saldırısı'nı gerçekleştirmesi ve buna karşılık Amerika'nın İkinci Dünya Savaşı'nda Japonya'da Hiroşima ve Nagazaki'ye nükleer silah atması dehşet dengesinin aşıldığı duruma en iyi örnektir. Burada orantılılık ilkesi aşılmış durumdadır (Aral, 1999, s.29).

2.3.3. Gereklilik ilkesi

Gereklilik ilkesi taraflar arasında barışçıl yöntemler çalışmadığı zaman artık saldırının gerekli olduğu manası anlamına gelmektedir. Bu kavram eski zamanlardan gelen haklı savaş kavramına benzemektedir. Haklı savaş kavramında da barışçı yolların tamamıyla sona ermesi ve başka bir yol kalmaması savaşın haklı olduğunu ortaya çıkarmaktadır. Haklı savaş, hem savaş öncesi (jus ad bellum) hem de savaş anında (jus in bello) savaşın haklı olduğunu göstermektedir. Eski zamanlardaki bu kavram sayesinde savaşı meşrulaştırmak kolay olmuştur. Yasal bir kural olmadığı için haklı savaş kavramı sözlü yollarla kanıksanmıştır. Yani günümüzde bu kurallar yapılageliş kuralı olarak adlandırılan teamül hukukuna benzetebilir. Fakat artık haklı savaş kavramı sınırları belli olacak bir şekilde daraltılmış ve belirli kurallara uyma zorunluluğu getirilmiştir (Gardam, 2004, s.4-6).

2.4. Meşru Müdafaa Hakkının Kullanımına İlişkin Örnekler

Kuvvet kullanımı hem iç hukuk hem de uluslararası hukuku kapsayan genel bir kavramdır. İç hukukta bahsedilen kuvvet kullanımı devletin bireylere uyguladığı kuvvet kullanımıdır. Uluslararası hukuktaki kuvvet kullanımı ise devletlerin birbirine karşı uyguladığı kuvvet kullanımıdır. Uluslararası hukuktaki kuvvet kullanımı durumlarına birkaç örnek verilebilir; Falkland Adası harekâtı, Arap-İsrail Savaşları, Amerika'nın Irak'ı İşgali, Rusya'nın Ukrayna'yı İşgali, Rusya'nın Gürcistan'ı İşgali (Pazarcı, 2016, s.517-520).

2.4.1. Falkland adası harekâtı

Falkland Adası, 5 Nisan 1764'e kadar sahipsiz mülk (res nullius veya terra nullius) olarak tanımlanan bir adaydı. Ada ilk olarak Fransız toprağı olarak anılmış ve

İspanya ise adaya olan yakınlığı üzerine adada hak iddia etmiştir. Daha sonra Arjantin adayı sahiplenmiş ve İngilizler'in de adayı toprağı sayması üzerine iki devlet arasında savaşa varan çatışmalar gerçekleşmiştir. Adanın çevresinin yer altı kaynakları bakımından zengin olması adanın devletler arasında paylaşılmasına sebep olmuştur (Calvert, 1983, s.405-413). 1982 yılına kadar adaya hakim olan İngiltere'ye karşı Arjantin bir deniz savaşı başlatmıştır. Arjantin bu deniz savaşını 1800'lü yıllarda adaya hakim olanın o olduğunu iddia ederek gerçekleştirmiştir. İngiltere savaş için adada yeterli donanımına sahip olmadığı için 8000 mil öteden ek kuvvet getirmiştir ve bu sevkیات büyük bir başarı olarak tarihe geçmiştir. Arjantin'in konumu itibariyle Falkland adalarına yakın olması savaşı kazanması için yeterli olmamıştır. İngiltere'nin sahip olduğu güç ve donanma savaşın 8000 mil öteden kazanılmasını sağlamıştır (Freedman, 1982, s.196-210).

Bugünkü uluslararası hukuk sisteminde de sahipsiz mülk olan bir bölgeye, İngiltere'nin Falkland adasına yaptığı gibi sahiplenmek günümüzde dahi kabul edilen bir durumdur. Res nullius veya terra nullius kapsamında sahipsiz mülkü ilk sahiplenilen devlet o yerde hak sahibidir. Mülkiyet ile ilgili kuralların temelinde Roma hukuku ve İngilizlerin yapılageliş kuralları yer almaktadır. İngiltere'nin terra nullius kavramını meşrulaştırması ve yaptığı işgallere hukuk boyutunu katması birçok yeri kontrol altına almasına sebep olmuştur. İngiltere'nin Avustralya'yı işgal etmesi ve oradaki Aborjinler'e soykırım uygulaması bu sayede olmuştur. Terra nullius kavramı sayesinde dünyada çoğu bölge devlet yönetimine geçmiş fakat geçmeyen tek bir bölge kalmıştır ve bu bölge ise kutup bölgeleridir (Fitzmaurice, 2007, s.1-15). Kutup bölgelerinin kime ait olduğu durumu yıllardır tartışıl原因 bir konudur. Kuzey Kutup Bölgesi'nde yer alan petrol ve doğalgaz kaynakları bu bölgeyi devletler açısından cazibe merkezi yapmaktadır. Bu sebepten dolayı bölgeye yakın olan devletler burada hak iddia etmeye çalışmaktadırlar (BBC, 30.04.2022).

2.4.2. Arap-İsrail savaşları

Birinci Dünya Savaşı sonrasında Osmanlı ordusunun yenilmesiyle beraber, Osmanlı'ya ait olan Filistin toprakları İngiliz egemenliğine girmiştir. 1917 yılından beri İngiltere Filistin topraklarındaydı fakat İkinci Dünya Savaşı sonrası İngiliz imparatorluğuna ait toprakların denetlenmesi zorlaştığında İngiltere Filistin için karar

vermek durumunda kaldı. İngiltere Filistin'in durumu karşısında BM'ye başvurmuştur. Filistin sorunu karşısında BM, ABD baskısıyla bir karar aldı ve Filistin'e ait bölgelerin %55'inden daha fazlası Yahudilere verildi. 14 Mayıs 1948 yılında İngiltere bölgeden çıkmış ve Filistin halkını Yahudilerle çatışma içinde bırakmıştır.

Yahudilerin İsrail'e göç etmesinin arkasında İsrail'in ilk başbakanı olan David Ben-Gurion bulunmaktadır. Gurion ailesindeki kişilerin bahsettiği Filistin topraklarından çok etkilenmiş ve kendini oraya odaklamıştır. Amacı Filistin'e yerleşmek olan Gurion, bir kulüp kurarak 1906 yılında kulüp üyeleriyle beraber Filistin'e yerleşmiştir. Gurion gemiyle getirdiği kulüp üyelerine bir bildiri sunarak İncil'in tarihinden başlayan bir bildiri okumuştur. Ardından Filistin'e Yahudi göçünün sağlanması için çağrıda bulunmuştur. Hükümet ve anayasanın oluşturulabilmesinin birkaç ay süreceğini belirtmiştir. Yahudilerin Nazilerden gördüğü işkencelerden sonra yeni bir yurda yerleşmeleri ve kendilerine ait bir yere sahip olmaları onlar için umut verici bir durum olmuştur (Wagner, 2002, s.1-13).

Yeni bir yere sahip olduktan sonra orada bağımsızlık elde edip İsrail devleti kurabilmeleri 1948 yılına kadar sürdü. Devletin kurulma kararı BM tarafından oylama neticesinde alındı. 1948 yılından sonra İsrail, Filistin ve Arap devletleri birbirleriyle savaş içine girmiştir. Mısır, Suriye, Ürdün, Lübnan ve Irak, İsrail ile savaş haline girmiş ve böylece Arap İsrail savaşlarının ilki meydana gelmiştir. İsrail'in destekçileri arasında Amerika ve Rusya yer almaktadır. Savaştan dolayı Filistin'den göç eden Filistinli sayısı 750.000'i bulmaktaydı. Yapılan bu göçlerden dolayı İsrail'in yeri daha da genişlemeye başlamıştır. Bu savaşın diğer bir sonucu Arap ülkelerindeki Yahudilerin Filistin'e göç etmesi olmuştur.

1967 yılında yeni bir Arap-İsrail savaşı gerçekleşmiş ve bu savaşa "Altı Gün Savaşı" adı verilmiştir. Yapılan bu savaşta da İsrail'in kazanmasıyla beraber İsrail topraklarına yeni topraklar katmıştır. İsrail hızlı genişlemesi nedeniyle BM İsrail'e 1967 öncesi topraklarına dönmesi kararını almıştır. İsrail'e karşı Araplar, Arap Birliği ve Filistin Kurtuluş Örgütünü kurmuştur. Bu örgüt ve birliğin amacı Filistinlilere destek olmak ve İsrail'in işgallerinin önüne geçebilmektir. Fakat bu örgüt ve birliklere üye olan Mısır ve Lübnan'ın İsrail ile ılımlı ilişkilere geçmesi nedeniyle Araplar arasındaki birlik sekteye uğratılmıştır (Kaştan, 2007, s.1797-1817).

2.4.3. Amerika'nın Irak'ı işgali

Amerika, çoğu zaman kendini Ortadoğu'nun kurtarıcısı rolünü üstlenen bir devlet olarak görmüştür ve bu konuda hem Ortadoğu'daki devletlerle hem de diğer devletlerle anlaşmazlıklar yaşamıştır. Amerika'nın Ortadoğu'da bulunmasının görünen sebebi olarak her zaman Ortadoğu'da demokrasi yayma çabası olduğu gösterilmektedir fakat arka planda yatan nedenlere bakıldığında birçok sebebinin olduğunu veya Ortadoğu'da bulunmak üzere olmayan sebeplere sığındığı söylenilebilir. Amerika'nın Irak'ı işgali ise bu sebeple ortaya çıkmış bir durumdur. Amerika'nın Irak'ı işgal etmesinin temelinde 11 Eylül Saldırıları'ndan dolayı Amerika'nın güvenlik stratejilerini değiştirmesi ve müslümanlara karşı düşman kimliği oluşturması önem kazanmıştır.

Bush'un başkanlığa gelişinin ilk yılında 11 Eylül saldırıları gerçekleşmiştir. El Kaide'nin gerçekleştirdiği bu saldırı Amerika gibi büyük bir gücü ve halkını derinden sarsmıştır. Amerika'nın bu noktaya gelişinin temelinde 1998 yılında Amerikan büyükelçiliğinin Kenya ve Tanzanya'da El Kaide tarafından bombalanması yatmaktadır. Bill Clinton, Usame Bin Ladin'i sınır dışı etmesi için Taliban ile uzlaşmaya çalıştı. Usame Bin ladin'i yakalamak ve öldürmek için tutulan ajanlar bu ölçüde yetersiz kaldı ve Usame Bin Ladin'i durdurmadı. Uçak Operasyonu adında 11 Eylül'ün kaçınılmaz bir şekilde gerçekleşmesine neden oldu (The National Commission on Terrorist Attacks Upon The United States, s.108-113).

Birbiri ile bağlantısı olan 4 uçak kaçırıldı ve bunlardan ikisi İkiz Kuleler'e çarptı. Diğer uçaklardan biri Pentagon'a çarptı ve ardından sonuncu uçak ise yolcuların müdahalesi üzerine boş bir alana düştü. Eğer uçağa yolcular müdahale etmeseydi sonuncu uçağın Kongre binasını hedeflediği düşünülüyordu. Bu teröristlerin uçaklara ellerinde silahlarla kolayca binebilmeleri havalimanı güvenliklerinin yetersiz olduğunu düşündürmektedir. Amerika'nın CIA gibi üst düzey bir merkezi istihbarat teşkilatına sahip olması 11 Eylül'ün gerçekleşmesini engelleyemedi veya Amerika bunu engellemek istemedi. Bunun üzerine günümüzde birçok komplo teorisi bulunmaktadır. Amerika'nın bu saldırıya müdahale etmeme sebebi, El Kaide Amerika'ya saldırdığında Amerika meşru müdafaa hakkını öne sürüp geri El Kaide'ye saldırmayı planlanması

olabilir. Hatta komplo teorisi olarak söylenen cümlelerden biri budur (BBC, 06.09.2021).

Amerika'nın Irak'ı işgal etme sebebinin sadece terörizm odaklı olmadığı Irak'taki yeraltı kaynaklarından beslenme isteği olabilir. Çünkü Amerika kendi bölgesindeki yeraltı kaynaklarının yetersizliğinden şikâyet etmiş ve yeni arayışlar içine girmiştir. O dönemdeki en büyük petrol üreticisi olan iki devlet Suudi Arabistan ve Irak'tı. Fakat Suudi Arabistan'da petrol çıkarma maliyetinin artması, Amerika'nın yönünü Irak'a çevirmesine sebep olmuştur (Hinnebusch, 2007, s.9-27).

Bush ve Dışişleri Bakanı Colin Powel Irak'ta nükleer silahların olduğunu iddia etmiştir. Tony Blair ise bu iddiayı kanıtlayacak nitelikte elinde belgeler olduğunu öne sürmüş ve kamuoyu bu iddiaların doğruluğuna inanmıştır (Independent, 20.03.2021). Fakat Bush'un asıl amacı Saddam Hüseyin'i ortadan kaldırmak ve Irak'ın sahip olduğu zenginlikleri elde edebilmektir. Amerika 19 Mart 2003'te Irak'a girme operasyonunu başlattı. İşgal sonucunda kitle imha silahlarının bulunmadığı ortaya çıktı. Ancak Amerika Irak'ın yeniden yapılanması sürecine başlamıştı.

Colin Powell Irak'ta nükleer silahların olduğuna dair açıklamalarda bulunmasına rağmen BM Silah Denetleme Komisyonu Irak'ta nükleer silah üretildiğine dair herhangi bir kanıt bulamamıştır. Bush ve Powell BM'yi Irak'ın nükleer silahlara sahip olduğuna ikna edemeyince, BMGK'dan herhangi bir onay almadan Irak'a karşı savaş ilanı kararı almıştır. BMGK kararı alınmadan yapılan bu savaş ilanı ABD'nin uluslararası hukuk kurallarını çiğnemesine sebep olmuştur (Anadolu Ajansı, 20.03.2022).

Amerika'nın meşru müdafaa hakkına dayanarak kuvvet kullanması ve bir devletin iç işlerine karışması uluslararası hukuka aykırı bir durumdur. Tek kutuplu bir uluslararası düzende Amerikan hegemonyasını göz önünde bulundurduğumuzda Amerika'nın herhangi bir yaptırımla karşılaşmaması normaldir. Çünkü hegemon devlet her zaman diğer devletleri bastırır (Miller, 2003, s.8-28).

2.4.4. Rusya'nın Ukrayna'yı işgali

Vladimir Putin, modern, Batı eğilimli Ukrayna'nın sürekli bir tehdit olduğu ve bu yüzden de Rusya'nın kendini güvende hissedemeyeceği gerekçesi ile İkinci Dünya

Savaşı'ndan bu yana Avrupa'daki en büyük savaşı başlattı. İşgalin başlamasından önce Putin, işgal sebebinin Ukrayna'yı asker ve nazilerden temizlemek olduğunu söyledi. Daha sonra NATO'nun Ukrayna'yı üyesi haline getirmek istediğini, Rusya'ya kadar ilerleyeceğini ve Ukrayna'nın hiçbir uluslararası örgüte bağlı olmadan tarafsız bir durumda kalması gerektiğini belirtti. Rusya bu sebeplere bağlı olarak Rusya'nın sınırında bulunan Donetsk ve Luhansk bölgesine girerek işgallerine başladı ve daha sonra Mariupol'e girdi. Rusya Kiev'e yakın bölgeleri ele geçirdikten sonra Ukrayna güçleri bu bölgeleri geri Ruslar'ın elinden aldı. Savaş başlayalı üç sene oldu ve halen devam etmektedir. Savaşın geleceği ve Ukrayna'nın durumu tartışılmaktadır (BBC, 24.02.2023).

Rusya'nın Ukrayna'ya karşı yaptığı saldırı, savaş suçu kategorisine girmektedir ve bu suçun cezalandırılmasında Uluslararası Ceza Mahkemesi önemli bir rol oynamaktadır. Rusya'nın savaş sürecinde işlediği suçlardan dolayı Uluslararası Ceza Mahkemesi'nden bir savcı soruşturma başlatmıştır. Ukrayna ve Rusya UCM'ye taraf olmamasına rağmen taraflardan birinin yani Ukrayna'nın soruşturma istemesi hasebiyle soruşturma başlatıldı (BBC, 03.03.2022). Ukrayna'nın soruşturma istemesi 2014 yılına dayanmaktadır. Soruşturmanın sebebinin Donbas bölgesindeki liderlerin Ukrayna vatandaşlarına soykırım yapması sonucu gerçekleştiği belirtilmiştir. 2020 yılında UCM tarafından yayınlanan rapora göre ise böyle bir suçun bulunduğu ve savaş suçunun işlendiği tespit edilmiştir. UCM tarafından görevlendirilen bir savcı olan Karim Khan, Ukrayna'da işlenen savaş ortamının UCM'ye taşınıp soruşturmanın hızla ilerlemesi için devletlerin bu konuyu öne çıkarmaları gerektiğini söylemiştir. Savcının çağrısının ardından 41 devlet bu konuyu öne çıkardıklarını tebliğ etmişlerdir.

Rusya'nın Ukrayna'yı işgalini Amerika'nın Irak'ı işgaline benzetebiliriz. İki devletin savunduğu argümanlar ile devletlerin iç işlerine karışma hakkı elde etmeleri ve uluslararası hukuka aykırı bir suç işlemelerine rağmen herhangi bir yaptırımla karşılaşmamaları oldukça benzerdir. Fakat iki saldırının uluslararası alanda nasıl bir tepkiyle karşılandığına dair farklılıklar mevcuttur. Amerika'nın Irak'ı işgalinde Bush için saldırı suçu işlediğine dair devletler ortak bir görüş içine girseler de BM'ye suçlamaya dair herhangi bir başvuruda bulunulmamıştır. Rusya için durum değişkenlik göstermektedir. Amerikanın devletler üzerinde tek lider konumunda görülmesi ve hegemon alanının genişliği nedeniyle, bu hegemonyayı kabul eden devletler

Amerika'nın arkalarında olduğunu bildikleri için Rusya'ya karşı çeşitli yaptırımlar uygulamıştır. Amerika'nın Irak'ı işgalinde Irak'ta askerlerin işlediği suçlar için UCM herhangi bir yaptırımda bulunmamışken, Rusya'nın Ukrayna'da işlediği savaş suçları için UCM, Putin'in tutuklanmasını talep etmiştir. Amerika'nın ve Rusya'nın işlediği suçlarda farklı tepkilerle karşılaşmalarının en büyük sebebi Amerika'nın liderliğinin dünya üzerinde hala kabul edilebilir olmasıdır (The Guardian, 20.03.2023).

İki tarafın isteklerini gerçekleştirebilmek için karşı tarafta düşman kimliği oluşturarak yaptığı saldırılar, iki devletin kendi mantık çerçevelerinde bir saldırı sebebi olarak kabul etmelerine sebep olmuştur. Bush'un Saddam Hüseyin'i ve Putin'in Zelenskiyi devrilmesi gereken lider olarak görmesi, dış politikalarını bu sebeplere dayanarak inşa etmelerini gerektirmiştir. Yapılan bu saldırılar neticesinde Amerika ve Rusya'nın gerçekleştirdiği işgallerde BM Şartı'na bağlı kalmaması, uluslararası hukukun gerekliliklerinin ihlal edilmesi devletlerarası bir düzenin tam olarak gerçekleştirilemediğinin bir göstergesidir (Al Jazeera, 01.04.2023).

Rusya Ukrayna savaşında sadece geleneksel savaş teknikleri değil ayrıca siber savaş teknikleri de kullanılmıştır. Artık geleneksel savaşın yetmediği durumlarda siber savaşlarında kullanılması devletlerin yeni çağa uyum sağlamaya çalıştığının göstergesi olmuştur. Siber savaşları en çok kullanan ülkeler başta Rusya olmak üzere İsrail, İran ve Ukraynadır. Rusya'nın Ukrayna'ya siber saldırılar düzenlemesi 2014 yılında başlamıştır. Fakat yapılan bu saldırılar Ukrayna'nın siber altyapısının güçlenmesinde etkili bir rol oynamıştır. Ukrayna siber altyapısının güçlendirmesini yaparken müttefik olduğu devletler ve Google, Amazon ve Microsoft gibi özel şirketlerden de yardım almıştır. 23 Şubat 2022 yılında Rusya Ukrayna işgaline başlamadan önce Microsoft, Ukrayna'ya karşı siber saldırıların başladığını gözlemlemiştir. Temmuz 2022 sonrası Rusya Ukrayna'nın enerji şirketi olan DTEK'e siber saldırı düzenlemiş ve Ukrayna'nın enerji altyapısının kesmeye odaklanmıştır (European Parliament, 2023, s.1-11).

2.4.5. Rusya'nın Gürcistan'ı işgali

Rusya, Gürcistan'ı 2008 yılının Temmuz ayında Güney Osetya'daki karışıklılığa bağlı olarak işgal etti. Batı'nın Kosova'nın bağımsızlığını tanınması ve NATO Bükreş Zirvesi'nde Kafkasya'nın durumunun konuşulması Rusya'nın bu saldırıyı

başlatmasında önemli rol oynamıştır. Gürcistan'ın Avrupa'ya doğru ilerleme göstermesi ve NATO'nun da Kafkasya odaklı çalışmaları Rusya için Gürcistan'a saldırı sebebi olmuştur. Geniş bir perspektiften bakıldığında savaşın temelini Sovyetlerin dağılmasına dayandığı söylenilebilir. Savaşa "Güney-Osetya savaşı veya Beş Gün Savaşı" ismi verilmiştir. Savaşın 7 Ağustos 2008 ile 12 Ağustos 2008 olarak beş gün sürmesi bu isimle adlandırılmasına sebep olmuştur.

1999 yılında Rusya'ya lider olarak Putin'in seçilmesinden itibaren, Putin Sovyetlerin arka bahçesi olarak gördüğü devletlere odaklanmaya başladı. 2003 yılında Gül Devrimi'nin gerçekleşmesiyle beraber Mikheil Saakasvili'nin iktidara gelmesi Putin'in odak noktasını Gürcistan'a yöneltmesine sebep olmuştur. Gül devriminde iktidardan düşen Şevardnadze döneminde Gürcistan'ın durumu çok etkisizdi ve aktif değildi. Fakat Gül Devrimi sonrası gelen Saakasvili döneminde Gürcistan aktif bir politika izlemiş ve Rusya'nın Gürcistan'daki etkisini reddetmiştir. Avrupa ise Gürcistan'daki enerji kaynaklarına olan ihtiyaçtan dolayı Gürcistan'a yönelik isteklerine odaklanmıştır. Rusya hem Avrupa'yı hem de Amerika'nın Gürcistan'ı etkilemesini önlemek üzere otoritesini kanıtlamak için işgali gerçekleştirmiştir (Cornell ve Starr, 2009 s.1-7).

Güney Osetya, Rusya'ya sınır komşusu olup nüfus yoğunluğu açısından en fazla etnik grup olan Osetlilerden oluşmaktadır. Osetya Gürcistan'ın zayıf yönetiminden dolayı yıllarca Gürcistan'dan bağımsız hareket etmiştir. Gürcistan sadece Osetya bölgesinde azınlık statüsünde olan Gürcüler'i yönetti. Osetya'daki Gürcüler ise vergilerini ödediler ve Gürcistan seçimlerinde oylarını kullandılar. Bu ayrılıkçı hareketler 2008 yılında savaşın temellerinin atılmasında rol oynadı. Ağustos ayında yapılan savaşta Güney Osetya'daki ve Abhazya'daki Gürcüler'in Ruslar tarafından evleri yıkıldı ve ardından sınırdışı edildiler. Gürcüler yapılan bu sınırdışı edilme uygulamalarını soykırım olarak tanımladı. Osetyalılar ise kendilerini Gürcistan devletine ait hissetmediler (George, 2009, s.1-7).

Savaş Fransa'nın cumhurbaşkanı Sarkozy'nin çıkardığı Sarkozy Planı ile Rusya'nın Osetya'dan çekilmesiyle sona erdi. Rusya'nın Sovyetler Birliği'nin dağılmasından sonraki amacı, arka bahçesinde olan ülkelerde "böl ve yönet" politikası uygulayarak ülkelere müdahale edebilmektir. Fakat hem ABD hem de Avrupa Birliği

bu bölgeye müdahale edilmesine izin vermemektedir. Bu açıdan Sarkozy Planı Gürcistan ve Rusya arasında barışın korunması açısından önemli bir atılım olmuştur (Öztürk, 2009, s.1-12).

Rusya Gürcistan savaşında, Rusya'nın Gürcistan'a savaş boyunca yaptığı siber operasyonlar da vardır. İki devlette birbirine ağ operasyonları düzenledi. Estonya saldırılarında olduğu gibi Rusya, Gürcistan'da da DDos (hizmet engelleme saldırıları) gerçekleştirdi. Gürcistan'ın ulusal bankasına 9 Ağustos ve 18 Ağustos arası saldırılar gerçekleştirildi. Gürcistan'ın dışişleri bakanlığına yapılan saldırıda ise Saakasvili ile Adolf Hitler'in beraber resmi konuldu. Resmin yanında Güney Osetyalı bir grubun bu saldırıları gerçekleştirdiğine dair bir mesaj yerleştirildi. Bu resmin konulma amacı, saldırıları Rusya'nın yapmadığı ve bir iç mesele olduğuna inandırmaktı. Rusya yapılan saldırıları gerçekleştirdiğine dair sorumluluğu üstlenmedi (Deibert, Rohozinski ve Nishitata, 2012, s.7-10)

ÜÇÜNCÜ BÖLÜM

SİBER SALDIRI TÜRLERİ VE SİBER SALDIRILARDA MEŞRU MÜDAFAA VE KUVVET KULLANIMI

3.1. Siber Savaş Kavramının İncelenmesi

Soğuk savaştan bu zamana savaş kavramının içeriği ve kuvvet kullanımı değişkenlik göstermiştir. Siber savaşlar günümüzde yaygın olarak kullanılan bir savaş türü haline gelmiştir. Geleneksel savaşlara göre siber savaşların tercih edilmesi ve siber saldırı yapmak için gerekli olan bilgiye ve aletlere erişimin kolay olması siber savaş tercih edilebilir kılmaktadır (Heintze and Thielbörger, 2016, s.21). Bu savaşın sorumluları bilgisayar haydutları, siber alan suçluları ve internet eylemcileri olsa da bu savaşın arkasında devletler de bulunmaktadır (Powers and Jablonski, 2015, s.1-3).

Siber kavramı, tarihte ilk olarak Antik Yunan'da karşımıza çıkmaktadır. Fakat bu terimi genişçe kullanan biri olan Norman Wiener, 1948 yılında “Sibernetik” adlı kitabı yazmış ve canlılar ile makineler arasında nasıl bir bağlantı olabileceğini araştırmıştır (Richards, 2014, s.4-5). Tarihte bilgisayara bulaşan ilk virüs 1986 yılında “Brain A” adında bir virüstür. Bu virüsü yaratan iki kardeş, virüse kendi adlarını ve onlara nasıl ulaşabilecekleri bilgilerini işlemişlerdir. Kardeşler bu virüsü oluşturma konusunda herhangi bir kötü amaçlarının olmadığını savunmaktadır fakat bu virüs bulaştığı bilgisayar sahiplerine bilgisayarlarında herhangi bir işlem yapma şansı vermemektedir (Rosenzweig, 2013, s.17-18).

Siber saldırılar, bilgisayarlar ortaya çıktığı zamandan beri yavaş yavaş ortaya çıkıp kendini gösterme eğilimindedir. Fakat saldırıların en yoğunlaştığı zaman 11 Eylül sonrası zamanlardır. Artık geleneksel savaşlardan ziyade korku ortamı yaratmak amacıyla siber alan oldukça sık kullanılan ortamlardandır. Küreselleşmenin giderek artmasının güzel yönleri olması her zaman iyi sonuçlara yol açtığı anlamına gelmemektedir. Küreselleşme ile gelen birbirine bağımlılık kavramı, devletlerin zayıf

yönlerinin kolayca yakalanmasını sağlayabilmektedir. 2015 yılında Amerika da yapılan Pew Survey anketine göre siber saldırılardan korkanlar birinci sırada gelmekte olup, ikinci sırada ise islamcıların yaptığı saldırılar bulunmaktadır. Bu anketten yapabileceğimiz yorum artık Amerika’lılarda islamcılara karşı daha az korkunun olduğu ve 11 Eylül’ün travmatik etkisinin yavaşça atlatılmaya çalışıldığı fakat bunun yerine siber saldırıların artık daha çok korku zemini yarattığıdır. ABD başkanı Obama da siber güvenlik tehditlerinin çok önemli bir konu olduğunu belirtmiştir. Obama dönemi savunma bakanı olan Leon Panetta diğer bir Pearl Harbor’ın siber alanda gerçekleşeceğini söylemiştir. Rusya ise siber güvenliğin sağlanması için siber birlikler kurulmasını sağlamıştır. İki devletinde yaptıkları adımlar ve aldıkları aksiyonlar siber saldırıların güvenlikleştirilmesi konusunu öne çıkarmıştır. Güvenikleştirme yapılırken öncelikle saldırılar gündeme alınır ve halk üzerinde bir korku yaratılır. Ardından bu saldırılar güvenlikleştirilerek önlemler alınması sağlanır (Valeriano and Maness, 2015, s.2-3).

Devletler siber savaşların artması ve etki alanının geniş olması nedeniyle harekete geçme zorunluluğu hissetmiştir. Amerika Obama döneminde görevi siber operasyon gerçekleştirmek olan Birleşik Devletler Siber Komutanlığı (Cybercom) kurmuştur. Birleşik Krallık ise siber güvenlik alanında eksikliklerinin olduğunu fark ederek Siber Güvenlik Programı’nı yayınladı. NATO da siber savaşa uygulanacak olan hukuk üzerine “Tallinn Manual El Kitabı” yayınladı. Tallinn El Kitabı siber güvenlik üzerine yazılmış ve siber alan ile ilgili oldukça detaylı bir çalışmadır. Uluslararası hukuktaki kuralların siber alana uygulanması için 95 kuraldan bahsedilmektedir. Tallinn Manual’in kuralları yaratılırken ABD, Kanada, Birleşik Krallık ve Almanya’nın savaş kurallarından yararlanılması, el kitabının yanlı olmasının iddia edilmesine yol açmıştır (Robinson, Jones and Janicke, 2015, s.71-90).

3.2. Siber Saldırı Türleri

Siber saldırılar, sistemlere girerek bilgilerin çalınması ve verilerin değiştirilmesi gibi eylemler ile uygulamaya geçen saldırılardır. Bu saldırılar ile illegal yollarla bilgisayarlara izinsiz erişim sağlanmaktadır. Genellikle saldırılarda maddi kazanç elde etmek ve gizli bilgilere erişim sağlamak en önemli amaçlardandır. Saldırıların yapılması

için farklı türler bulunmaktadır ve her saldırı türünde kullanılan yollar farklıdır. En çok kullanılan siber saldırı türleri yedi ana başlıkta incelenecektir (http-1).

3.2.1. Hizmet engelleme saldırıları (DDos saldırıları)

Hizmet engelleme saldırıları adından anlaşılacağı üzere kullanıcılara erişim problemi yaratmak üzerine kuruludur. Bu saldırılar göz ardı edilemeyecek kadar önemli saldırılar arasında yer almaktadır. Bu tür saldırıları yapanlar genelde parasal destek ile ödüllendirilmektedir. Hizmet engelleme saldırılarının ortaya çıkış tarihi 2003 yılında olmuş ve o zamandan beri saldırılar artarak devam etmiştir. DDos saldırıları bir site üzerine birden fazla talep gönderip kapasiteyi aştığı zaman ise sitenin kullanılamamasını sağlar (Ansari, 2011, s.279-305).

3.2.2. Kimlik avı (Phishing)

Kimlik avı ile yapılan dolandırıcılıklarda kullanılan yöntem kurumsal bir şirketin e-posta logosunu, fontunu taklit ederek e-mail göndermek ve bu e-maili açan kişiye güvenilirlik sağlayıp bilgilerini çalmaktadır. Kişi gönderilen e-mailin güvenilir olduğuna inanıp kendi kimlik bilgilerini vererek dolandırıcılara fırsat tanımaktadır. Genelde bu mailde alıcıya hesabına izinsiz giriş olduğu, hesap için gerekli olan bilgilerin revize edilmesi gerektiği maili gelmektedir. Eğer kişi bu bilgileri düzenlemek için verilen linke tıklarsa ve bilgilerini girerse kimlik avı saldırısına maruz kalmış demektir (Lynch, 2005, s.259-263).

3.2.3.Yemleme kancası (Spear phishing)

Yemleme kancası aynı kimlik avı gibi e-posta yoluyla yapılmaktadır. Fakat burada e-mailde kişi kendi bilgilerini girmez. Kişiye e-mail içinde bir dosya eki bırakılır ve bu dosyayı bilgisayara indirmesi gerektiği belirtilir. Dahas sonra bilgisayara indirilen dosya sayesinde saldırganlar tarafından bilgisayardaki bütün bilgilere ulaşılır. İndirilen dosyanın silinmeden bilgisayarda unutulması sonucunda uzun süren bir saldırıya sebebiyet verilmektedir (Bossetta, 2018, s.97-106).

3.2.4. Ortadaki adam (Man in the middle attack)

Ortadaki adam saldırıları birbiriyle ilişkisi olan iki tarafın arasında iletişim bozulması veya değiştirilmesiyle ortaya çıkmaktadır. Örneğin, saldırganlar iki taraf arasındaki iletişimi bozmak için kötü amaçlı ve doğruluğu olmayan bilgiler yayar (Nitiynandan and Kamalakkannan, 2022, s.1-3).

3.2.5. Fidyeye yazılımı (Ransomware)

Fidyeye yazılımında suçlular bilgisayarlara erişir ve bilgisayardaki dosyaları şifreler. Bilgisayar sahibi bu dosyalara giremez ve bu dosyaları şifreleyen suçlular bilgisayar sahiplerinden fidye yani belirli bir ücret isterler. Fidyeye yazılımı işi çok tutulan bir iştir ve sadece Amerika’da 2019-2021 yılları arasında yani iki yılda bile %200 artış göstermiştir. Fidyeye yazılımı saldırılarının artış göstermesinin sebebi kripto paraların son yıllarda sıkça kullanılması olmuştur. 300 şirketin katıldığı bir ankete göre %64’ü bu saldırıya uğramış fakat %83’ü saldırganlar tarafından istenen fidyeyi ödemek zorunda kalmıştır. Bu ödeme boyunca karşılaşılabilecek en kötü durum ödeme yapılmasına rağmen şifreyi çözmek için gerekli olan anahtarın bilgisayar sahibine verilmemesidir. Bu durumda saldırganlar ikinci bir fidye hatta üçüncü bir fidye isteyebilmektedir. Bu saldırılara karşı yapılması gereken çözüm dosyaların her zaman bir yedeğini oluşturmak ve bunları başka bir yerde saklamaktır. Çünkü saldırganlar yedeklere de ulaşabilmekte onları da şifreleyebilmektedir (Leo, Işık and Muhly, 2022, s.1-4).

3.2.6. Kripto hırsızlığı (Cryptojacking)

Kripto hırsızlığında başka birinin bilgisayarı kripto hırsızlığı için kullanılır. Bu bilgisayara e-mail aracılığıyla gönderilen dosyanın indirilmesi ile yüklenir ve bu dosya arka planda çalışmaya başlar. Bilgisayarın işleyişini bozmaz ve bilgisayar sahibi tarafından anlaşılmaz. Burada amaç kişilerin bilgisayarına girerek kripto paraların elde edilmesini sağlamaktır. Kripto paraların çok kullanıldığı ve değerlerinin gerçek paralara

göre artış gösterdiği bu dönemde kripto hırsızlığı önem kazanmıştır (Hürriyet, 30.05.2018).

3.2.7. Kötü amaçlı yazılım (Malware)

Kötü amaçlı yazılım, bir sisteme kullanıcı rızası olmadan uzaktan giriş sağlanıp sistemi çökertmek gayesiyle yerleştirilen yazılım parçalarına verilen kapsamlı isimdir. Kötü amaçlı yazılımlar “aile” ve “varyant” olmak üzere ikiye ayrılmaktadır. Aile teriminin tanımı, diğer yazılımlardan farkını gösteren özgün yazılım parçalarına denmektedir. Varyant ise bu yazılım parçalarının başkalaşmış sürümlerini ifade eder. Kötü amaçlı yazılım parçaları virüsler, solucanlar, truva atı, mantık bombası, arka kapı, rootkit olarak geçmektedir (OECD, 2009. s.21-23).

3.2.7.1. Virüs

Virüsler, kullanıcının bilgisi olmadan bilgisayara girerek bilgileri kopyalar ve başkalarına bu bilgileri gönderebilirler. Sisteme girdikten sonra bilgisayarın güvenliği için alınan önlemleri kapatıp sistemde rahatça yayılabilirler. Virüsler çıkış tarihinin 1980 olduğu bilinmektedir ve bu tarihten beri virüsler evrim geçirmiştir. Artık bilgisayarı virüslerden koruyan programlar tarafından farkedilmesi güç olan virüsler geliştirilmiştir (Cifci, 2013, s.152).

3.2.7.2. Solucan (Worm)

Solucanlar, diğer bir adıyla kurt saldırıları, kimseye bağlı olmadan kendiliğinden türeyen ve yayılan bir saldırı türüdür. Solucanlar bir bilgisayarın açıklarından faydalanıp o bilgisayara girerler ve bilgisayardan bilgisayara bulaşma süresi saniyeler alır. Tarihteki en eski solucan saldırısı Morris solucanıdır. Morris adında bir gencin 1988 yılında bu solucanı oluşturması o zamana göre çoğu bilgisayarda karışıklık yarattı ve ardından Morris bu karışıklığı çözmek üzere bilgisayarlara uyarı göndermek istedi fakat bilgisayarlar solucan saldırısı altında olduğu için bu uyarıyı almakta zorlandı. Morris’in kapsam alanını düşündüğümüzde bulaştığı dönemde oldukça dardı. Fakat

günümüzde bu solucan bulaşsa internetin ancak %1'ine bulaşabilir (Hoover Institution, 2011).

3.2.7.3. Truva atı (Trojan horse)

Truva atı saldırılarının ismi Antik Yunan'da Yunanlıların Truva şehrini almak isteyip alamamaları ve daha sonra şehre içi askerlerle dolu büyük bir at hediyesi gönderip içinden askerlerin çıkmasıyla beraber şehrin işgal edilmesi hikayesinden gelmektedir. Truva atının bilgisayardaki mantığı da bu şekilde çalışmaktadır. Truva atı bilgisayara iyicil bir yazılım gibi indirilir fakat daha sonra bilgisayara zarar vermeye başlar. Fakat truva atları virüslerin aksine çoğalmazlar. (Canbek and Sağıroğlu, 2007, s.125) Stuxnet saldırısının altyapısına benzer olarak geliştirilmiş Duqu saldırısı, truva atı kullanılarak gerçekleştirilmiştir. 2011 yılında ortaya çıkan Duqu saldırısı, truva atının bilgisayarlara indirilmesiyle beraber klavye dinleme ve şifre kaydetme işlemlerini gerçekleştirmiştir. Duqu saldırısı Stuxnet kadar yıkıcı bir saldırı değildir (NATO Cooperative Cyber Defence Centre of Excellence, 2020, s.6).

3.2.7.4. Mantık bombası (Logic bomb)

Mantık bombası, bilgisayar programlarına kötücül kodların işlenmesidir. Bombanın amacı bilgisayardaki bilgilerin yok edilmesini sağlamak ve tekrardan kullanılmasını önlemektir (Aslay, 2017, s.24-28).

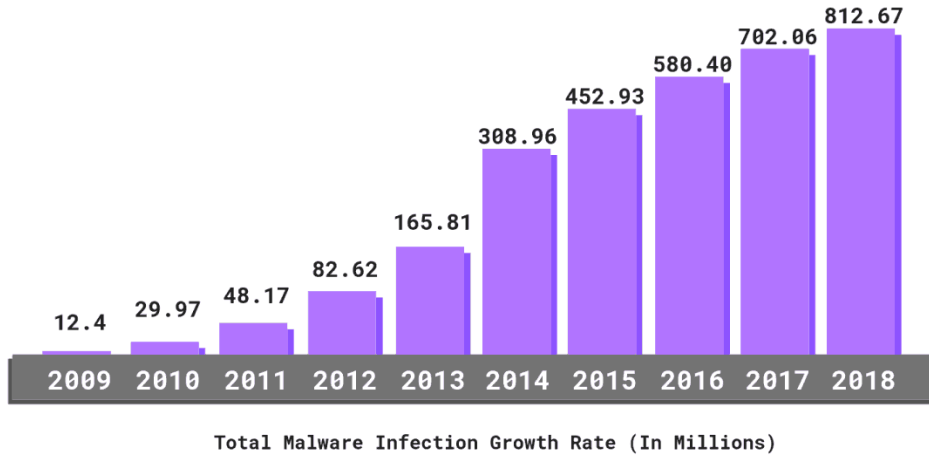
3.2.7.5. Arka kapı (Backdoor)

Arka kapı, bir sistemde olağan girme çıkma yerleri dışında veri sızmasının mümkün olduğu açık noktalara verilen bir isimdir (Kara, 2021, s.125). Bilgisayar korsanları bu saldırıları yazılım yapılırken kurulan arka kapılardan yararlanarak veya yeni bir arka kapı oluşturarak yaparlar. Örneğin, bir kasanın güvenlikler tarafından korunduğunu düşünelim ve kasanın olduğu yerdeki havalandırmayı burada güvenlik açığına benzetebiliriz (Tech Target, 2023).

3.2.7.6. Rootkit

Rootkit, bilgisayara sızan ve bilgisayardaki programlarda gizlice varlığını sürdüren kötü amaçlı yazılımlardan biridir. Rootkitler sayesinde bilgisayar korsanları ağ üzerinden yönetici konumunda kontrolü ele alabilir. Rootkitleri bilgisayardan arındırma işlemleri için çeşitli programlar kullanılmasına rağmen bazı siteler de temizlediği iddia etmektedir. Fakat bu sitelerin çoğu rootkitlerin bulaşmasında önemli bir rol oynamaktadır.

Tablo 3.1. *Kötü amaçlı yazılımların bilgisayarlara bulaş oranı (http-2)*



Yıllara göre kötü amaçlı yazılımın bilgisayara bulaşma oranı tabloda gösterilmiştir. Saldırıları, 2009 yılında oldukça az durumda iken 2018 yılına kadar artış göstermiştir. Kötü amaçlı yazılımların çoğunda kullanılan yöntemin e-posta olduğu söylenmektedir. Kötü amaçlı yazılımda en çok kullanılan truva atıdır (http-2).

3.3.Siber Saldırılarda Meşru Müdafaa ve Kuvvet Kullanımı

Birleşmiş Milletler Sözleşmesi'nin 51.maddesine göre yapılan bir silahlı saldırı karşısında, silahlı saldırıya maruz kalan devletin silahlı saldırıyı yapan devlete karşı meşru müdafaa hakkı doğmaktadır. Geleneksel savaşlarda meşru müdafaa'nın nasıl yapılacağı konusunda bir kolaylık varken, siber savaşlarda nasıl bir karşılık verileceği ve bu karşılığın kime verileceği yani atıf sorunu doğmaktadır.

Burada yer alan başka bir sorun ise “siber saldırı” ve “siber savaş” kavramlarının tanımlanması sorunudur. Yapılan saldırıların siber saldırı mı yoksa siber savaş mı olduğunun anlaşılması zordur. Siber saldırıların ölçü ve etki açısından değerlendirilmesi bu iki kavramın ayırt edilmesinde oldukça önemlidir. Tallinn Manual'ın editörü olan Profesör Schmitt, bir siber hadisenin BM Tüzüğü'ne göre bir saldırımı yoksa kuvvet kullanma olarak tanımlanıp tanımlanmayacağını belirten sekiz kıstas oluşturmuştur (McGhee, 2013, s.70-73). Kriterlerin oluşumuna katkıda bulunan Profesör Schmitt bu sekiz kriteri şöyle açıklar; 1) Şiddet (Severity) 2) Aciliyet (İmmmediacy) 3) Doğrudanlık (Directness) 4) İstilacılık (İnvasiveness) 5) Ölçülebilirlik (Measurability) 6) Askeri Karakter (Military Character) 7) Devlet Katılımı (State Involvement) 8) Varsayımsal meşruiyet (Presumptive Legality). Profesör Schmitt şiddet kriterini açıklarken bir olayın verdiği zararın büyük ve yıkıcı olup olmadığını anlamaktan bahsetmiştir. Bir olayın yıkıcı olup olmadığının kişilere veya mülklere zarar verilip verilmediğine bakılarak anlaşılabilirliğini belirtmiştir. Aciliyet kavramında ise bir siber durumun erken veya geç ortaya çıkması kastedilir. Örneğin, Stuxnet saldırısı sistemlere sızılıp aylarca bekledikten sonra ani bir vuruş ile ortaya çıkmış bir saldırdır. Erken ortaya çıkan bir siber olay, kötü etkileri için tedbir alınmasını zorlaştırır. Doğrudanlıkta anlatılan durumda ise bir olay ile bu olayın yarattığı etki arasındaki sebep sonuç ilişkisi kastedilmektedir. Diğer bir ölçüt olan istilacılık, bir düzene yayılmanın boyutunu ifade eder. Eğer saldırılarda tek bir devlet hedefleniyorsa saldırı istilacıdır. Ölçülebilirlik ise olay sonucunda verilen kaybın miktarını belirtmekte kullanılır. Varsayımsal meşruiyet ise bir yasağın bulunmadığı zamanlarda yapılan aksiyonların meşru olarak geçerli olması (propaganda, psikolojik operasyonlar, casusluk ve ekonomik baskılar uluslararası hukukta olup meşru sayılanlar) durumudur. Siber saldırılar ile ilgili kesin bir yasak olmadığı için bu saldırıların yapılması konusunda daha çok artış olabileceği

ihtimalinden bahsedilir. Başka bir kriter olan devlet katılımı ise yapılan operasyonlarda devletlerin doğrudan veya dolaylı olarak etkisinin olup olmadığı ile ilgilidir. Askeri karakter ise saldırılarda bir siber ordu gibi askeri nitelik olup olmadığını incelemek kastedilmektedir (Schmitt, 2017, s.333-337).

Bütün bu ilkeleri Amerika'da bir metroya yapılan sarin gazı saldırısı olayı üzerinden özetlemek ilkelerin anlaşılması açısından önemlidir. Bu saldırıyı yapmak için başka ülkelerden gelen saldırganların hudutu aşmış geldiğini düşünelim. Metroda yapılan saldırının aniden olması ve bir anda ortaya çıkması aciliyet ilkesini açıklar. Doğrudanlık kriterinde ise hangi olay karşısında bu sonuç oldu kısmına bakarız ve burda gaz atılmasının etki oluşturduğunu ve bu etkiyi yaratanların saldırganlar olduğunu söyleriz. İstilacılık ise saldırganların bu planı gerçekleştirebilmesi için başka devletlerden gelip hudutu aşmasıdır. Ölçülebilirlik gaz salınımı dolayısıyla yaralanan veya ölen kişilerin sayısı anlamına gelmektedir. Sadece fiziksel değil psikolojik nedenlerden dolayı yaralananlarda ölçülebilirlik kavramına dâhildir. Varsayımsal meşruiyette ise belirli bir yasağın bulunmadığı zamanlarda bir aksiyonun meşru olabileceğini belirtmektedir. Burada bahsedilen saldırganların yasak olan durumlara daha çok yönelme eğiliminin olmasıdır. Fakat burada varsayımsal meşruiyet yoktur çünkü hiçbir kişi ya da ulus devlet böyle bir saldırı başlatamaz (Wingfield, Michael ve Wijesekera, 2003, s.1-7).

Michael Schmitt kriterlerine göre bir saldırı kuvvet kullanımı seviyesine ulaştığında saldırıya maruz kalan devlet meşru müdafaa hakkına sahip olmaktadır. Tallinn Manual 2.0 versiyonu 71.maddeye göre meşru müdafaa'nın ise gereklilik, orantılılık, aciliyet (immediacy), yakınlık (imminence) kriterlerine uyduğu sürece yapılabildiği belirtilmektedir. (Schmitt, 2017, s.339)

Tallinn Manual'ın 72.maddesine göre yaklaşan bir siber saldırı veya gerçekleşmiş bir siber saldırı için gereklilik kriteri önemlidir. Örneğin, A devleti B devletine siber saldırıda bulundu ve B devleti karşılık verdi. Fakat daha sonra A devleti B devletinin haberi olmadan saldırıları durdurmaya karar verdi. Bu aşamada B devletinin yaptığı saldırılar gerekli olarak görülmektedir. (Schmitt, 2017, s. 349)

Orantılılık kriteri, siber saldırılarda meşru müdafaa konusu için önemlidir. Tallinn Manual 2.0 versiyonunun 23. maddesine göre bir siber saldırının gerçekleşmesine karşılık meşru müdafaa yapılması gerektiğinde silahlı saldırılardan da

yararlanılabilmektedir. Bu durum bir silahlı saldırıya siber saldırı ile karşılık verilirken de geçerliliğini korumaktadır. Fakat her iki durumda da eylemlerin orantılılık ilkesine uygun olması gereklidir. Orantılılık ilkesine dayanarak gereken tedbirlerin alınmadığı durumlarda, meşru müdafaa için gereken özen gösterilmediği için saldırıya maruz kalan devlet uluslararası hukuka aykırı davranmış olmaktadır. Örneğin, A ve B devleti ve ayrıca bir devlet dışı aktör düşünelim. Devlet dışı aktör A devleti üzerinden B devletine siber saldırıda bulunuyor. A devleti, devlet dışı aktörler karşısında gerekli önlemleri alması gereklidir. (Schmitt, 2017, s.127-130)

Tallinn Manual'ın 73. üncü maddesinde aciliyet ve yakınlık kriterinden bahsedilmektedir. Aciliyet kriteri, saldırıya maruz kalan devletin saldırı ve cevap arasında kalan zamanı olarak tanımlanmaktadır. Yakınlık kriteri ise bir saldırının öngörülmesiyle ilgilidir. Yakınlık kriterine göre bir devlet siber saldırıya maruz kalmaya yakın ise meşru müdafaa yapabilmektedir. (Schmitt, 2017, s.350-354)

DÖRDÜNCÜ BÖLÜM

SİBER SALDIRILARA UYGULANACAK OLAN HUKUK

4.1. Tallinn Manual ve Siber Saldırlara Uygulanacak Olan Hukuk

Siber saldırıların son yıllarda artışıyla beraber uluslararası alanda geçerli olacak hukuk kurallarına ihtiyaç duyulmuştur. NATO uzmanları tarafından 3 Eylül 2012 tarihinde Tallinn Manual adıyla siber savaşta uygulanmak üzere hukuk kuralları hazırlanmıştır. Uluslararası hukukta mevcut olan kuralların siber alana hangi şartlarda ve nasıl tatbik edileceği konusu üzerine gayri resmi bir belge niteliği taşımaktadır (Boyle, 2012, s.1-4). Belgede siber hukuk düzenini sağlamak için 95 kural bulunmaktadır. Bu kuralların uluslararası alanda bir yapılageliş kuralı olması hedeflenmiştir. Tallinn Manual'ın ikinci versiyonu ise 2017 yılının şubat ayında yayınlandı. Genel olarak bakıldığında ilk versiyon ve son versiyon arasında görülen en önemli fark el kitabının ismidir. İlk versiyonunun isminde “Tallinn Manual on the International Law Applicable to Cyber Warfare” ve ikinci versiyonun üstünde “Tallinn Manual 2.0 on the International Law Applicable to Cyber Warfare” yazmaktadır. İlk versiyonunda savaş (warfare) kavramının çok ağır ve endişe verici bir kavram olduğunu farketmiş olmalı ki ikinci versiyonunda siber operasyonlar (cyber operations) kavramını kullanarak değişikliğe gitmişlerdir (Ginsburg, 2017, s.205-206).

Tallinn Manual'ın hazırlanmasında NATO uzmanlarının katkısı olduğu için hazırlanan el kitabının siyasi yönelimi oldukça eleştirilmiştir. Yapılan projede Amerikan etkisinin bulunması ve projenin Amerikan çıkarını üstte tuttuğu düşünülmesi, yapılan eleştiriler arasında yer almaktadır. Fakat Tallinn Manual 2.0'ın yazımında farklı ülkelerden geniş bir uzman kitlesine başvurulmuş ve elliden fazla devletten yararlanılmıştır (Liu, 2017, s.390-391).

Tallinn Manual 3.0 projesi ise NATO Kooperatif Siber Savunma Mükemmeliyet Merkezi tarafından 2021 yılında başlatılmıştır. Tallinn Manual 1.0 ve Tallinn Manual 2.0 de daha önce rol oynayan Profesör Schmitt Tallinn Manual 3.0'ün de direktörlüğünü

yapmaktadır (http-3). Tallinn Manual'ın 3.0 versiyonunda yeni konulara değinileceği ve en fazla 5 yıl içinde bitirileceği söylenmektedir (http-4). Tallinn Manual uluslararası alanda bağlayıcılığı olmayan esnek bir belge olduğu için devletler açısından kabul edilmesi veya edilmemesi devletlerin tercihinine bırakılmıştır. Devletlerin siber hukuk alanında ortak bir görüş çerçevesinde Tallinn Manual'ın oluşturulmasına yardımcı olması, siber hukuk alanı için önemli bir katkı sağlamıştır.

4.1.1. Devletin gerçekleştirdiği siber saldırılar

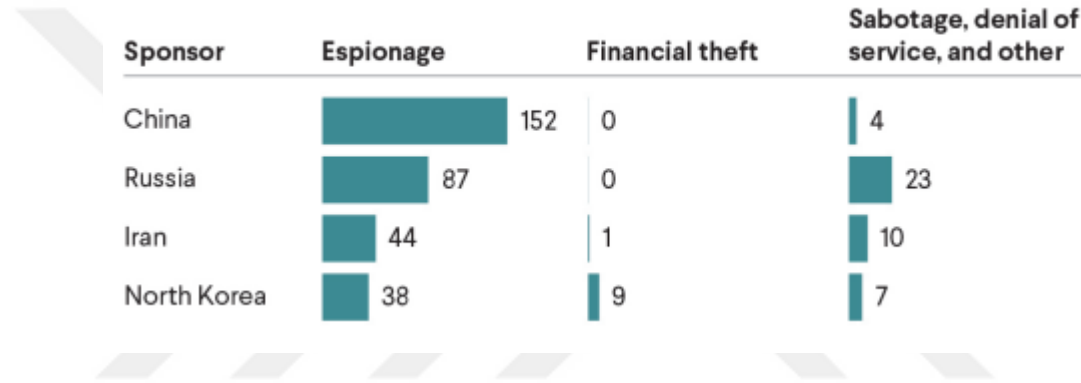
Uluslararası hukukta sorumluluğun ortaya çıkması için devletlerin hukuka aykırı bir durum sergilemesi gerekmektedir. Tallinn Manual'i yazan ekip devletin sorumluluğunun siber alanı da içine aldığını belirtmektedir. Uluslararası hukuk temel hukuk ve yardımcı hukukun tamamını oluşturmaktadır. Temel hukuk kuralı olarak BM Şartı'nın 2/4 maddesi örnek verilebilir. Bu maddede kuvvet kullanımının yasaklandığı belirtilmekte olup genel bir kural olduğu için birincil hukuka girmektedir. Yardımcı kurallar ise ikincil kurallar olarak adlandırılır ve siber hukuk kuralları bu kategoriye dahil edilmektedir.

Uluslararası hukukta devletin sorumluluğunun oluşabilmesi sadece devletin yaptığı fiillerden dolayı oluşmamaktadır. Devlet dışı bir aktörün yapacağı bir siber saldırıda devlet müdahalesi bulunursa, saldırı devletin sorumluluğuna girmektedir. Fakat bir siber saldırının devletin sorumluluğunda olup olmadığının detaylıca araştırılması gerekmektedir. Çünkü devletler yaptıkları siber operasyonlardan sorumlu tutulmamak için bulunduğu bölge dışından bu operasyonu yapabilirler. Bu bağlamda bir devletin bulunduğu topraklarda yapılan siber operasyonların denetlemesi oldukça zordur (Schmitt, 2017, s.79-80).

Devlet destekli gerçekleştirilen siber faaliyetler üç ana başlıkta incelenir; 1) Politik Mülahazalar 2) Espiyonaj 3) Bilgi Çarpıtma. Politik mülahaza kavramı ile bahsedilen durum, devlet büyüklerine yapılan siber saldırılardır. Bu saldırılarda devlet büyüklerinin veya devlet kurumlarının sosyal medyadaki hesaplarının ele geçirilip, hesaba ait kişi veya kurumun aleyhine olacak şekilde paylaşımlar yapılması bu saldırıların politik yönüne örnektir. Espiyonaj ise devletlerin casusluk yaparak bilgi elde etmek üzere yaptığı siber faaliyetlerdir. Espiyonajda elde edilen bilgiler karşı tarafı zor

durumda bırakmak için koz olarak kullanılabilir. Örneğin, bir devlet büyüğünün saklamak istediği bir bilgiye espionaj sayesinde ulaşan bir devlet, diğer devletin adımlarını yönlendirebilir. Bilgi çarpıtmada ise devlet kurumlarının hesaplarının çalınıp, farklı bilgiler yayımlanarak halka yalan haberler vermek amaçlanmaktadır (Hukuk ve Bilişim Dergisi, 2022).

Tablo 4.1. 2005'ten 2022'e kadar devlet destekli olduğundan şüphelenilen siber operasyonların sayısı, seçilmiş ülkeler



Kaynak: CFR Cyber Operations Tracker

Yukarıdaki tabloda 2005-2022 yılları arasında Çin, Rusya, İran ve Kuzey Kore'nin devlet destekli olduğundan şüphelenilen siber operasyonların amaçlarının espionaj, finansal hırsızlık ve sabotaj olduğu belirtilmiştir. Çin espionaj konusunda diğer üç ülkeden daha yüksek durumda gözükmektedir. Amerika'nın gizli devlet bilgilerinin çalınması ve Çin'in ekonomisini geliştirmek için gerekli olan dış dünyaya bağımlılığın azalmasını sağlayacak bilgilerin çalınması Çin'in espionaja başvurma sebepleri arasındadır (Council on Foreign Relations, 2022, s.25-26).

Siber operasyonların devlet destekli yapılıp yapılmadığının anlaşılabilmesi için UAD'nin yürüttüğü ABD'nin Nikaragua'ya karşı müdahalede bulunması ile ilgili olan Nikaragua Davası kararında bahsedilen "etkili kontrol ve ajans testi" testinin uygulanması gereklidir. Etkili kontrol testi sayesinde devletin olaylar karşısında gruplar üzerinde etkisinin ne kadar olduğunun ölçülebilmesi sağlanmaktadır. Bu kontrol sonucunda bir grubun arkasında devlet desteğinin olup olmadığının net bir kararı

verilmektedir. Devlet desteğinin ölçülmesinde belirli kriterler yer almaktadır. Kriterlerden ilkinde uluslararası insancıl hukukun gruplar tarafından devlet adına ihlal edilmesi belirtilmektedir. Başka bir kriter devletin bu gruplara talimat verebilmesidir. Diğer bir kriter ise grupların devlet tarafından finansının sağlanabilmesidir. Nikaragua davasında devletin finansman sağladığı üç gruptan bahsedilmektedir; 1) Devlet memurları ve askerler 2) Devletin görevlisi olmayıp devletin finansal destek verdiği bireysel olarak çalışanlar (ABD Vatandaşlığı yok ve talimatlı çalışan kişiler diğer adıyla UCLA'lar) 3) Kontralar. Temsilcilik testi (agency test) sayesinde ise bu gruplardaki kişilerin kamu görevlisi olup olmadığı araştırılmaktadır. Devletlerin bu gruplara verdiği desteklerden dolayı uluslararası hukuku ihlal etme durumu, davaların koşullarına göre değişiklik gösterebilmektedir. Siber saldırılarda da bu şekilde bir kontrol ve temsilcilik testinin gerçekleştirilmesi yargılanma aşamasında önem kazanacaktır (United Nations, 1999, s.41-48).

Michael Schmitt tarafından Ölçek ve Etkiler Okulu (The Scale and Effects School) adında bir yaklaşım ortaya atılmıştır. Bu yaklaşım siber saldırıların ölçeğine göre silahlı saldırı olarak değerlendirilip değerlendirilmeme ayrımının BM Şartı'na göre yorumlanmasını savunmaktadır. Bu yaklaşıma göre silahlı saldırıya ulaşmamış bir siber saldırı karşısında devletler, Güvenlik Konseyi'ne bildirmek ve meşru müdafaa olmadan saldıran devlete karşı küçük yaptırımlarda bulunmaktan başka herhangi bir adım atma şansı bulunmamaktadır. Her yaklaşımda olduğu gibi bu yaklaşım içinde önyargılar bulunmaktadır. Önyargı olarak geleneksel savaşın yarattığı tahribatın siber saldırılardan daha fazla olduğu savunulmaktadır. Geleneksel savaş ile siber saldırıların mukayese edilemeyeceği ve Tallinn Manual'in kusurlu olduğu konusu üzerine odaklanılmıştır (Eaton, 2021, s.716-717).

4.1.2. Denizde yapılan siber saldırıların durumu

Devletlerin münhasır ekonomik bölgesi, iç sular, karasuları, takımda devletlerinin takımda suları hariç bütün deniz bölümleri açık denizi oluşturur. Uluslararası hukukta farklı bir durum olmadığı sürece, açık denizde yapılan siber faaliyetler yalnızca barışçıl amaçlar ile yürütülmektedir. Açık denizde yapılan siber operasyonların meşruluğu sadece devletlere aittir ve devlet dışı aktörlerin burada faaliyet göstermeleri yasal değildir (Schmitt, 2017, s.233).

Münhasır ekonomik bölge bir devletin esas çizgisinden başlayıp 200 deniz miline kadar uzanan alana denilmektedir ve devletler bu alanda yargı yetkilerini kullanabilmektedir. Bu alanda başka bir devlet barışçıl amaçlar ile siber operasyonlar yapabilir. Fakat MEB’de kıyı devletinin zararına yapılacak herhangi bir siber saldırı durumunda kıyı devleti müdahale hakkına sahiptir. Barışçıl amaçlar için bile olsa kıyı devleti önlem alabilir (Schmitt, 2017, s.239). Bu kuraldan yola çıkarak diğer bir kural olan izleme hakkı ile bu kuralı bağdaştıralım ve bir örnek oluşturalım. Bir devlet başka bir devletin münhasır ekonomik bölgesinde barışçıl olmayan siber operasyonlar yaptıktan sonra açık denizlere kaçıyor ise eğer kıyı devletinin izleme hakkı açık denize kadar gidebilmektedir. Tallinn Manual’ın her iki versiyonuna baktığımız zaman münhasır ekonomik bölgede izleme hakkı üzerine bir kural yoktur. Ancak izleme hakkının bitişik bölgede FISC kurallarının ihlalinde yapılabileceğinden bahsedilir. FISC kuralının ihlalinde kıyı devleti gemiyi ya bitişik bölgeden ayrılmadan önce ya da ayrıldıktan sonra sıcak takip ile durdurma hakkına sahiptir. Tallinn Manual henüz geliştirilebilme aşamasında olduğu için izleme hakkı ile ilgili yeni kurallar konulabilir (Schmitt, 2017, s. 249).

Karasuları ise esas hattan 12 mile kadar ileri sürülebilen bir bölgedir. Bir devlet kıyı devletinin karasularından geçerken zararsız geçiş hakkı ile geçebilmektedir. Zararsız geçiş hakkı adındanda anlaşılacağı üzere kıyı devletine hiçbir zarar vermeden karasularından geçmek demektir. Bu zarar içinde siber operasyonları da dâhil edebiliriz. Kıyı devleti eğer karasularında siber operasyon yapmak isterse zararsız geçişi bir süreliğine kapatabilir. Ayrıca kıyı devletinin karasularındaki diğer bir devlet zararsız geçişte, kıyı devletine değil de başka bir devlete siber operasyonda bulunur ise kıyı devletinin güvenliğini tehlikeye düşürebilir. Uzmanlar bu konuda kıyı devleti ile siber operasyona maruz kalan devletin ilişkilerine göre durumun değişebileceğini söylemektedir. Uzmanların bu konuda bulduğu çözüm, kıyı devletinin zararsız geçişte bulunan devlete geminin acilen ayrılması için siber faaliyette bulunması gerektiğinin mümkün olduğudur (Schmitt, 2017, s.241-242). Uluslararası hukuka göre yorum yapmak gerekirse, bir devletin kıyı devletinin aleyhine zararsız geçişte yaptığı faaliyetlerle ilgili yargı yetkisi bulunmaktadır. Fakat burada konu kıyı devletinden bağımsız yürütülmekte olup, başka bir devlete saldırı olduğu için kıyı devletinin yargı yetkisinin bulunmadığı yorumu yapılabilir (Pazarcı, 2016, s.268). Kıyı devleti eğer

zararsız geiřte bulunan devlete hukuka aykırı olarak siber operasyonda bulunursa, saldırıya maruz kalan devlet karřı siber saldırı yapabilir. Bu mdahalenin diğerk uluslararası hukuk kurallarını zarara uğratmayacağı belirtilmiştir (Schmitt, 2017, s.244). Herhangi bir milletlerarası silahlı çatıřma ıkma durumunda, kıyı devletinin karasularında yapılan siber faaliyetler sonucunda savařan taraflar arasında kıyı devletinin ayırım gözetmemesi gerektiğı belirtilir. Tarafsız bir devletin karasularından geen bařka bir devlet, geminin gvenliğı iin siber faaliyette bulunabilir. Ayrıca tarafsız bir devletin karasularında bulunan devlet, tarafsız devlete karřı bir siber faaliyet yrtrse tarafsızlık yasasına gre tarafsız devlet karřı saldırıda bulunabilir (Schmitt, 2017, s.245-246). Srekli tarafsız devletlerin tarafsızlık statsnden dolayı hibir saldırıya girmediğı bilinmektedir. Ancak tarafsız devletlerde kendilerine bir saldırı geldiğinde karřı saldırı yapabilir ve bu tarafsız yasasının ihlaline neden olmaz (Pazarcı, 2016, s.179).

Bitiřik blge devletlerin kıyılarından 24 mile kadar uzanan blgeye denilmektedir. Bitiřik blgede kıyı devletleri siber operasyonlarda bulunabilir. Bu operasyonları yapabilmek iin bu blgede bulunan gemilerin parasal, g, saėlık ve gmrk yasalarını ihlal etmesi gereklidir (Schmitt, 2017, s.249).

Uluslararası boėazlara sınırdař devletler boėazlardaki deniz yatağı ve sulardan sorumludur ve karasularında yrrlkte olan haklardan faydalanırlar. Devletler uluslararası boėazlardan transit geiř hakkı ile hızlı geiř yapabilir. Transit geiřin zararsız geiřten farkı, transit geiřte boėazlara sınırı olan devletler herhangi bir mdahalede bulunamazlar. Uluslararası boėazlardan geerken de devletler siber saldırılar yapılabilir. Uluslararası bir çatıřma durumunda ise transit geiř yaparken devletler siber faaliyetlerde bulunamazlar. Transit geiř yaparken siber faaliyetler yapıldığında, kıyı devleti bu faaliyetten dolayı transit geiř yapan devleti yargılayamaz. Transit geiř yaparken herhangi bir siber faaliyet yapıldığında kıyı devleti sadece boėazı terk etmesini isteme yetkisi bulunmaktadır. Bazı durumlar gemilerin boėazdan geiřini etkileyebilir. Bu durumlar ise boėazın dar olması ve boėazda rejimlerin farklı olmasıdır. İki duruma rnek olan İstanbl boėazıdır (Schmitt, 2017, s.249-251).

Takımada sularında da siber operasyonlar yapılabilir. Fakat buradaki řart bu sularda geerli olan rejimle siber operasyonların orantılı olmasıdır. Takımada sularından

geçiş yapan devletler kendi güvenliğini sağlamak için siber operasyonlarda bulunabilir. Diğer maddelerde olduğu gibi takımda sularında kıyı devletine karşı yapılan bir siber saldırı da veya kıyı devletine değil de başka bir devlete yapılan saldırıda, kıyı devleti siber saldırı yapan devlete karşı takımda sularından ayrılması gerektiği uyarısında bulunabilir.

Denizaltı iletişim kabloları ise devletlerarası iletişim ve veri gidiş gelişinin sağlanması açısından önemlidir. Kıyı devletinin karasularında, uluslararası boğazlardan transit geçişle geçilen yerlere denizaltı kabloları yerleştirilebilir ve bu kabloların yerleştirilmesinden dolayı kıyı devleti bu duruma riayet etmelidir. Fakat bu kablolar karasularından ve boğazlardan geçişleri engellememelidir. Bu tür kablolarla yapılan saldırılar uluslararası iletişimin tıkanmasına sebep olmaktadır. Devletler denizaltı iletişim kablolarında sonucu öngörülemez değişimlere sebep oldukları zaman bu durumlardan mesul tutulamazlar (Schmitt, 2017, s.251,252).

4.1.3. Hava sahalarında gerçekleştirilen siber saldırıların durumu

Yeni nesil uçaklar uzaktan bilgisayarlar üzerinden yönetilebilirler ve birbirlerine bağımlıdırlar. Bu iki taraflı bağ, başka bilgisayarlar tarafından koparılabilir veya değiştirilebilir. Bundan dolayı uçaklar siber operasyonlara karşı zayıf durumdadır. Uçaklara siber operasyon yapılarak yanlış sinyaller gönderilmesi sağlanır. Özellikle asker uçaklarına gönderilen sinyaller dolayısıyla uçakların hedef yönleri değiştirilebilmekte ve silahların farklı yönlere dağılmasına sebep olmaktadır.

Uluslararası hava alanında seyir halinde olan devletlere ait uçaklar, başka devletlere karşı siber faaliyetler yapabilir. Fakat yapılan siber faaliyetin kötü amaçlar içerdiği durumlarda uluslararası hukuka aykırı olması kaçınılmaz bir durumdur. Yapılan bir siber faaliyet dünyayı aşp uzayı da kapsıyorsa hem hava hukuku hem de uzay hukuku uygulanır. Burada verilebilecek en iyi örnek, bir hava taşıtının uyduya siber operasyon yapması olmaktadır. Çünkü havada yapılan operasyon hava hukukunu, uzayda bu operasyonun sonuca bağlanması da uzay hukukunun uygulanmasını gerektirmektedir. Herhangi bir silahlı çatışma durumunda siber faaliyetler için hava taşıtlarının kullanılması, çatışmalara dahil olup olmamak fark etmeksizin devletlerin hareket özgürlüğü kapsamına girmektedir.

Bütün devletler, kendi ulusal hava sahasının giriş çıkışlarını düzenlemekle yükümlüdür. Chicago Sivil Havacılık Sözleşmesine göre tarifeli uçakların ulusal hava sahalarından geçişi serbesttir ve önceden izin alınmasına gerek yoktur. Tarifeli uçaklar ile uçakların gidiş dönüş saatinin önceden programlanmış olduğu uçaklar kastedilmektedir. Tarifersiz seferlerde belirli bir süreklilik görülmez. Tarifeli uçaklar geçişinde öncesinden izin alınma durumu yoktur fakat tarifersiz uçaklar da hava sahasından geçmeden izin alınması gereklidir. Ayrıca devletler herhangi bir güvenlik sıkıntısı yaşadığı olağanüstü durumlarda ise kendi topraklarında hava yolunu kapatma yetkisine sahiptir. Devletler kendini tehlikede gördüğü ve hava yoluyla yapılacak siber operasyonlar dolayısı ile de hava sahasını kapatma yetkisini elinde tutar.

Devletler kendi hava sahasında yetkiye sahip olduğu için hava sahasında işlenen suçlardan dolayı hava araçlarının inmesini talep edebilir. Bu işlenen suçlara siber operasyonlar da dâhildir. Örneğin, ulusal hava sahasında başka bir devlet uçağının internet bağlantılarını hacklemesi, kişisel verilerin dinlenmesi ve bu verilerin yayımlanması üzerine yapılan suçlarda hava taşıtının inmesi talep edilebilir. Eğer ulusal hava sahasını ihlal eden devletin yaptığı siber operasyonlar silahlı çatışma durumuna ulaşırsa, silahlı çatışmaya maruz kalan devletin meşru müdafaa hakkına ve buna istinaden kuvvet kullanmaya başvurma hakkı vardır. Bir devletin kendisi de kendi ulusal hava sahası içerisinde siber faaliyetler yürütme hakkına sahiptir.

Uluslararası hava sahası ise ulusal olmayan hava sahalarının dışında kalan alanlara denmektedir. Bu alanlarda hiçbir devlet hak iddia edemez. Bu yüzden de burada siber operasyonlar yapmak serbesttir. Fakat bu alanda yapılan yasal olmayan müdahaleler uluslararası hukuka aykırı nitelik taşımaktadır (Schmitt, 2017, s.259-269).

4.1.4. Uzayda gerçekleştirilen siber saldırıların durumu

Uzayın sınırlarının belirlenmesi yıllardır tartışılan bir konudur ve bu tartışmaların üzerinden hava sahası ve dış uzay arasında bulunan bölgenin uzay olduğu kararlaştırılmıştır. Bu alanda hiçbir devlet gök cisimleri üzerinden hak iddia edemez. Uzayda yapılan siber operasyonlara uyduların hacklenmesi, uzaydan yeryüzüne yapılan iletişimin bozulması, verilerin değiştirilmesini örnek verebiliriz.

Uzaydaki gök cisimlerinde siber faaliyetler yürütülebilir fakat bu faaliyetler barışçıl olma amacı taşımalıdır. Bir devlet başka bir devletin barışçıl amaçlar ile uzayda yaptığı bir faaliyeti engelleyemez. Fakat uzayda olan silahlı saldırı niteliği taşıyan siber saldırı konusunda devletler engelleyebilme hakkına sahiptir. Bu engelleme hakkı ise meşru müdafaadan gelmektedir.

Uzaya gönderilen aletler ile ilgili Tescil devleti sorumludur. Bir ürünün tescil devleti her zaman tektir. Örneğin, uzaya birkaç devletin iş birliği ile tek bir uydu gönderildiğini varsayalım. Bu gönderilen uydunun tescil devleti tek bir devlet olmalıdır. Bunun kararını devletler ortaklaşa verir ve bir devlet seçerler. Seçilen devlet uzay aracının Tescil devleti olur. Gönderilen uyduya herhangi bir zarar verildiğinde, Tescil devleti o zararın yaptırımını ve tazmini üzerine etkin bir rol oynamaktadır.

Uzaya gönderilen astronotlar insanlığın uzaydaki temsilcisi olarak anılmaktadır. Astronotlar uzayda herhangi bir problemle karşılaştıklarında devletler ortaklaşa yardım etmekle yükümlüdür. Uzaya yönelik bir siber operasyonun yapılması sırasında astronotlara zarar verilmesi durumu oluşmasından dolayı devletler bu konuya dikkat etmelidir (Schmitt, 2017, s.270-283).

4.1.5. Uluslararası hukuka göre dokunulmazlıktan yararlanan konuları hedefleyen saldırılar

Uluslararası hukukta dokunulmazlık durumunda olan dini yerler, kültürel yerler, sivil halkın yaşamını idame ettirebilmesi için gerekli olan yerlere saldırılar Cenevre Sözleşmelerine İlişkin Ek Protokol olan Uluslararası Silahlı Çatışma Kurbanlarının Korunmasına İlişkin Protokolünde yasaklanmıştır (Pazarcı, 2017, s.598). Tallinn Manual 1.0 versiyonunun 47.maddesinde dokunulmazlık durumunda yer alan bu yerlere yapılan siber saldırıların yasaklanmasını içerir (Schmitt, 2017, s.152). Tallinn Manual 2.0 versiyonunda ise 109.maddede dokunulmazlık durumunda olan yerlere yapılan saldırılardan bahsedilmiştir. Maddede Eski Yugoslavya İçin Uluslararası Ceza Mahkemesinin kararıyla sivillere yapılan saldırıların uluslararası hukuka aykırı olması konusuna referans verilmektedir (Schmitt, 2017, s.463-464).

4.1.6. Önleyici savaş kavramının siber saldırılarda geçerlilik durumu

Önleyici savaş kavramı, bir devlet, saldırı yapmaya meyilli diğer devletin saldırı yapacağını önceden bildiğinde, saldırı yapması muhtemel olan devlete karşı önceden müdahale yapması anlamına gelmektedir. Tallinn Manual 1.0 versiyonunun 15.maddesinde bu konuya değinilmiş olup önleyici meşru müdafaanın siber saldırılarda geçerli olduğu sonucuna varılmıştır (Schmitt, 2013a, s.152). Maddede Caroline Olayı önleyici meşru müdafaaya örnek olarak verilmiştir. Bu olaya göre 1837 yılında Kanada ile İngiltere arasında yapılan bir savaşta, Kanada'ya Amerika yardım etmiş Caroline gemisini vermiştir. Caroline gemisi Kanada'ya silahlı yardım yapmıştır. Kendisini tehdit altında gören İngiltere Caroline gemisini Niagara Şelalesi'nden atmıştır. İngiltere'nin yaptığı bu eylem tarihe önleyici meşru müdafa olarak geçmiştir (Değdaş, 2017, s.32-35).

Geleneksel savaşta olduğu gibi siber saldırılarda da önleyici meşru müdafa durumunun tartışmaları sürmektedir. İki savaş türünde de önleyici meşru müdafaanın uluslararası hukukta yerinin olup olmayacağı konusunda tartışma yer almaktadır. Önleyici meşru müdafa kavramının geleneksel savaşta kullanılabilmesi kolay olmaktadır. Çünkü saldırı yapmaya meyili olan karşı tarafın kim olduğu bellidir. Fakat siber saldırılarda saldırıyı yapan tarafın kim olduğunu bulabilmek zordur. Bir devlet başka bir devlet üzerinden de silahlı saldırı yapabilir bu durumda tam olarak siber saldırının hangi devlete isnat edilebilirliği konusunda sıkıntı çıkabilmektedir (Kadıoğlu, 2022, s.35-41).

Düşmanlıkların Açılmasına İlişkin Lahey (Convention relative to the Opening of Hostilities. The Hague) sözleşmesinin 1.maddesinde devletlerin saldırı yapacakları zaman, bu saldırıyı kimin yapacağına ve bu saldırının kime yapılacağına ilişkin bir uyarı vermesi gerektiği belirtilmiştir. Fakat siber saldırılarda sadece saldırıya uğrayan tarafın belirli olması nedeniyle bu madde önemini yitirmektedir (http-5).

4.1.7. Diplomatik ve konsolosluk hukuku temsilcileri tarafından gerçekleştirilen siber saldırılar

1961 Diplomatik İlişkiler Viyana Sözleşmesi ve 1963 Konsolosluk İlişkileri Viyana Sözleşmesine göre diplomatik temsilcilikler ve konsolosluklarda çalışan kişilerin dokunulmazlık hakkı bulunmaktadır. Ayrıca 1969 Özel Görevler Sözleşmesine dayanarak geçici görevlendirme ile gönderen devletin kabul eden devlette bir temsilci bulundurması ve bu temsilcinin dokunulmazlık kararı tartışmalıdır. Uluslararası Uzmanlar Grubuna göre bu temsilciler de dokunulmazlık hakkından yararlanabilmektedir. Fakat temsilciyi gönderen devletin kabul eden devlette siber alanı kullanarak casusluk suçuna karışması dokunulmazlık hakkına hâlel getirilmesi hepsi için geçerli sayılmaktadır (Schmitt, 2017, s.209-230).

4.1.8. İnsan hakları hukukuna aykırı yapılan siber saldırılar

Uluslararası uzmanlar grubuna göre, insan hakları hukukunda geleneksel olan kurallar ve anlaşmalar ile getirilen kuralların siber saldırı yapılarak ayrı bir şekilde incelenmesi gerektiği belirtilmiştir. Antlaşmalar hukukuna göre saldırıların yorumlanması farklılık gösterebilmektedir. Devletlerin bazı koşullarda insan haklarını kısıtlayabilme hakkı bulunmaktadır ve bu siber saldırılar içinde geçerli olabilir. Devletlerin tamamı uluslararası yapılmış olan insan hakları ile ilgili antlaşmalara dahil olmadığı için siber saldırıların insan haklarını ihlal etmesi farklı şekillerde yorumlanabilir. Uluslararası antlaşmalara bağlı olan her devlet anlaşmayı onayladığı anlamına gelmemektedir. Devletler antlaşmalarda bazı maddelere çekince koyabilmektedir ki bu da siber saldırıların yorumlanmasını etkileyebilir (Schmitt, 2017, s.179-207).

4.2. Avrupa Konseyi Siber Suçlar Sözleşmesi

Avrupa Konseyi Siber Suçlar Sözleşmesi, Avrupa Konseyi Siber-Uzay Suçları Uzman Komitesi tarafından beş yıllık bir çalışma ile hazırlanmış ve 2001 yılında yayınlanmıştır. Siber suç alanının ilk milletlerarası sözleşmesidir ve bu sözleşmenin diğer adı Budapeşte Sözleşmesi olarak geçmektedir. Sözleşmenin imzacı devletleri hem

Avrupa Konseyi üyeleri hem de Konsey'e üye olmayan devletleri içermektedir. Sözleşmeye imza atan devletlerin sayısı 68 olmuştur. Sözleşmeye devletlerin kolayca çekince koymaları, imzacı devletlerin temsil sürecinde yeterince eşit davranılmaması gibi durumlar nedeniyle eleştirilmiştir.

Sözleşme 48 madde içermekte ve 4 bölümden oluşmaktadır. İlk bölümde siber suç kavramlarının tanımlarına değinilmektedir. İkinci bölümde ise ulusal düzlemde alınacak tedbirleri içermektedir. Üçüncü bölümde ise yargı yetkisi konuları ele alınmaktadır. Son bölüm ise Sözleşmenin devam edilebilirliğinin sağlanması için gerekli olan hükümler bulunmaktadır. BM Antlaşması'nın ikinci maddesinde uluslararası iş birliğinin öneminden bahsedildiği gibi, Siber Suçlar Sözleşmesi 23.maddesinde de iş birliğinden bahsedilmektedir (Aliusta ve Benzer,2018, s.37-38).

Sözleşmede 4 ana suç grubundan bahsedilmektedir ve bunlar; 1) bilgisayarda bulunan verilerin gizliliğini ihlal eden suçlar, 2) bilgisayarla ilgili sahtekarlık ve dolandırıcılık suçları, 3) çocuk pornografisi gibi içerik suçları 4) telif hakkının ihlali ile ilgili suçlar. Sözleşmede bu alanlar ile ilgili herhangi bir durum oluştuğunda dijital delillerin toplanması konusu ile ilgili iş birliğinin yapılması hususuna değinilmektedir. İşbirliğinin kolayca sağlanabilmesi için sözleşmeye taraf devletlerin ulaşabileceği ortak bir ağ yaratılması belirtilmiştir (Clough,2014, s.699-707).

Sözleşmede siber saldırıların yargı mekanizması olarak saldırının işlendiği yerdeki kanunlara bırakıldığı 22.madde yargı yetkisi başlığı altında açıkça belirtilmiştir. Yapılan bir saldırıya sözleşmeye taraf birden fazla devletten yargı talebi geldiğinde, konunun muhatabı tarafların, en uygun olan biçimde yargılanma konusunun takibinin nasıl olacağını birbirlerine danışması öngörülmüştür.13.maddede imzacı devletlerden her birinin sözleşmede geçen suçlar için gerekli olan önlemleri alacağından bahsedilmiştir. Madde 45 ve 46'ya göre, imzacı devletler arasında herhangi bir anlaşmazlık olduğunda, sorunların çözümü için Suç Problemleri ile İlgili Komite'ye (CDPC) ilk olarak başvurabilmektedir. CDPC bu sözleşmenin yorumlanmasında ve imzacı devletlere aktarılmasında önemli bir yer tutar ve ardından imzacı devletler bir hakem veya UAD'ye başvurabilirler (Avrupa Konseyi Siber Suçlar Sözleşmesi, 2001, s.11-22).

4.3. Siber Suçlar Üzerine BM Genel Kurul Kararları

Son 20 yılda bilgisayar güvenliğine saldırıların artması devletler arasında paniğe yol açmıştır. Bu endişeler karşısında BM siber alanın güvenliği konusunda yeni kararlar alma girişimi başlatmıştır. Vatandaşlar, şirketler ve devletlerin siber alanda güvenliğini sağlayabilecek kararlar alınmıştır. BM Güvenlik Konseyi siber alanın güvenliği konusunda şimdiye kadar 2341 (2017) sayılı karardan başka bir karar almamıştır. Fakat siber alanın başka yönlerinin düzenlenmesine ilişkin BM Genel Kurulu'nun üç komitesi nin verdiği taslak kararlar Genel Kurul'a bildirilmiş ve Genel Kurul tarafından kabul edilmiştir. Silahsızlanma ve Uluslararası Güvenlik Komitesi, Ekonomik ve Mali Komite ve Sosyal İnsani Komite taslak kararların hazırlanmasında katkısı bulunan komitelerdendir. Silahsızlanma ve Uluslararası Güvenlik Komitesi, siber güvenlik alanında kural oluşturma konusunda Rusya'nın 1998 yılında verdiği önergeden beri faaliyet göstermektedir. Rusya siber güvenlik konusunda yaptığı girişimlere 2001 yılında sunduğu öneri ile yeni bir boyut getirmiştir. Bu öneride siber güvenlik alanının geliştirilmesi ve tehditlerin ele alınma şekillerinin oluşturulması için 15 kişiden oluşan Uzmanlar Grubu oluşturulması talep edilmiştir. ABD Rusya'nın önerilerine karşı çıksa da Obama döneminde Rusya'ya karşı izlenen ılımlı politika neticesinde Rusya ile siber alanda iş birliği yapmaya karar vermiştir.

UNGA 65/201 sayılı karar ABD ve Rusya iş birliği ile 2010 yılında çıkmıştır. Diğer Amerika Rusya iş birliği ile alınan karar 2015 yılında çıkan UNGA 70/174 sayılı karardır. BM Genel Kurulu tarafından 58/199 sayılı karar 2003 yılında çıkmıştır. BM İnsan Hakları Konseyi 20/8, 26/13, 68/167 ve 69/166 sayılı kararlarını siber alanda insan haklarının korunabilmesi üzerine çıkarmıştır. 2017 yılında alınan UNGA 72/237 sayılı kararda meşru müdafaa hakkı ve insancıl hukukun siber alanda nasıl uygulanacağından bahsedilmektedir. UNGA 73/266 sayılı karar neticesinde 2019 yılında Açık Uçlu Çalışma Grubu kurulmuştur. 2002 yılında yayınlanan UNGA 57/239 sayılı kararda siber güvenlik kapsamında bir siber kültür oluşturmaktan bahsedilmektedir. UNGA 58/199 sayılı karar ile devletlerin sahip olduğu kritik altyapıların korunması konusunda iş birliği yapmayı anlatmaktadır. Kritik altyapılarla ilgili diğer bir karar ise UNGA 64/211 sayılı karardır (Eldem, 2021, s.17-45).

4.3.1. 57/239 numaralı karar

Birleşmiş Milletler, gelişen yeni teknolojilerin savaş şartlarını değiştirmesi üzerine siber alanda güvenliğin sağlanması için kararlar yayınlamıştır. 20 Aralık 2002 tarihli 57/239 numaralı karar incelendiğinde kararda siber alan güvenliğinin sağlanması için devletlerin ortak bir kültür oluşturmasını anlatmaktadır. Bu kültürün oluşması için dokuz madde verilmiştir; 1) Farkındalık 2) Sorumluluk 3) Yanıt 4) Etik 5) Demokrasi 6) Risk değerlendirmesi 7) Güvenlik tasarımı ve uygulaması 8) Güvenlik yönetimi 9) Yeniden değerlendirme.

Farkındalık konusu devletlerin siber güvenlik alanı ile ilgili farkındalık sahibi olabilmelerini ve sorumlulukta ise konu hakkında ne yapmaları gerektiği üzerine adım atmaları kastedilir. Yanıtta katılımcılardan yapılan faaliyetler ile ilgili hızlıca aksiyon almaları beklenmektedir. Etik konusu devletlerin birbirlerinin menfaatlerini zora düşürecek davranış sergilememesini içerir. Demokrasi ise devletlerin birbirleri ile istişare içinde olmaları anlamına gelir. Risk değerlendirmesinde devletlerin risk almaya açık olmaları söylenmektedir. Güvenlik tasarımı ve uygulamasıyla devletlerin güvenliğinin sağlanması için sistem ve ağ tasarımını uygulamalarını anlatmaktadır. Güvenlik yönetimi, devletlerin kapsamlı bir güvenlik idaresi anlayışını özümsemesini kasteder. Yeniden değerlendirme ise devletlerin siber güvenlik gerekli önlemleri almaları, sistemlerin güvenli olup olmadıklarının gözden geçirilmesi gibi görevlere tabi olunmasını anlatmaktadır (BM Genel Kurul Kararı, A/RES/57/239, 31.01.2003).

4.3.2. 58/199 numaralı karar

23 Aralık 2003 tarihli 58/199 sayılı BM kararı ile devletlerin siber alanda mücadele etmede iş birliği yapmalarını, siber alan ile ilgilenen bireyler yetiştirmeleri, siber alan ile ilgili ulusal faaliyetler yapmalarını ve bu faaliyetler ile asayişin sağlanmasını anlatmaktadır. Bu kararda karşımıza kritik bilgi sistemlerinin korunmasına yönelik maddeler çıkmaktadır. Birinci maddede güvenlik açıkları için devletlerin hızlı uyarı sistemlerine sahip olması, ikinci maddede siber güvenlik alanına ilişkin farkındalığın artması, üçüncü maddede altyapıların gözden geçirilmesi ve aralarındaki bağın anlaşılmasını incelemek, dördüncü maddede kamu ve özel sektörün siber güvenlik konularıyla ilgili bilgi alışverişinde bulunması, devletlerin kriz anında

birbirleriyle haberleşmeleri için ağ kurmaları ve bu ağların güvenli kalmaları üzerine denenmesi, altıncı maddede verilerin kullanılması üzerine oluşturulan politikaların kritik bilgi altyapılarını dâhil etmesi, yedinci maddede kritik bilgi altyapısına yapılan saldırıların incelenmesi ve bu saldırıların bilgilerinin diğer devletler ile paylaşılması, sekizinci maddede herhangi bir saldırıya karşı eğitimler düzenlenmesi ve tatbikatların yapılması, dokuzuncu maddede devletlerin siber saldırılara uygulanacak olan araştırmaları yapmaları için personel yetiştirmeleri, onuncu maddede uluslararası işbirliğinin öneminden, sonuncu maddede ise hem ulusal hem de uluslararası arge projelerinin yürütülmesinin teşvik edilmesinden bahsedilmektedir (BM Genel Kurul Kararı, A/RES/58/199, 30.01.2004).

4.3.3. 55/63 numaralı karar

22 Ocak 2001 tarihli 55/63 numaralı kararda bilginin kötü amaçlı kullanımı ile mücadele başlığı bulunmaktadır. Bilginin kötüye kullanımına ilişkin nasıl önlemler alınması gerektiği maddelerle açıklanmıştır. Birinci maddede devletlerin yasalarda suçluların suç işlemlerini sağlayabilecek herhangi bir açık bırakmamasından bahsedilir. İkinci maddede uluslararası suçların bilişim teknolojileri kullanılarak işlenmesi durumunda, yasal işlemlerin yürütülmesi için tüm devletler arasında iş birliği yapılması ve suçların araştırılarak mahkemeye taşınması gerekli olduğu belirtilmiştir. Üçüncü madde siber suçlarla mücadele etmek için devletler arasında bilgi alışverişi yapmak gerektiği söylenmektedir. Dördüncü madde siber suçlarla mücadele ederken, kolluk kuvvetlerinin bu mücadele hakkında bilgilendirilmesinin öneminden bahsetmektedir. Beşinci maddede cezai soruşturmalara ilgili hukuki sistemler tarafından verilerin saklanması ve gerektiğinde erişiminin sağlanması üzerine çalışmalar yapılması gerektiği belirtilmektedir. Altıncı maddede yapılan suçların zamanında soruşturulması ve delillerin zamanında toplanması gerektiğinden bahsedilmektedir. Yedinci maddede suçların tanımlanması ve mücadele etme konusunda halkın bilgilendirilmesi gerektiği belirtilmektedir. Sekizinci maddede bilgi teknolojilerinin suçluların belirlenmesi, izlenmesi ve kanıtların yardım etmesi gerektiğinden söz edilmektedir. Dokuzuncu maddede ise hükümetlerin bilgi teknolojileri üzerine yapılan suçlarla ilgili çözüm arayışında olmaları gerektiği belirtilmektedir (BM Genel Kurul Kararı, A/RES/55/63, 22.01.2001).

4.3.4. 74/247 numaralı karar

Metin, bilgi ve iletişim teknolojilerinin devletlerin gelişimine yardım ettiği, ancak aynı zamanda suç seviyelerinin ve karmaşıklığının artmasına sebep olduğunu belirtmektedir. Gelişen bilgi teknolojilerinin ve suç seviyelerinin artmasının devletlerin kritik yapılarına ve bireysel alana tehdit oluşturduğundan ve bu tehditlerin devletlerarasında iş birliği yapılarak bertaraf edilebileceğinden bahsedilmektedir. Alınan kararda bilgi ve iletişim teknolojilerinin kötü kullanımına istinaden bir uluslararası sözleşme hazırlamak ve devletlerarası ad hoc uzmanlar komitesi kurmaya davet etmektedir. Ad hoc komitenin finansmanı üzerine BM bütçesinden belirli bir pay verilmesi talep edilmektedir (BM Genel Kurul Kararı, A/RES/74/247).

4.3.5. 73/27 numaralı karar

Kararda bilgi ve iletişim teknolojilerinde güvenliğin artırılmasına yönelik devletlerin işbirliği içinde olmaları ile ilgili maddeler yer almaktadır. Uluslararası hukukun gerekliliklerine dayanarak devletler hukuka aykırı davranışlarda bulunmamalıdır. Siber saldırılarda atıf sorunları oluşabileceğinden dolayı yapılan bir saldırı detaylıca incelenmeli, saldırıyı yapan devlet mi yoksa o devletin bilgi ve teknoloji sistemleri kullanılarak oluşturulan bir saldırı mı bu ayrımın yapılabilmesi oldukça önemli olduğu belirtilmiştir. Bir devlet başka bir devlet ile anlaşarak siber saldırı yapılması için kendi toprağının kullanılmasına izin vermemelidir.

73/27 numaralı karar diğer kararlara bakıldığında siber güvenlik alanında bir norm oluşturma konusunda hukuki açıdan önemli bir karardır. Diğer kararlarda bahsedilen devletler arasında uluslararası işbirliği durumu bu karar içinde geçerlidir. Kararda bahsedilen diğer konulardan biri bir devlet siber saldırıya maruz kaldığında başka bir devlet bu saldırının kovuşturulması için maruz kalan devlete yardım edebilme hakkına sahiptir. Bu maddeyi koruma sorumluluğu kavramına benzetebiliriz. Koruma sorumluluğunda muhtaç olan devlete yardım etme hakkı vardır. Bu madde koruma sorumluluğu kavramının siber alanda uygulanmasına dair yeni tartışmalara sebep olabilir (BM Genel Kurul Kararı, A/RES/73/27, 11.12.2018).

4.4. Avrupa Birliđi ve Siber Gvenlik Kararları

Siber sular, iyi kaynaklara sahip devlet aktrleri ve devlet dıřı aktrler tarafından iřlenerek AB yesi lkelerin karřı karřıya olduđu benzersiz bir zorluđa neden olmaktadır. Avrupa'daki endstriler ve dıřıřleri bakanlıđı yapılan tehdit ve casusluklarla karřı karřıya olmaktadır. 2020 yılında Almanya'da bir hastaneye yapılan siber saldırıdan dolayı hastane sisteminin kullanılamaz hale gelmesi bir rnek olarak karřımıza çıkmaktadır (Weber and Toriser, 2021, s.2). Dijitalleşmenin gelişmesiyle birlikte devletler siber tehditlere açık hale gelmiştir. Avrupa Komisyonu'nun açıkladıđı verilere gre sadece 2020 yılında yapılan siber saldırıların maliyeti 5.5 trilyon Euro olarak belirtilmiştir ([http-6](http://6)).

AB'de 1976 yılından beri siber gvenlik hakkında uzmanlar grüş alıřveriřinde bulunmuřtur. Yapılan bu uzman grüşmelerinin szleşmeye dklmesiyle 2001 yılında "Avrupa Siber Sular Szleşmesi" ortaya çıkmıştır. Ardından siber gvenlik alanıyla ilgili AB'nin yaptıđı en nemli řey 2019 yılında "Siber Gvenlik Yasası" çıkartmak olmuřtur (Nezgitli ve Benzer, 2020, s.11). AB siber tehditler karřısında yasal mevzuatlar çıkarmaya devam etmektedir. AB'nin amacı siber saldırganların soruřturması yapılırken oluřabilecek hataların en aza indirgenmesinin sađlanması iin mevzuatın uluslararası bir hale gelmesini gerekleřtirebilmektedir. AB'nin uluslararası bir mevzuat çıkarma yolunda ye devletlerdeki siber gvenlik mevzuatlarının karřılařtırılması ve uyumlu duruma getirme abaları devam etmektedir (Redford, 2011, s.34-37).

AB'nin siber saldırıların ciddi bir boyuta ykseldiđini kabul ettiđi ilk saldırı Estonya saldırısıdır. 2007 yılında Rusya'nın Estonya'ya yaptıđı geici hizmet saldırıları AB'nin siber alan ile ilgili hazırlıksız olduđunu ortaya çıkardı. AB yapılan saldırılar karřısında kaynak eksikliđi ve belirli bir strateji olmamasından dolayı hi bir destek sađlayamadı. Ardından Notpedya adında Rusya'nın çıkardıđı iddia edilen bir virs Avrupa lkelerine yayıldı. (Martinez, 2018)

Geleneksel savařlarında AB'nin siber saldırılar ile ilgili politika yapımı srelerinde etkisi olmuřtur. rneđin, Rusya'nın Ukrayna'yı iřgali sonrası AB, devletlerin siber gvenliđinin sađlanabilmesi iin "AB Siber Savunma Politikasını" ne srmuřtur. AB'de Dijital řef olarak grev alan Margrethe Vestager'e gre siber

savunmanın AB için oldukça önemli olduğunu ve askeri ve sivil kaynaklarımızı koruma kabiliyetimizi artırdığını söylemektedir. (Bertuzzi, 2020)

Avrupa Birliği'nin siber güvenliğinin sağlanmasında önemli bir kurum olan ENISA (European Union Agency for Cyber Security), AB ve dünyanın maruz kaldığı siber alanla ilgili olayları araştırmış ve bir rapor oluşturmuştur. Dünya üzerinde her gün 230 binden fazla yeni kötü amaçlı yazılımların ortaya çıktığı, verilerin gizliliğini ihlal eden durumların tespit edilebilmesinin 6 ay gibi bir süre gerektirdiği ve kurum ve kuruluşlarda çalışanların bilgisayarlarından birbirine bulaşan kötü amaçlı yazılımların oldukça arttığı belirtilmiştir. Dış tehditlerin giderek artmasıyla beraber AB, üye devletler arasında koordinasyonu sağlamak ve üye devletlerin siber alanda güvenliğinin sağlanması için bazı yasalar ortaya çıkarmıştır. AB Siber Güvenlik Yasası, AB Siber Dayanıklılık Yasası, AB Siber Güvenlik Stratejisi, Ağ ve Bilgi Sistemleri Direktifi, AB'nin hazırladığı yasalar arasındadır. (Sciacca, 2020, s.2-17)

4.4.1. Avrupa Birliği siber güvenlik yasası (Cyber act)

Avrupa Birliği Siber Güvenlik Yasası 2019 yılında yürürlüğe girerek siber güvenliğin sağlanmasında önemli bir kurum olan ENISA'nın güçlenmesine katkı sağlamaktadır. Siber Güvenlik Yasası, ENISA'ya siber güvenlik sertifika çerçevesi hazırlama yetkisini verdi. ENISA, yapılan sertifikalar ve belgelendirmeler hakkında bilgilendirme yapmak üzere görevlendirildi. ENISA, AB'ye üye devletler arasında siber alanda gerçekleşecek saldırılar karşısında üye devletler arasındaki iş birliğini artırma amacını taşımaktadır (Upguard, 2023). ENISA siber güvenlik alanı hakkında AB kurum ve kuruluşları dışında uzmanlardan tavsiyelerini göz önünde bulundurmaktadır. Hukuki yönden ise ENISA siber güvenlik alanı ile ilgili hukukun oluşturulması ve geliştirilmesi için gerekli olan tüm faaliyetlerle ilgilenmektedir. Avrupa Birliği alanı içinde tehditlere hazırlıklı olmak amacıyla ENISA siber güvenlik alanı ile ilgili tatbikatların yapılmasını amaçlamaktadır. Bu çerçevede ENISA AB'nin siber güvenlik alanındaki bütün gelişmeleriyle ilgililecek ve AB'nin bu alanda geliştirilmesini sağlayacak çalışmalar yapacaktır. ENISA'nın yönetiminde her AB üyesi ülkelerden bir temsilci ve AB Komisyonu tarafından belirlenen iki temsilci yer almaktadır. Temsilciler tarafından alınan kararların yürütülmesinden sorumlu beş kişiden oluşan bir yürütme kurulu yer almaktadır. Temsilciler sayesinde AB ülkeleri ve ENISA arasındaki iletişim

kolaylaşmaktadır. ENISA'nın gelişimine yardımcı olmak üzere kurulan "Paydaş Siber Güvenlik Sertifikasyon Grubu" ENISA'ya tavsiyelerde bulunabilmektedir ([http-7](http://7)).

4.4.2. Avrupa Birliği siber dayanıklılık yasası (Cyber resilience act)

Tüketiciler için daha güvenli bir ortamın oluşması ve güvenilir cihaz ve yazılımların kullanılmasının sağlanması için Avrupa Komisyonu adını "Siber Dayanıklılık Yasası" verdiği yasa teklifini getirmiştir. Bu yasaya göre tüketicilerin kullandığı yazılım ve cihazların daha güvenli hale getirilmesi sağlanacak ve ürünleri piyasaya sürenlerden ürünlerdeki güvenlik açıklarının giderilmesi beklenmektedir. Ürünleri piyasaya sürenler sunduğu ürünlerde açık tespit ederse AB siber güvenlik birimlerine bildirmesi gerekecektir. Kurum ürünün piyasadan çekilmesine karar verebilme hakkına sahiptir. Eğer üründe güvenlik açığı bulunduğu halde bu açığı bildirmeyen şirketler bulunursa, bu şirketler 15 milyon avro veya küresel cirolarının %2,5'u kadar para cezasına çarptırılacaktır (Anadolu Ajansı, 15.09.2022).

Siber Dayanıklılık Yasası, kamuoyu incelemesi ve danışması sonucunda ortaya çıkmıştır. İç pazardaki devamlılığın sağlanabilmesi için iki temel amaç ve dört özel hedef içermektedir. İki temel amaç; 1) Siber güvenliğin en üst seviyede sağlandığı yeni akıllı cihaz ve yazılımlar üretebilmek 2) Kullanıcıların bu ürünleri seçerken siber güvenlik alanında dayanıklı olup olmadığını irdelemelerini sağlamak. Dört özel amaç; 1) Yazılım oluşturucuları için siber güvenlik kurallarına uymalarını sağlayacak bir siber güvenlik çerçevesi yaratmak 2) Dijital ürünlerin üretiminde rol alan üreticilerin ürünlerin siber güvenliğinin sürekliliğini sağlamak 3) Dijital ürünlerde şeffaflık olması açısından güvenlik bilgilerinin açıkça belirtilmesi 4) Hem kurumların hem de kişilerin dijital ürünleri rahatça ve güvende kullanmalarını sağlamak.

Siber güvenliği artırmak için dijital cihazların düzenlenmesi gerekliliği kabul edilmesine rağmen, uzmanlar yasanın hemen onay sürecine giremeyeceğini onay sürecinden geçmesi gerektiğini belirtmektedir. Diğer bir durum ise yasa geçtikten sonra yasanın ürünleri uygulanma sürecinin iki yıl süreceği öngörülmesidir. Piyasada varlığı süren ürünlerde herhangi bir değişiklik yapılmaması durumunda bu ürünler

düzenlemenin dışında kalacaktır. Bu sebeplerden dolayı Siber Dayanıklılık Yasası'nın 2026 yılına kadar yürürlüğe girmesi mümkün gözükmemektedir (http-8).

4.4.3. Avrupa Birliği siber güvenlik stratejisi (Cyber security strategy)

Avrupa Birliği, artan siber saldırılara karşı AB Komisyonu ve Yüksek Temsilcisinin kararı ile birlikte AB Siber Güvenlik Stratejisini tanıttı. Pandeminin gelişile beraber toplumda dijitalle olan yönelim siber alanda tehditlerin fazlalaşmasına ve siber alana yapılan saldırıların artmasına sebep olmuştur. Sunulan bu stratejide AB, siber alanda sahip olduğu tüm araçlarını nasıl seferber edeceğini belirtmiştir. Strateji, sağlık, enerji ve ulaşım alanındaki nesnelerin güvenli olabilmesi amacını taşımaktadır. Siber saldırılar gerçekleştiği zaman Ortak Siber Birim'in yapılan bu saldırılara nasıl karşılık verebileceği stratejinin konusunu oluşturmaktadır (http-9).

Pandemi döneminde Avrupa'da artan sağlık, ulaşım ve finasta kritik altyapılara olan siber saldırılarda 2019 yılında 450 saldırı kaydedilmiştir. Ayrıca, 2015 yılında Alman parlamentosuna yapılan siber saldırı, Avrupa'da siber saldırılar üzerine yeni düzenlemelere ihtiyaç duyulmasının gerekli olduğunu göstermiştir. Aralık 2020 yılında yapılan bu güvenlik stratejisi sayesinde herhangi bir siber saldırı olduğu zaman bu saldırılara karşılık verecek kolluk kuvvetlerinin kurulacak olan Ortak Siber Birim sayesinde güçlendirilmesi amaçlanmıştır (Bendiek and Kettemann, 2021, s.2-4).

4.4.4. Ağ ve bilgi sistemleri direktifi (NIS directive)

AB'nin 2016 yılında yayımlanan siber güvenlik ile ilgili ilk yasası olan bu direktif, AB üyeleri arasında ortak bir siber güvenlik çerçevesi oluşturmuştur. AB'de sosyoekonomik refah için gerekli olan hizmetlerdeki ağ ve bilgi sistemlerinin güvenliğinin sağlanması için NIS Direktifi bir sözlük olarak görülebilmektedir. Direktif hizmetlerin daha korunaklı olabilmesi ve güvenliğin en iyi şekilde gerçekleştirilebilmesini sağlayan kural ve yönergeleri içinde bulundurmaktadır (Ducuing, 2021, s.2).

NIS Direktifi, Avrupa Birlięi içinde siber güvenlięin artırılmasının saęlanması için oluřturulmuř bir mevzuattır. 2016 yılında yrrlęe giren NIS1 Direktifi 2023 yılında NIS2 Direktifi olarak yenilenmiřtir. Direktif sayesinde kamu ve zel teřebbslerin siber gvenliklerinin artırılması ve herhangi bir saldırı olduęunda mdahale edebilme yeteneklerinin artırılması beklenmektedir. Direktifin amaları e ayrılmaktadır; 1) AB yesi devletlerin siber saldırılar ile ilgili altyapılarını hazırlamaları 2) AB yesi devletler arasında iř birlięinin geliřtirilmesi ve devletler arasında grř alıřveriřinin yapılması 3) Kamu ve toplumun yařamının devamını ettirebilmesi iin gerekli olan alanlarda siber gvenlik kltrnn oluřturulabilmesi (http-10).

4.5. Uluslararası İnsancıl Hukuk ve Siber Saldırıları

Uluslararası insancıl hukuk konusu gnmzn en nemli konularından birisidir. nk insancıl hukuk savař ve benzeri durumlarda kimsenin ięnemesine izin verilmeyen ve savunulması gereken hakları ele almaktadır. İnsan haklarının savunulması konusu insancıl hukukun oluřmasına sebebiyet vermiřtir. İnsan hakları konusunda uluslararası szleřmeler ve protokoller bulunur. Szleřme ve protokollere uyulmadıęı durumlarda Birleřmiř Milletler devreye girmekte ve insancıl hukukun uygulanması zerine adımlar atmaktadır. Birleřmiř Milletler İnsan Hakları Szleřmesi, La Haye ve Cenevre Szleřmeleri insancıl hukukun en nemli kaynaklarındandır. BM bu szleřmeler sayesinde insan haklarını koruma altına almıřtır (Trkay, 2013, s.1195-1197).

Uluslararası silahlı atıřmalar, savařa varan ve varmayan silahlı atıřmalar olmak zere ikiye ayrılmaktadır. 1949 Cenevre Szleřmesi'nin 2.maddesinde bu iki atıřma trne insancıl hukukun uygulanabileceęi sylenmektedir. Tallinn Manual 1.0'ın 20.maddesine gre siber saldırıların silahlı atıřma hukukuna tabi olabileceęi belirtilmiřtir (Yıldız ve Bier,2020, s.215-255).

İnsancıl hukukun siber alana uygulanabilmesi iin yapılan siber saldırının silahlı saldırı nitelięi tařıması gereklidir. Siber saldırılar kinetik kuvvet uyguladıęı durumda, bu saldırılar silahlı bir saldırı olarak adlandırılır. Siber saldırılar her zaman bir şeyin

tamamıyla yok olmasına veya yıkılmasına doğrudan sebebiyet vermeyebilir. Dolaylı olarak yapılan siber saldırılarda, yapılan siber saldırı yapıldığı yeri etkilemez fakat o yeri kullananları etkileyebilir. İnsanların temel ihtiyaçlarına yapılan bir siber saldırının insanları etkilemesi buna bir örnek olarak verilebilir. İnsanların bu ihtiyaçları arasında en temel ihtiyacı olan suyun siber saldırı ile kesilmesi insan haklarının ihlali olarak ele alınması gereklidir.

2011 yılında Amerika'nın eyaletlerinden biri olan Illinois'te yapılan bir siber saldırıda uzaktan pompanın arızalanması sağlanmış ve halkın suyu kesilmiştir. Bu saldırı da Scada sistemi kullanılmış ve uzaktan pompanın açılıp kapanmasıyla beraber bozulması sağlanmıştır. Siber saldırıyı yapan kişi veya kurumu FBI araştırdığı zaman, IP adresine bakıldığında Rusya kaynaklı olduğu görülmüştür. Amerika'nın İç Güvenlik Bakanlığı bu saldırının herhangi bir tehdit oluşturmadığını ve kamu düzenini bozmadığını söylemiştir. Fakat daha sonra tesiste çalışanlardan bir kişinin Rusya'da tatile çıktığı ve uzaktan tesisle alakalı bir iş yapması gerektiği istendiği ve bu sebeple pompa arızası gerçekleştiği anlaşılmıştır. Bazen bazı saldırıların devletlere atfedilmiş olması sorunlar yaratabilirken, bu olayda herhangi bir sorun yaşanmamış olay tırmanmadan gerçeğe ulaşılmıştır. Yukarıda bahsedilen insancıl hukuk konusu için bu olay önemli bir örnektir (Richards,2014, s.2-3).

4.6. Uluslararası Ceza Mahkemesinin Siber Saldırı Kararları

Uluslararası Ceza Mahkemesi savaş suçları, soykırım suçları ve insanlığa karşı işlenen suçlara bakmakla görevlidir. Mahkemenin yetki alanının siber alanı da kapsayarak genişletilmesi, siber saldırıların UCM'nin yetki alanına giren konularda yarattığı olayların kovuşturulması açısından önemlidir. SCADA gibi sistemler ve nükleer faaliyet içeren yerler yapılan siber saldırıların dolaylı sonuçlarında can kaybı olabilmektedir. Bu şartlar da UCM'nin devreye girebilmesi ve olayın incelenmesi gerekmektedir. Fakat Roma Tüzüğü'nde yapılabilecek olan herhangi bir değişiklik için devletlerin onay vermesi gerekir. Devletler kendi çıkarlarını ve ulusal egemenliklerini etkileyeceği için bu konuda onay vermekte çekingen davranabilmektedir (Roscini, 2019, s.247-255).

Norveçli bir yargıç olan ve ayrıca East West Enstitüsü Başkanı (Siber Suçlar Yasal Çalışma Grubu) olan Stein Schjolberg, Siber Uzak için Uluslararası Ceza

Mahkemesi (ICTC) kurulmasını önerdi ve çalışma grubuyla birlikte ICTC tüzüğü oluşturdu (<https-11>) Uluslararası Ceza Mahkemesi'nin savcısı Karim Khan da siber saldırıların da geleneksel savaştaki gibi yıkıcı etkilere sahip olabileceğini, insanların üzerinde etki bırakabileceğini belirtmiştir. Roma Statüsü'nde belirtilen suçların sonuçlarıyla siber suçların yarattığı sonuçların aynı olabileceğini ve bu yüzden Roma Statüsü'ndeki suçların arasında siber suçların eklenebileceğini söylemiştir (Statement by ICC Prosecutor Karim A.A. Khan KC on conference addressing cyber-enabled crimes through the Rome Statute system, 2024).

Rusya'nın Ukrayna'ya yaptığı siber saldırıların siber suç olarak kayda geçebilmesi hakkında UC Berkeley İnsan Hakları Merkezi'ndeki araştırmacılardan biri olan Lindsay Freeman, Roma Statüsü'nün 15.maddesine dayanarak siber suçların soruşturma kapsamında değerlendirilebileceğini belirtti. Rusya'nın Ukrayna'daki elektrik şebekelerine yaptığı saldırıların sivilleri de etkilediği için saldırı suçu olarak değerlendirilebileceğini belirtti. Lindsay siber suçlar da niyet durumunun geleneksel savaşa göre kolayca belirlenebildiği iddia etmiştir. Bu iddiayı somutlaştırmak üzere geleneksel savaşta devletlerin yaptığı saldırılarda “biz bunu planlamamıştık” gibi bahaneler ile devletlerin öne çıkacağını fakat siber saldırılarda saldırı öncesi aşamanın izlenebilmesinin daha kolay olduğunu belirtmiştir “(Uluslararası Barolar Birliği, 13.11.2023).

BEŞİNCİ BÖLÜM

SİBER SALDIRILARA ÖRNEKLER

5.1. Stuxnet Saldırısı

Günümüz dünyasında toplumlar bilgisayar sistemlerine ve ağlara bağlı duruma geldiler. Bireyler veya özel kuruluşlar tarafından kişisel kazanç amacıyla siber suçlar işlenmeye başladı. Bilgisayar, veri ve sistemlerin gizliliğine, bütünlüğüne ve erişilebilirliğine karşı işlenen suçlar esasen bir iç hukuk meselesi gibi düşünülse de devletler tarafından diğer devletlere karşı yürütülen siber faaliyetler uluslararası hukuk tarafından düzenlenir hale geldi. Siber suçlarda suçlunun bulunması zor olduğu için suçun kime atfedileceği sorunu yaşanmaya başladı. Siber saldırılar hakkında hukuk alanında belirli bir yasağın olmaması siber suç işlemenin yasal izinli hale geldiğini göstermektedir. Devletler atıf sorununun olmadığı ve yasal bir mevzuatın bulunmadığı durumda suç işlemeye meyilli olacaklardır. Devletlerarası yapılan ve atıf sorununun halen tartışıldığı saldırılardan olan Stuxnet saldırısını detaylıca inceleyelim (Roscini, 2014, s.19).

Kötü niyetli yazılım başlığı altında solucanlardan bahsetmiştik. Stuxnet saldırısı yapılırken kullanılan kötü amaçlı yazılıma ise solucan olarak adlandırılmaktadır. Diğer kötü amaçlı yazılımlardan Stuxnet farkını göstermektedir. Stuxnet, 2010 yılının temmuz ayında keşfedilmiştir. O zamana kadar uzmanlar siber savaşın etkisinin sadece bebek elektronlara etki ettiğini düşünürdü. Fakat Stuxnet ile gerçek bebeklerinde bundan etkilenebileceğini, kötü amaçlı bir yazılımın bebekleri bile öldürebilme kapasitesinin olduğunu anladılar. Stuxnet yazılımının üretimindeki amaç, İran'ın uranyum tesislerine saldırmak ve uranyumun üretilmesini engellemektir. Stuxnet yazılımının oluşum sürecine etki eden devletin ABD ve İsrail olması üzerine basının bildirileri bulunmasına rağmen hala hangi devlet olduğuna dair kesin bir sonuç bulunmamaktadır (Rosenzweig, 2013, s.2-3).

Stuxnet solucanı, Beyaz Rusya'ya ait bir virüs programına İran'dan gelen şikâyet nedeniyle ortaya çıkmıştır. Daha sonra bu olayı araştıran müfettişler koda yazılı olan Stuxnet adını görmüş ve adını burdan almıştır. İstihbarat Teşkilatı CIA ve Amerika'nın Ulusal Güvenlik Teşkilatına göre Stuxnet saldırısı diğer saldırılardan farklı olarak siber alanda bir yıkım yerine gerçek bir yıkım ortaya koyan ilk saldırıdır (Lindsay,2013, s.369). Langner adında Ralph Langner'in kurduğu bir şirket Stuxnet virüsünü detayıyla inceledi. Araştırmalar sonucunda Stuxnet solucanının iki tanınmış şirketten çalma yoluyla alınmış, sertifikalar aracılığıyla güvenilirlik kazandırılmış bir solucan olarak üretildiği anlaşıldı. Bu iki şirketin Tayvan'da olduğu belirtildi. Stuxnet yazılımı öyle ince işlenmiş bir yazılımdır ki Siemens bilgisayarlarına odaklanmış, Siemens dışı bilgisayara bulaştığında kendi kendini imha eden bir yazılım olarak geliştirilmiştir (Friedman ve Dinger, 2015, s.157-163).

Stuxnet'in yaratılma amacı Siemens'in belirli bir modelini hedeflemek olmuştur fakat bu solucan kendi kendini kopyalayabilen bir yapıda olduğu için farklı bilgisayarlara da bulaşmıştır. Stuxnet solucan türü eski solucanlara göre farklılık içermektedir. Bu farklılıklardan biri solucanın boyutudur. Örneğin, daha önce yapılan saldırılardan biri olan Nimda solucanı saldırısında solucanın boyutunun 60 kilobayt ile en fazla olduğu bilinmekteydi fakat Stuxnet bir ilki başarıp 500 kilobayt bir solucan olarak oluşturulmuştur.

Stuxnet fabrikalarda PLC adı verilen fabrikanın işleyişinin kontrolünü yapan özel bilgisayarları hedef almaktadır. Bu solucan yardımıyla bilgisayarlara “.dll” adında bir dosya yüklenir ve PLC'deki asıl “.dll” dosyasını değiştirilir. Bu dosyanın yüklenmesi sayesinde fabrika içi tüm iletişimlerin izlenmesi ve gerektiğinde engellenebilmesi hakkı elde edilmektedir. Stuxnet solucanının bulaştığı ülkelerin sıralaması yapıldığında %58 ile en çok İran ve ardından Endonezya, Hindistan ve Azerbaycan gelmektedir. İran'da Siemens bilgisayarın fazla olmasının bu yüzdenin yüksek olmasında etkisi bulunmaktadır. Stuxnet'in yayılmasında usb belleklerin etkisinin olduğu düşünülmektedir. Çünkü Stuxnet usb belleklere bulaşmak üzere tasarlanmıştır. Bir usb bellek için yayılma sürecinin 21 gün olduğu belirtilmiştir. Buradan anlaşılan bu virüsün fazlaca yayılmasının engellenmesidir (Chen ve Abu-Nimeh, 2011, s.91-92).

İran Başkan Yardımcısı ve İran Atom Enerjisi Başkanı olan Ali Ekber Salehi, yapılan bu Stuxnet saldırısının sistemlerde herhangi bir yavaşlatma yaratmadığı ve uzmanların kolayca virüsün yayılmasını durdurduğunu söylemiştir. Salehi Batıların yapmak istediklerini başaramayınca bir yıl sonra konuyu açtıklarını ve bu başarısızlığı hazmedemediklerini belirtmiştir. Fakat Uluslararası Atom Enerjisi'nin verilerine göre Mayıs 2009'da İran'da çalışan santrifüj sayısının 4920 olup, Eylül 2010 da çalışan santrifüjlerin 3772'ye düştüğü belirtilmiştir (BBC, 23.11.2010). Fakat İngiliz Güvenlik Araştırma Merkezi bir rapor hazırlamış ve virüsün nükleer santralin gelişimine olanak sağladığı ortaya çıkmıştır. Raporda yapılan analizde virüsün nükleer santrale tamamıyla bulaştığının söylenemediği fakat santrifüj sayısının düştüğü belirtilmiştir. Ayrıca 2010 Şubattan beri nükleer tesisin uranyum zenginleştirmesinin %20 arttığı da belirtilmiştir. Yapılan saldırı sonrası uranyumun zenginleştirilmesinde herhangi bir sıkıntının olmaması aksine daha çok artırılması virüsün santralin işleyişinde bir sıkıntı yaratmadığını kanıtlamaktadır. CIA Başkanı olan Michael Hayden'e Obama tarafından "İran'ın uranyum zenginleştirme miktarı nedir?" diye sorulduğunda Hayden, İran'daki uranyumun nükleer faaliyet oluşturabilecek bir seviyede olmadığını söylemiştir (http-12).

Stuxnet saldırısı gerçek alanda bir yıkım yarattığı için geleneksel savaşlarda yapılan bombalı saldırıyla eş değer olduğu belirtilmektedir. Geleneksel savaşta tabi olan uluslararası hukuk kurallarının Stuxnet içinde geçerli olması bu yüzden önemlidir. Saldırının saldırı boyutunu aştığı için BM Şartı'nın 2/4'üncü maddesi açısından yargısal olarak incelenmesi gereklidir. Tallinn Manual'e göre siber saldırı boyutu aşıldığı zaman, mağdur devletin meşru müdafaa hakkına sahip olması gerekiyor. BM Şartı'nda 39.maddede ise mağdur devletin konuyu BM Güvenlik Konseyi'ne taşıması gerektiği ve Konsey'den tavsiye alabileceği belirtiliyor. Tallinn Manual'e göre 2012 yılı sonrası yapılan bütün siber faaliyetlerin (2007 Estonya Saldırısı da dahil) kamuoyuna silahlı saldırı olarak yansıtılmadığı kanaatindedir (Lucas, 2016, 58-61).

Michael Schmitt'in siber saldırıların saldırı boyutunu aşip aşmadığının incelenmesi için oluşturduğu Schmitt kriterlerine göre Stuxnet saldırısını incelemekte fayda vardır. Stuxnet saldırısı saldırı boyutunu aştığı için şiddet (severity) kriterini doğrulamaktadır. Stuxnet saldırısının planlanma ve saldırının gerçekleşme aşamasının uzun sürmesi, saldırının geç farkedilmesi aciliyet (immediacy) kriterine uymamaktadır.

Doğrudanlık (directness) kriterinin gerekliliklerine göre saldırının karşı tarafı doğrudan (ekonomik yaptırım gibi dolaylı olmadan) zarara sokması, doğrudanlık kriterinin olduğunu belirtmektedir. İstilacılık (Invasiveness) kriterine göre yapılan saldırının birden fazla devleti etkilediğini görüyoruz ve bu ise istilacılığın kriterlerine uymamaktadır. Ölçülebilirlik (measurability of effect) kriterine göre değerlendirildiğinde yapılan saldırı nedeniyle İran'ın santralindeki meydana gelen hasarın boyutu kastedilir ve hasar boyutu yüksek olduğu belirtilmiştir. Saldırıdan sonra santrifujlerin sayısında azalmanın olması saldırıların ölçülebilirliğini anlamak için önemlidir. Askeri karakter (military character) ilkesine göre bir devletin askeri kaynakları kullanılarak saldırının yapıldığına bakılmaktadır ve saldırılarda herhangi bir askeri karakter varlığından söz edilmemektedir. Varsayımsal meşruiyet (presumptive legality) açısından bakıldığında siber saldırılar ile ilgili mevzuat olmadığı için yapılan saldırılar meşrudur anlamı çıkarılmaktadır. Devlet sorumluluğu (state responsibility) kriterinde ise saldırıyı yapan tarafın belirlenebilmiş olması kastedilir. Siber saldırılarda sorumluluk kavramı biraz tartışmalı olsa da saldırının amacı ve saldırının kime yapıldığından, saldırıyı kimin yaptığının çıkarımı yapılabilir. Stuxnet'te saldırının İran'a ve İran'ın nükleer tesisine yapılmış olması İran'ın nükleer alanda büyük güç olmasını istemeyen Amerika tarafından veya İran'da hükümete muhalif kişiler tarafından yapılabilme ihtimalini ortaya çıkarıyor. Yapılan bu analiz çerçevesinde Schmitt kriterlerine göre Stuxnet saldırı boyutunu aşmış ve güç kullanımı seviyesine gelmiş bir saldırı olarak nitelendirilebilir (Foltz, 2012, 40-46).

5.2. Titan Rain

Titan Rain saldırıları Çin'in Amerika ve İngiltere üzerine yaptığı siber saldırıların geneline FBI'ın verdiği bir isimdir. Çin, ABD ve İngiltere'nin devlet kurumlarına yönelik saldırıları artırarak ABD sisteminde bozulmalar meydana getirmiştir. Özellikle bu saldırıların ortak noktası olarak savunma ve dışişleri bakanlıkları hedef alınmıştır. Yapılan bu saldırıların dört yıl boyunca sürdüğü belirtilmektedir. Saldırıların başlama tarihinin 2005 yılı olduğu söylene de 2003 yılı itibarıyla başladığı anlaşılmıştır ([http-13](http://13)).

Titan Rain karmaşık bir özelliği olmayan bir program olarak tasarlanmasına rağmen, ABD'ye etkisinin oldukça büyük olduğu belirtilmektedir. Genelde saldırılar

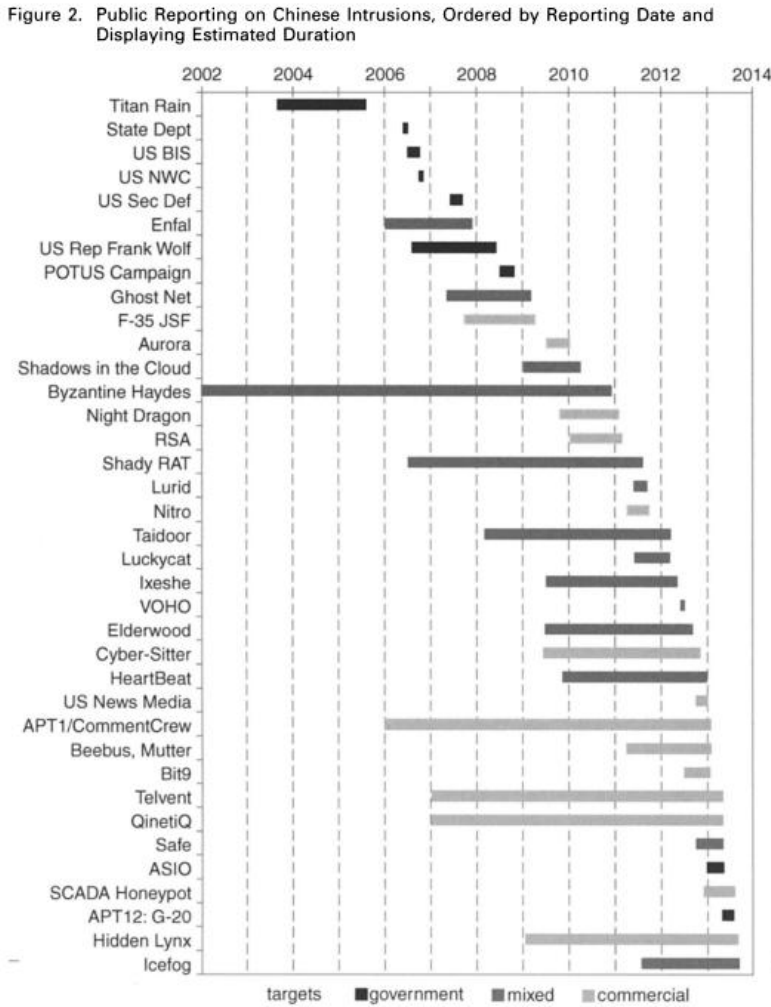
ABD'nin her eyaletindeki ordu ve savunma ile ilgili kurumlarına yapılmıştır. California için Naval Ocean System Center, Alabama için Birleşik Devletler Ordusu Uzay ve Stratejik Savunma kurumu ve Virginia için Savunma Bilgi Sistemleri Teşkilatı bunlara örnektir. Çin yapılan saldırıların Çin'e ithaf edilmesinin yanlış olduğunu belirtti (TIME, 25.08.2005).

Fakat Titan Rain'e karşından bir meşru müdafaa saldırısı gelmedi. Amerika'nın bu saldırılara karşı herhangi bir saldırı gerçekleştirmemesi Çin tarafından yapılan bu operasyonların çoğalmasına sebep oldu. Bu saldırılar üzerine Bush yönetimi, 2008 yılında "Kapsamlı Ulusal Siber Güvenlik Girişimini" başlattı. Bu girişim ABD'de siber güvenliğin sağlanmasına yönelik eğitimler ve ar-ge çalışmalarını kapsamaktadır (Hodgson, Shokh ve Balk, 2022, s.26-30).

ABD Sandia Ulusal Laboratuvarlar'ında çalışan Shawn Carpenter'a Lockheed Martin adında bir şirket tarafından sistemine sızan bir virüs hakkında araştırma yapması beklendi. Aylar sonra ABD ordusuna yapılan bir izinsiz girişin Lockheed Martin şirketine yapılan saldırıya benzer olduğu fark edildi. Ardından Carpenter yapılan bu saldırıların Çinliler tarafından gerçekleştirilen bir dizi saldırı olduğunu farketti. Yapılan bu saldırıların çok hızlı ve kompleks olarak yapıldığı anlaşıldı. Bu saldırıların izini sürebilmek için Carpenter, virüslü bir e-posta hazırlayıp bu virüse dinleme kodu tanımladı. Bu virüs sayesinde siber saldırıları yapan kişiler ne zaman hareket ederse Carpenter'a yeni bir e-posta gelecekti. Yapılan araştırmalara göre iki haftada 23.000'den fazla hareket gerçekleşti ve bu hareketlerin maili geldi. Carpenter bu çalışmalarla sınırlı kalmayıp Güney Kore'de zombi adı verilen bilgisayarlarda gizlenen ABD'nin devlet belgelerine ulaştı. Bu belgeler arasında itme sistemleri, güneş panelleri ve yakıt tanklarının çizimleri ve ABD Kara Hava ve Füze Komutanlığından çalınan gizli dosyaları içermektedir. 2007 yılı haziran ayında ise ABD Savunma Bakanlığı Pentagon'a yapılan siber saldırı ABD'ye yapılan şimdiye kadar ki saldırıların en büyüğüydü ve birçok bilgisayar bu saldırıdan etkilendi. Bu saldırıları yapan Çin Halk Kurtuluş Ordusu siber savaş konusunda uzmanlardan oluşmaktadır (Mcfadyen, 2009, s.342-349). Uzmanlar Pentagon'da bulunan bilgisayarların fazla olmasından dolayı bu saldırılara maruz kaldığını belirtti. ABD bu konuda önlem olarak Pentagon'da bulunan bilgisayar ve ağların güvenliğinin ve yönetiminin sağlanmasını ABD Stratejik Komutanlığı altında bulunan Küresel Ağ Operasyonları Müşterek Gücüne bıraktı.

Yetkililere göre yapılan saldırılar ABD'nin siber güvenlik sisteminin yeniden düzenlenmesine ve bilgisayarlarının güvenliğinin artırılmasına katkı sağladı. Stuxnet ile karşılaştırıldığında Stuxnet saldırısının uranyum zenginleştirmeyi sağladığı gibi Titan Rain saldırıları da Amerika'nın siber güvenlik sistemini geliştirmesi için bir fırsat yarattı (Washington Post, 24.08.2005).

Tablo 5.1. Çinlilerin izinsiz girişleri ile ilgili raporlama (Lindsay, 2014, s.22)



SOURCE: Jon R. Lindsay and Tai Ming Cheung, "From Exploitation to Innovation: Acquisition, Absorption, and Application," in Lindsay, Cheung, and Derek S. Reveron, eds., *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain* (New York: Oxford University Press, forthcoming), table 3.1.

Kaynak: Lindsay, J. (2014). The Impact of China on Cybersecurity. *International Security*. Vol (39). No:3, The MIT Press, s.22

Tabloda Çin'in Amerika'ya karşı 2005-2013 yılları arasında yaptığı saldırıların kamuya açıklanma tarihleri sırayla gösterilmektedir. Başlangıç saldırıları Titan Rain ile başlamış olup, en son Icefog saldırılarıyla sona ermiştir. Tabloda Byzantine Haydes'in ABD'ye en uzun süreli yapılan saldırılar arasında olduğu görülmektedir. En kısa süreli yapılan saldırılar arasında VOHO'nun olduğu belirtilmektedir (Lindsay, 2014, s.22).

Titan Rain saldırılarını Schmitt Kriterine göre inceleyelim. Saldırıları büyük boyutlu saldırı olmadığı için şiddet (severity) kriterinde değerlendirmek mümkün olmamaktadır. Yapılan bu saldırı aciliyet (immediacy) kriterinin gerekliliğini karşılayamamaktadır. Çünkü saldırılar 2003 yılında gerçekleşmiş fark edilmesi 2004 yılını bulmuştur. Saldırıların doğrudan ABD'nin kritik altyapılarını hedeflemiş olması doğrudanlık (directness) ilkesinin gerekliliklerini karşılamaktadır. Saldırıların ABD odaklı olup başka devletleri etkilememesi saldırının istilacı (invasiveness) olduğunun göstergesidir. Ölçülebilirlik (measurability) kavramını incelediğimizde saldırı ile ilgili verilere ulaşamamaktadır. Stuxnet saldırısında arıza oranından ölçülebilirlik hakkında çıkarım yapılabilir fakat Titan Rain saldırısı casusluk ile alakalı olduğu için verilerin ölçülebilirliği hakkında bilgi sahibi olunamamaktadır. Varsayımsal meşruiyet (presumptive legality) kavramı açısından incelendiğinde, saldırının bir casusluk saldırısı olduğu ve uluslararası hukukta casusluk kavramının fiziki sonuç vermediği sürece meşru olduğu belirtilmiştir. Titan Rain saldırıları, herhangi bir yasanın olmadığı durumlarda saldırıların meşru olabileceği durumlar olduğu için varsayımsal meşruiyetin olduğundan bahsedilebilir. Titan Rain saldırısı bir yandan casusluk saldırısı olduğu için ve casusluk fiziki zarar vermediği ölçüde meşru sayılabildiği için varsayımsal meşruiyetin olduğundan söz edilebilir. Askeri karakter (military character) ve devletin katılımından (state responsibility) söz edilemez çünkü yapılan saldırıların hangi devlet tarafından gerçekleştiği ve devletin askeri kaynaklarının bu saldırıda kullanılığ kullanılmadığı belli değildir. Schmitt kriteri ile Titan Rain saldırısı genel olarak incelendiğinde, saldırı boyutunu aşmayan siber saldırı olarak nitelendirilebilir. Saldırı boyutunu aşmadığı için silahlı çatışma hukuku, Tallinn Manual ve BM Şartı'na göre meşru müdafaa durumu geçersizdir (Schmitt, 2017, s.333-337).

5.3. Estonya Saldırısı

Dünyada güvenlik algısı değişim gösterdikçe, küçük devletler büyük devletlere oranla tehditlere daha çok açık olmaktadır. Küçük devletler, kendilerini güvence altına almak için koruma kalkanı isterler ve burada BM ve NATO gibi uluslararası kuruluşlar devreye girer. Fakat son zamanlarda siber savaşlar devletleri geleneksel savaşlardan daha çok etkilediği için küçük devletler siber savaşlardan en çok etkilenen devletler arasında olabilmektedir. Küçük devletler kritik altyapılarını koruma konusunda savunmasız olabilmektedir. Estonya'ya yapılan siber saldırı ise küçük devletlere yapılan siber saldırıların en önemli örneğidir.

Rusya'nın Estonya'ya bu saldırıları gerçekleştirmesine sebep olacak tarihsel arka planı incelemek burada önemli olacaktır. İkinci Dünya Savaşı'nda Sovyetlerin Estonya'yı işgaliyle Estonya'ya sayısı çok fazla Rus akını gerçekleşti. Sovyetlerin dağılmasından sonra Estonya bir karar alarak ülkede yaşayan herkese vatandaşlık vermeyi reddetti ve vatandaşlık alabilmek için yeni prosedürler uyguladı. Bu durum Rusların vatandaşlık almasını zorlaştırdı (Siber Bülten, 2024).

2007 yılında gerçekleştirilen Estonya siber saldırısı, Estonya'da Sovyetler ile ilgili İkinci Dünya Savaşı'ndan kalma "Tallinn Kurtarıcısı" anıtının kaldırılmak istenmesinin ardından meydana gelmiştir. Saldırıların 3 hafta sürdüğü belirtilmekte olup, saldırılar Rusya tarafından doğrudan mı yoksa dolaylı olarak mı desteklendiği tam olarak bilinmemektedir (Crandal ve Allan, 2015, s.351-352). Yapılan saldırıların hizmet reddi saldırıları (DDos attack) olduğu belirtilmektedir. Hizmet reddi saldırılarında saldırıya uğrayan yere birden fazla talep gönderilip, sistemin yoğunlaşması sağlanır ve sistem aşırı talep karşısında çökmeye maruz bırakılır. Estonya'nın küçük ve saldırılara açık bir sistemi olmasından dolayı saldırı kolayca gerçekleşmiştir. Saldırıları devlet kurumları, basın yayın ve banka gibi yerlerin internet sitelerine düzenlenmiştir. Kısacası ülkede günlük yaşamda kullanılan hayati birimlere erişim engellenmiştir. Estonya, IP adreslerinden Rusya bağlantılı saldırganlar olduğunu tespit etse de Rusya saldırıları yalanlamıştır. Fakat Rusya'da bir öğrencinin Estonya'ya yapılan saldırılarda yer alması üzerine Rusya, öğrenciye para cezası uygulanmıştır. Bu durum bireysel yapılan devlet destekli saldırıların da siber savaşta kullanılmasının bir örneği olabilir (Haataja, 2017, s.159-165).

Estonya saldırısından iki yıl sonra Kremlin'in bu saldırıyı örgütlemek için bir grup oluşturduğu isminin ise "Gençlik Grubu" olduğu grup üyeleri tarafından açıklandı. Grup üyeleri yaptıkları saldırının yasal olduğunu belirtti. Saldırının sebebinin Estonya'nın Estonya'daki Rus vatandaşlarına yapıldığı iddia edilen ayrımcılık olduğu belirtildi. Grup üyeleri yaptıkları Hizmet Engelleme Saldırılarını itiraf ettiler ve Estonya'nın bu saldırılara cevap verememesini altyapı eksikliği ve teknik açıdan adı altında eleştirdiler (Reuters, 13.03.2009).

Rusya bazı sitelerden Estonya'ya saldırımları için insanları teşvik etme girişiminde bulundu. Rusya halkın milliyetçilik duygularına odaklanıp, anıtın kaldırılmasının Ruslara bir hakaret olduğu düşüncesini saldırganlara dayatarak bu saldırıları gerçekleştirdi. Estonya'nın Savunma Bakanı Jaak Aaviksoo'nun talebi sebebiyle NATO'dan yardım istendi ve NATO yardıma karşılık vererek Estonya'ya birliklerini gönderdi. Estonya saldırısı sayesinde NATO siber güvenlik kavramını gündemine dahil etti. İngiliz bir raportör olan Lord Jobling'in terörizm hakkında yazılan güvenlik belgesine siber güvenlik kavramının dahil edilmesinde yardımı olmuştur. NATO'nun Bükreş Zirvesi siber güvenlik konusundaki farkındalığın artırılması üzerine önemli bir girişim olmuştur. Bildirge metninde NATO'nun siber saldırılara karşı mücadele edeceğinden bahsedilmiş fakat bu konu için gereken finansmanın nereden sağlanacağı konusunda herhangi bir cümle geçmemiştir. NATO'ya üye devletlerin birbirlerine yardım etmesi gerektiği konusuna önem verilmiştir. Bükreş Zirvesi'nin gerçekleştirilmesinden sonra siber güvenlik için iki önemli kurumun kurulmasına karar verildi. İlki NATO Siber Savunma Yönetimi Otoritesi, ikincisi ise Tallinn merkezli NATO Siber Savunma İş birliği Mükemmeliyet Merkezidir (Bıçakçı, 2012, s.215-218).

Saldırılardan 15 yıl gibi bir zaman geçtikten sonra Estonya Girişimcilik ve Enformasyon Teknolojileri Bakanı Kristjan Järvan, 2022 yılında yapılan bir açıklamada Estonya saldırısı karşısında önceki hükümetin 30 milyon euro siber güvenlik amaçlı harcadığını belirtti. Herhangi bir büyük siber saldırı karşısında artık Estonya bilgisayar ağlarının güvenliğinin zarar almayacağını söyledi ([http-14](http://14)).

Estonya saldırısı, Uluslararası Uzmanlar Grubu'na göre saldırı boyutunu aşmayan siber saldırı olarak geçmektedir. Uzmanlar, Estonya saldırısında herhangi bir devlet müdahalesinin olmadığını ve bu yüzden de silahlı çatışma hukukunun

uygulanamayacağını belirtmiştir (Lucas, 2016, s.58-76). Fakat Schmitt kriterlerine göre Estonya saldırısını detaylıca incelemekte fayda vardır. Doğrudanlık (directness) ilkesine göre incelendiğinde, hizmet engelleme saldırılarının etkilerinin uzun vadede (dolaylı olarak) oluşacağı düşünüldüğünde doğrudanlık kriterinden bahsedilememektedir. Şiddet (severity) kriterine göre saldırının ülkenin günlük yaşantısında gerekli olacak hayati organları etkilemesi (devlet kurumları, banka, basın yayın) saldırının şiddetli olduğunun göstergesidir. Saldırıların günlük hayatı etkilemesi saldırının erken ortaya çıkmasına yol açmış ve aciliyet (immediacy) ilkesinin gerekliliklerini karşılamıştır. İstilacılık (invasiveness) kriterine göre bakıldığında saldırının sadece Estonya'ya yapılması başka ülkelere sıçramaması istilacı olduğu anlamına gelmektedir. Ölçülebilirlik (measurability) kriterine göre incelendiğinde net veriler elde edilemez fakat devletin organlarındaki iş akışının yavaşladığını belirtebiliriz. Askeri karakter (military character) ve devlet katılımı (state involvement) açısından bakıldığında Rusya'nın "Gençlik Grubu" oluşturup bu saldırıları düzenlediğinden dolayı devlet destekli siber saldırılar olarak nitelendirildiğinin yorumu yapılabilir. Fakat bu grubun askeri olarak mı yoksa bireysel mi çalıştığının yorumu yapılamamaktadır. Varsayımsal meşruiyete (presumptive legality) göre herhangi bir kanun olmadığı durumlarda yapılan saldırılar (propaganda, psikolojik baskılar, casusluk ve ekonomik ambargo da dahil) meşrudur. Estonya saldırısı Rusya'nın yaptığı bir propaganda olarak değerlendirilebilir ve bu sebeple varsayımsal olarak meşrudur. Bütün kriterler değerlendirildiğinde Estonya saldırısının Stuxnet saldırısına nazaran şiddetinin az olduğu söylenebilir ve silahlı çatışma hukuku kapsamında değerlendirilmemektedir. Tallinn Manual de geçici olan hizmet reddi saldırılarının ve geçici olarak uygulanan ekonomik zorlamanın silahlı çatışma hukuku kapsamına girmediği de ayrıca belirtilmiştir. Silahlı çatışma hukuku içermeyen saldırıları BM Şartı'nın 2/4 maddesi açısından incelemek mümkün değildir. Buna istinaden 51.maddede belirtilen silahlı çatışmalarda gerçekleşen meşru müdafaa şartının geçersiz olduğunun yorumu yapılabilir. Saldırıyı gerçekleştiren ülkenin belirlenememesi durumunda hem silahlı çatışma hukuku hem de Tallinn Manual'in devreye giremediği görülmektedir (Schmitt, 2017, s.333-337).

5.4. Duqu Saldırısı

Duqu saldırılarının 2011 yılında ortaya çıktığı fark edilse de 2010 yılının şubat ayında saldırılar başlamıştır. Stuxnet ile benzer yönünün çok olduğu, Duqu saldırısını yapan kişilerin ve hedeflerin aynı olabileceği düşünülmektedir. Hedeflerinde İran'ında olması bu düşünceye varılmasında önemli bir etkidir. Saldırıların Microsoft Word programında bulunan True Type font açığı kullanılarak yapıldığı bilinmektedir. Fakat Duqu yazılımı Stuxnet gibi kendini çoğaltmamaktadır. Stuxnet gibi çoğalmamasından dolayı dar bir alanda etki göstermiştir (Akın ve Sağıroğlu, 2017, s.6).

Duqu'da Stuxnet'in yaptığı gibi SCADA sistemlerine yönelik çalışılmamış, onun yerine keylogging sistemi kullanılmıştır. Keylogging yolu bilgisayarların klavyelerini dinleme anlamına gelmekte ve bu yolla istihbarat elde edilmektedir. Duqu'da kullanılan diğer bir yöntem kimlik avı yöntemi olmuştur. Kişiye gönderilen bir e-postaya gizlenmiş kötü amaçlı yazılımın linke tıklanarak bilgisayara indirilmesi üzerine yapılan kimlik avı saldırıları Duqu'da kullanılmıştır (<http-15>).

Duqu saldırısının 2015 yılında 2.0 versiyonu ortaya çıkmıştır. Bu versiyon Duqu'nun eski versiyonuna göre daha gelişmiştir ve üç tane sıfır gün açığı kullanılmıştır. Bu saldırının en önemli özelliğinin bilgisayarın belleğinde kodu gizli tutma özelliği olduğu söylenmektedir. Hedef aldığı alan ise BM'nin daimî üyeleri olan devletlerin İran'ın nükleer programı üzerine beraber yaptığı faaliyetlerdir (<http-16>). İran'ın Sivil Savunma Bakanı olan Gholamreza Celali, Duqu virüsüyle mücadele etme konusunda yeni bir yazılım oluşturulduğunu ve bu yazılım sayesinde virüsün kontrol altına alındığını belirtti. Duqu saldırısının Stuxnet ile benzer yönlerinin olabileceği hakkında net bir bilgi olmasa da saldırıyı yapanların aynı olabileceği düşünülmektedir. Times'ın yaptığı habere göre ABD ve İsrail, İran'ın nükleer faaliyetini geliştirmesini önlemek üzere iş birliği yapmıştır (<http-17>).

Duqu saldırısını Schmitt kriterleri açısından inceleyelim. Şiddet (severity) kriteri Duqu saldırısında Stuxnet'e nazaran daha azdır. Çünkü Duqu saldırısında keylogging üzerinden bilgi toplayıp casusluk yapılmıştır fakat Stuxnet saldırısında fiziksel bir hasar meydana gelmiştir. Aciliyet (immediacy) kriterine göre incelendiğinde, Duqu saldırılarının 2011 yılında ortaya çıktığı belirlenmesine rağmen saldırıların 2010 yılında

başlamış olması, aciliyet kriterine uymamaktadır. Doğrudanlık (directness) ilkesine göre saldırının doğrudan zarara uğratma amaçlı yapılması doğrudanlık ilkesini karşılamaktadır. İstilacılık (invasiveness) açısından incelendiğinde Duqu saldırısında hedeflenen İran olduğu için ve başka ülkeler bu saldırıdan etkilenmediği için saldırının istilacı olduğu anlaşılabilmektedir. Ölçülebilirlik (measurability) kriterine göre saldırı incelendiğinde, Duqu saldırısında amaç casusluk olduğu için tam olarak saldırının zararlarını ölçebilmek mümkün değildir. Varsayımsal meşruiyete (presumptive legality) göre Duqu saldırıları casusluk amaçlı yapılan saldırılardandır ve uluslararası hukuka göre casusluk, fiziksel bir zarar verilene kadar meşru sayılmaktadır. Duqu saldırısında Stuxnet'teki gibi bir fiziksel saldırı olmadığı ve amacının sadece casusluk olduğu göz önünde bulundurulduğunda, yapılan saldırının meşru sayıldığı yorumu yapılabilir. Askeri karakter (military character) ve devlet katılımı (state involvement) ile ilgili net olarak bir şey söylenememektedir. Duqu saldırısı genel olarak incelendiğinde, saldırı boyutunu aşmayan siber saldırı olarak nitelendirebilir. Saldırı boyutunu aşmadığı için silahlı çatışma hukuku, Tallinn Manual ve BM Şartı'na göre meşru müdafaa durumu geçersizdir (Schmitt, 2017, s.333-337).

SONUÇ

İnsanlık tarihinin en önemli icatları arasında yer alan internet, modern zamanların en vazgeçilemez kaynakları arasında yer almaktadır. Uluslararası ilişkiler açısından bakıldığında internet, devletlerin birbirleri ile ilişki kurabilmesinin kolaylaşmasına katkı sağlamıştır. Fakat devletlerarası ilişkiler kolaylık kazansa da bazen ilişkilerin kopma noktasına gelmesine sebep olmuştur. Çünkü devletler artık geleneksel savaş yöntemlerini tercih etmeyip, siber alan üzerinden birbirleri ile savaşmaya başlamışlardır. Geleneksel savaş için oldukça fazla insan gücü gerektiğinden dolayı buna yatırım yapmak çok maliyetli olabilmektedir. Ancak siber alanda geleneksel savaşta kadar insan gücüne gerek olmadığı gibi siber alanın maliyeti oldukça azdır. Devletler siber alanın farkına vardıklarından beri hem saldırı amaçlı hem de korunma amaçlı kendi bütçelerinden ayırabilmektedir. Devletlerin siber alana ayırdıkları maliyete dayanarak “siber alanda dehşet dengesi” kavramı yaratılabilmesi bile mümkündür.

Siber savaş bu kadar revaçta iken bu savaşın kurallarını koyabilecek bir uluslararası hukuk kuralları oluşturmak önem arz etmektedir. Savaşlara nasıl müdahale edileceği, hangi çerçeve içerisinde siber saldırıların meşru olabileceği konularının dahil edilmesi gerekmektedir. Siber savaş alanında bu kuralları oluşturabilecek en önemli kaynak Tallinn Manual’dır. Uluslararası Uzmanlar Grubu tarafından hazırlanan bu metin uluslararası siber hukukun oluşabilmesi için önemli bir kaynaktır. Tallinn Manual yumuşak hukuk olarak nitelendirilse de gelecekte siber savaşların daha çok arttığı ve dehşet dengesi durumuna geldiği zamanlarda sert hukuk olarak anılabilmek ihtimali yüksek bir belgedir. Norveçli bir yargıç olan ve ayrıca East West Enstitüsü Başkanı (Siber Suçlar Yasal Çalışma Grubu) olan Stein Schjolberg, Siber Uzay için Uluslararası Ceza Mahkemesi (ICTC) kurulmasını önermiştir. Gelecekte siber saldırıların yargılanması için bu gibi bir mahkeme kurulduğunda Tallinn Manual, Uluslararası Adalet Divanı Statüsü benzeri bir hukuki dayanak olacaktır. Bu mahkemede siber saldırıların silahlı saldırı olarak nitelendirildiği saldırılar yargılanabilir ve bu saldırıların silahlı saldırı olup olmadığının kararının verilmesinde Schmitt kriterlerine başvurulabilir. Siber saldırıların yargılanması için uluslararası bir ceza mahkemesinin kurulması devletler üzerinde caydırıcılığın artmasında oldukça önemli olacaktır.

Tallinn Manual gibi uluslararası olması öngörülen bu belgenin iç hukuka dönüştürülmesi sağlandığı zaman, devletler kendi içlerinde bir siber hukuk kuralları oluşturacak ve siber suçlar ile ilgili bakanlıklar kurabileceklerdir. Devletlerin anayasalarında uluslararası antlaşmalar kanun hükmündedir veya başka bir örnek olarak uluslararası antlaşmaların kıyas yöntemine dayanarak iç hukuka transforme edildiği yazmaktadır. Tallinn Manual uluslararası bir sözleşme olduğunda, sözleşme ile iç hukuk ters düştüğü durumlarda sözleşme kanun hükmünde sayılıp problemlerin çözülmesi kolaylaşacaktır. Fakat şu zamanda Tallinn Manual'in durumu sadece siber saldırıların düzenlenmesi için gerekli olacak kuralları içeren bir yumuşak hukuka dayalı belgeden ibarettir. Tallinn Manual dışında siber hukuk kurallarının oluşmasını sağlayan uluslararası örgütlerin hazırladığı belgelerde bulunmaktadır. Avrupa Konseyi Siber Suçlar Sözleşmesi, BM Genel Kurul Kararları, Avrupa Birliği kararları, uluslararası örgütlerin oluşturduğu siber hukuk kuralları arasında yerini almaktadır. Uluslararası örgütlerin siber alan ile ilgili aldığı kararlar Tallinn Manual'i destekleyici yardımcı kaynaklar olarak sıralandırılabilir.

Devletlerin hukuki açıdan yargılanabilmeleri için siber saldırıyı yapan devletin öncelikle bulunması gereklidir fakat atıf sorunu nedeniyle siber saldırıya uğrayan devlet maruz kaldığı zararın tazminini yapamamaktadır. Bu nedenden dolayı siber saldırılar, geleneksel saldırılardan daha çok tercih edilebilir durumdadır. Atıf sorunu çözülmediği sürece yapılan saldırılar muallakta kalacaktır. Uluslararası üst otoritelerin siber saldırıların önlenmesi için gerekli olan tedbirleri alması gereklidir. Gerçekleşen saldırılar için herhangi bir geriye dönük müdahale yapılamaz fakat gerçekleşmesi muhtemelen saldırılar için önlemler alınabilir. Fakat siber saldırılar için hazırlanan kararların yumuşak hukuk niteliğinde olması devletler açısından caydırıcılık konusunda yetersiz kalmaktadır.

Yumuşak hukukun esnek yasallaştırma ile sert hukuka dönüşmesi sonucu çoğu kural uluslararası hukukta bağlayıcı nitelik kazanabilir. Siber alan ile ilgili yumuşak hukuk belgesi olup esnek yasallaştırma sebebiyle sert hukuka dönüşebilecek nitelikte olan iki belge vardır; 1) Tallinn Manual 2) Avrupa Siber Suçlar Sözleşmesidir. Bu iki belge sert hukuka dönüştüğü zaman sözleşme genel anlamda siber saldırıların yasaklanmasını sağlarken Tallinn Manual ise siber saldırıların detayına inip hangi şartlar altında hangi kuralların uygulanacağını belirten önemli bir kaynak olacaktır.

Siber saldırılarda geleneksel savařlarda olduđu gibi kuvvet kullanımı ve meřru mődafaa kavramı őne ıkmaktadır. Fakat siber saldırılarda kuvvet kullanımı ve saldırı arasında belirli bir fark vardır. Kuvvet kullanımı, siber saldırının saldırı boyutunu ařtıđı ve bőyők apta olaylara sebebiyet verdiđi durumlar olarak belirtilebilir. Geleneksel savařta devletlerin birbirlerine karřı kuvvet kullanması durumunda devletlerin meřru mődafaa hakkı vardır. Yapılan saldırıların kuvvet kullanımı sayılıp sayılmadıđını incelemek iin Michael Schmitt'in oluřturduđu sekiz kriterden faydalanabilir. Siber saldırıya maruz kalan devlet meřru mődafaa olarak hem silahlı bir karřılık hem de siber saldırı yaparak karřılık verebilmektedir. Tallinn Manual'e gőre yapılan saldırıların orantılılık, gereklilik, aciliyet (immediacy), yakınlık (imminence), kriterlerine uyma kořulu bulunmaktadır. Atıf sorunu özőldőđő zaman devletler meřru mődafaa hakkını bu kriterlere dayanarak kullanabilecektir.

KAYNAKÇA

(2024). *Statement by ICC Prosecutor Karim A.A. Khan KC on conference addressing cyber-enabled crimes through the Rome Statute system.* <https://www.icc-cpi.int/news/statement-icc-prosecutor-karim-aa-khan-kc-conference-addressing-cyber-enabled-crimes-through> Erişim Tarihi: 21.04.2024

“The 9 and 11 Commission Report” The Final Report of the National Commission on Terrorist Attacks Upon the United States, <https://9-11commission.gov/report/> (Erişim Tarihi: 18.12.2022)

Abbott, K. ve Snidal, D. (2000). Hard and Soft Law in International Governance. The University of Wisconsin Press Journal Division, Vol (54), No:3, s.421-436

Ahmed, Arif. ve Mustofa, J.(2016).Role of Soft Law in Environmental Protection. *Global Journal of Politics and Law Research*, Vol (4), No:2, s.1-14

Akande, D.ve Liefänder, T. (2013). Clarifying Necessity, Imminence, and Proportionality in the Law of Self Defence. *The American Journal of International Law*. Vol (107), No:3, s.563-568

Akın, M. ve Sağiroğlu, Ş. (2017). Gelişmiş Sürekli Tehditler. *Türkiye Bilişim Vakfı Bilgisayar Bilimleri ve Mühendisliği Dergisi*, Cilt (10), No:1, s.6.

Aliusta, C. ve Benzer, R. (2018). Avrupa Siber Suçlar Sözleşmesi ve Türkiye’nin Dahil Olma Süreci. *Uluslararası Bilgi Güvenliği Mühendisliği Dergisi*, Cilt (4), No:2, s.37-38.

Ansari, N. (2011). On the new breed of denial of service (dos) attacks in the internet. *Strategic Studies Institute*, s.279-205

Aral, B. (1999). *Uluslararası Hukukta Meşru Müdafaa Hakkı*. Ankara: Siyasal Kitabevi.

Aslay, F. (2017). Siber Saldırı Yöntemleri ve Türkiye’nin Siber Güvenlik Mevcut Durum Analizi. *International Journal of Multidisciplinary Studies and Innovative Technologies*, Volume 1, No 1, s.24-28.

Avrupa Konseyi Siber Suçlar Sözleşmesi, 2001

Bailliet, C. (2012). *Non-State Actors, Soft Law and Protective Regimes*. United Kingdom: Cambridge University Press

Bendiek, A. ve Kettemann, C. (2021). Revisiting the EU Cybersecurity Strategy: A Call For EU Cyber Security Diplomacy, *SWP Comment*, No:16, s.2-4

Bıçakcı, S. (2012). Yeni Savaş ve Siber Güvenlik Arasında NATO'nun Yeniden Doğuşu. *Uluslararası İlişkiler Dergisi*, Cilt (9), No:34, s.215-218.

Biçer S. ve Yıldız, A. (2020). *Yeni dünya ekonomi ve güvenlik mimarisi*. İstanbul: TASAM YAYINLARI

BM Genel Kurul Kararı, A/RES/55/63, https://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_55_63.pdf (Erişim Tarihi:15.03.2023)

BM Genel Kurul Kararı, A/RES/57/239, https://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_57_239.pdf Erişim Tarihi: 04.02.23

BM Genel Kurul Kararı, A/RES/58/199, https://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_58_199.pdf Erişim Tarihi: 04.02.23

BM Genel Kurul Kararı, A/RES/73/27, <https://undocs.org/Home/Mobile?FinalSymbol=A%2FRES%2F73%2F27&Language=E&DeviceType=Desktop&LangRequested=False> Erişim Tarihi:13.09.2023

BM Genel Kurul Kararı, A/RES/74/247, <https://undocs.org/Home/Mobile?FinalSymbol=A%2FRes%2F74%2F247&Language=E&DeviceType=Desktop&LangRequested=False> Erişim Tarihi: 16.03.2023

Bossetta, M. (2018). The Weaponization of Social Media. *Journal Of International Affairs*, Vol 71, No 1.5, s.97-106.

Boyle, A. (2012). *Moving Towards Tallinn: Drafting the Shape of Cyber Warfare*. America: American Security Project.

- Bozkurt, E. (2003). *Birleşmiş Milletler Sisteminde Kuvvet Kullanımı*. (1.Baskı). Ankara: Nobel Yayınları.
- Bunn, E. (2003). Preemptive Action: When, How, and to What Effect. *Institute for National Strategic Studies National Defense University*. No:200, s.3
- Calvert, P. (1983). Sovereignty and the Falkland Crisis. *International Affairs*, Vol 59, No.3, s.405-413.
- Canbek, G. and Sağiroğlu, Ş. (2007). Kötücül ve Casus Yazılımlar: Kapsamlı Bir Araştırma. *Gazi Üniversitesi Müh.Mim.Fak. Dergisi*, Cilt 22, No 1, s.125.
- Chen, T. ve Abu Nimeh, S. (2011). Lessons From Stuxnet. *IEEE Computer Society*, April 2011, s.91-92.
- Cifci, H. (2013). *Her Yönüyle Siber Savaş*. Ankara: Tübitak Yayınları.
- Clough, J. (2014). A World of Difference: The Budapest Convention on Cybercrime and the Challenges of Harmonisation. *Monash University Faculty of Law Legal Studies*. Vol 40, No:3, s.699-707
- Council on Foreign Relations. (2022). *Confronting Reality in Cyberspace*. United States of America: FSC Publishing
- Crandal, M. ve Allan, C. (2015). Small States and Big Ideas: Estonia's Battle for Cybersecurity Norms. *Contemporary Security Policy*, Volume (36), No:2, s.351-352.
- Değdaş, U. (2017). Uluslararası Hukukta Önleyici Meşru Müdafaa Hakkı. *Anadolu Üniversitesi Hukuk Fakültesi Dergisi*. Cilt 4, Sayı 6, s.32-35
- Deibert, R., Rohozinski, R.ve Nishihata, M. (2012). Cyclones in cyberspace: Information shaping and denial in the 2008 Russia–Georgia war, February 2012, Vol 43, No 1, s.7-10
- Dönmez, S. (2017). Kuvvet Kullanma Kapsamında Ön Alıcı ve Önleyici Saldırı Kavramları. *Balkan and Near Eastern Journal of Social Sciences*, 3 (3) , s.8-15.

Ducuing, C. (2021). Understanding the rule of prevalence in the NIS Directive: C-ITS as a case study, *Computer Law&Security Review*, Volume 40, April 2021, s.4

Dündar, H. (2018). Yeni Hegemonya Anlayışı Çerçevesinde Bush Doktrini Üzerine Bir İnceleme. *Elektronik Siyaset Bilimi Araştırmaları Dergisi*, Cilt (9), Sayı:2, s.53-55

Eaton, Thomas. (2021). Self-defense to cyber force: combatting the notion of ‘scale and effect. *American University International Law Review*, Volume 36, Issue 4, s.716-717

Eldem, T. (2021). Birleşmiş Milletler Sistemi ve Küresel Siberalan Güvenliği Regülasyonu. *Marmara Üniversitesi Siyasal Bilimler Dergisi*, Cilt 9, Sayı 1, s.17,45

Eliantonio, M., Aho, E. Ve Stefan, O. (2021). *EU Soft Law in the Member States*. Ireland: Hart Publishing

Elshtain, J. (1992). *Just War Theory*. New York University Press

Erkul, S. (2018). Askeri Güvenlik Çalışmalarına Dönüş: Önleyici Savaş. *Süleyman Demirel Üniversitesi İktisadi ve İdari Bilimler Fakültesi*, Vol 23, No 2, s. 643-654.

European Parliament. (2023). *The role of cyber in the Russian war against Ukraine: Its impact and the consequences for the future of armed conflict*. Brussel: European Union

Filipovic, M. ve Buncic, S. (2015). Global Economic Governance: A New Regime through Soft Law? *Uluslararası İlişkiler Dergisi*, Vol (11), No: 44, s.103-114

Fitzmaurice, A. (2007). The Genealogy of Terra Nullius. *Australian Historical Studies*, Vol 129, s.1-15

Foltz, A. (2012). Stuxnet, Schmitt Analysis, and the Cyber “Use-of-Force” Debate. *Joint Force Quarterly*. Issue 67, 4th Quarter. s.40-46

Freedman, L. (1982). The War of the Falkland Islands. *Foreign Affairs*, Vol 61, No 1, s.196-210.

Friedman, A. ve Singer, P. (2015). *Siber Güvenlik ve Siber Savaş*. Ankara: Buzdağı Yayınevi.

Gardam, J. (2004). *Necessity, Proportionality and the Use of Force by States*. New York: Cambridge University Press.

George, J. (2009). *The Politics of Ethnic Separatism in Russia and Georgia*. New York: Palgrave Macmillan

Ginsburg, T. (2017). Introduction to Symposium on Sovereignty, Cyberspace, and Tallinn Manual 2.0, Tallinn Manual Symposium, https://www.jstor.org/stable/pdf/27003730.pdf?refreqid=excelsior%3Aacccec7e94102e8dd95ef8f420d47aea&ab_segments=&origin=&acceptTC=1. (Erişim Tarihi: 03.02.23)

Glanville, L. (2012) "The Responsibility to Protect Beyond Borders," *Human Rights Law Review*, Vol 12, No:1, s. 9-10.

Goldmann, M. (2012). We Need to Cut Off the Head of the King: Past, Present, and Future Approaches to International Soft Law, *Leiden Journal of International Law*, Volume (25), Issue:2, s.335-339

Graham, B. (2005) Hackers Attack Via Chinese Web Sites, *Washington Post*, <https://www.washingtonpost.com/archive/politics/2005/08/25/hackers-attack-via-chinese-web-sites/03559eb7-4e56-40bf-b406-8198bd1e1131/> Erişim Tarihi: 25.04.2023

Haataja, S. (2017). The 2007 Cyber Attacks Against Estonia and International Law on the Use of Force: An Informational Approach. *Law, Innovation and Technology*, Vol (9), No:2, s.159-165.

Handl, G., Reisman, M., Simma, B., Dupuy, P. ve Chinkin, C. (1988). A Hard Look at Soft Law, *Amerikan Society of International Law*, Vol (82), s.371-393

Hathaway, O., Crootof, R., Levitz, P., Nix, H., Perdue, W. ve Spiegel, J. (2012). The Law of Cyber Attack. *California Law Review*, August 2012, Vol. 100, s.838-841

Heintze, H. ve Thielbörger P. (2016). *From Cold War to Cyber War: The Evolution of the International Law of Peace and Armed Conflict Over the Last Year 25 Years*. Switzerland: Springer International Publishing.

Hilpold, P. (2004). *The Responsibility to Protect: A New Paradigm of International Law*. USA: Hotei Publishing.

Hodgson, Q., Shokh, Yuliya. ve Balk, Jonathan.(2022). *Many Hand In the Cookie Jar*. California: RAND Corporation.

Jablonski, M. ve Powers, Shawn. (2015). *The Real Cyber War*. USA: University of Illinois Press.

Kadioğlu, C. (2022). Siber Uzayda Kuvvet Kullanma Yasağı ve Yasağın İstisnalarının Geçerliliğinin Tallinn Rehberi Kapsamında Değerlendirilmesi. *The Turkish Yearbook of International Relations, Volume 53* (2022), s. 21 – 40

Kale, Dündar. (2021). “Yalanlarla Başlayan Operasyon: ABD’nin Irak’ı İşgali” <https://www.indyturk.com/node/332831/20-mart-yalanlarla-ba%C5%9Flayan-operasyon-abdnin-irak-i%C5%9Fgali>, *Independent Türkçe*, (Erişim tarihi:18.12.2022)

Kara, İ. (2021). The Spy Next Door: A Digital Computer Analysis Approach for Backdoor Trojan Attack. *European Journal of Science and Technology*, Volume 24, s.125.

Karaalp, Haydar. (2022). ABD'nin 19 yıl önce Irak'a 'demokrasi' vaadiyle başlattığı işgalin getirdiği kaos sürüyor. *Anadolu Ajansı*, <https://www.aa.com.tr/tr/dunya/abdnin-19-yil-once-iraka-demokrasi-vaadiyle-baslattigi-iskalin-getirdigi-kaos-suruyor/2540550> (Erişim Tarihi:19.12.2023)

Kaştan, Y. (2007). "Orta Doğu'da Arap- İsrail Mücadeleleri ve Türkiye," 38.*ICANAS*, Ankara, Turkey, s.1797-1817

Keskin, F. (1998). *Uluslararası Hukukta Kuvvet Kullanma: Savaş Karışma ve Birleşmiş Milletler*. Ankara: Mülkiyeliler Birliği Vakfı.

Lango, J. (2014). *The Ethics of Armed Conflict: A Cosmopolitan Just War Theory*. Edinburg University Press

Leo, P., Işık, Ö. And Muhly, F. (2022). The Ransomware Dilemma. *MIT Sloan Management Review*, Vol 63, No 4, s.1-4.

- Lesaffer, R. (2011). *Kellogg-Briand Pact*. In R. Wolfrum (Ed.), *Max Planck Encyclopedie of Public International Law* Oxford University Press.
- Lindsay, J. (2013). Stuxnet and The Limits of Cyber Warfare. *Security Studies*, Volume (22), No:3, s.369
- Lindsay, J. (2014). The Impact of China on Cybersecurity. *International Security*, Vol (39). No:3, The MIT Press, s.22.
- Liu, I. (2017). The Due Diligence Doctrine Under Tallinn Manual. *Computer Law&Security Review*, Volume 33, Issue 3, s.390-391.
- Lotrionte, C. (2018). Reconsidering the Consequences for State-Sponsored Hostile Cyber Operations Under International Law, *The Cyber Defense Review*, Vol 3, No:2, s.76-78
- Lowe, C. (2009). Kremlin loyalist says launched Estonia cyber-attack, *Reuters*, <https://www.reuters.com/article/idUSTRE52B4D8/> (Erişim Tarihi:21.01.2024)
- Luban, D. (2004). Preventive War. *Philosophy&Public Affairs*. Vol 32, No:3 s.207-209
- Lucas, G. (2016). *The Tallinn Manual: International Law in the Aftermath of Estonia*. Oxford University Press
- Lutkevich, B. (2023). What is backdoor, *Tech Target*, <https://l24.im/UV8N/>, (Erişim Tarihi:07.06.2024)
- Lynch, J. (2005). Identity theft in Cyberspace: Crime Control Methods and Their Effectiveness in Combating Phishing Attacks. *Annual Review of Law and Technology*, Vol 20, No 1, s.259-263.
- Martirosyan, A. (2023). Time for an International Cyber Court? Russian International Affairs Council, <https://russiancouncil.ru/en/analytics-and-comments/analytics/time-for-an-international-cyber-court/>, (Erişim Tarihi: 07.06.2024)
- Mcfadyen, R. (2009). Protecting the Nation's Cyber Infrastructure: Is The Department of Homeland Security Our Nation's Savior or the Albatross Around our Neck, *Journal of Law and Policy For the Information Society*, Vol (5), No:2, s.342-349

McGhee, J. (2013). Cyber Redux The Schmitt Analysis, Tallinn Manual and US Cyber Policy. *Journal of Law&Cyber Warfare*, Vol (2), No:1, s.70-73.

McGhee, J. (2014). Hack, Attack or Whack; The Politics of Imprecision in Cyber Law. *Journal of Law & Cyber Warfare*, Vol. 4, No. 1, s. 30

Miller, D. *The War Against Iraq*, The Lucent Terrorism Library, 2003, Lucent Terrorism Library.

Milletler Cemiyeti. (1935). *Covenant of the League of Nations*.

Min, Z. (2015). Legal governance to prevent cyber attacks from the perspective of national security, *Communist Party of China News Network*, <http://theory.people.com.cn/n/2015/0901/c386965-27537572.html>, (Eriřim Tarihi: 07.06.2024)

Murray. W. (2017). Preemptive Strike Or Preventive War? *Hoover Institution*, <https://www.hoover.org/research/preemptive-strike-or-preventive-war>, (Eriřim Tarihi: 07.06.2024)

Nato Cooperative Cyber Defence Centre of Excellence. (2020). *Data as a Weapon: Refined Cyber Capabilities Under Weapon Reviews and International Human Rights Law*. Estonya

Nezgitli, S. ve Benzer, R. (2020). Avrupa Birlięi Siber Gvenlik Kanunu, *Biliřim Sistemleri ve Yntem Arařtırmaları Dergisi*, Cilt (2), No:1, s.11

Nitiynandan, S. and Kamalakkannan, S. (2022). Detection and Prevention of Man in the Middle Attack in İOT Network Using Regression Modeling. *Advances in Engineering Software*, Volume 169, s.1-3.

OECD. (2009). *Computer Viruses and Other Malicious Software*. Paris.

Oęurlu, E. (2023). International Law in Cyberspace: An Evaluation of the Tallinn Manuals. *Annales de la Facult de Droit d'Istanbul*, s.332-341

ztrk, A. (2009). Rusya-Grcistan Krizi: Yerel Bir atıřma, Kresel Yansımalar.*Uluslararası Stratejik Arařtırmalar Kurumu*, Cilt (4), Sayı (7), s.1-12

Pazarcı, H. (2016). *Uluslararası Hukuk*. Ankara: Turhan Kitabevi.

Reddy, Micah. (2023). Ukraine war: Did Putin learn from Bush's Iraq horrors? *Al Jazeera*, <https://www.aljazeera.com/features/2023/5/1/ukraine-war-did-putin-learn-from-bushs-iraq-horrors>

Redford, M. (2011). US and EU Legislation on Cybercrime, European Intelligence and Security Informatics Conference'da sunulan bildiri. <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6061188> (Erişim Tarihi:27.03.2023)

Richards, J. (2014). *Cyber- War: The Anatomy of the Global Security Threat*. New York: Palgrave Macmillan.

Robinson, M., Jones, K. and Janicke, H. (2015). Cyber Warfare: Issues and Challenges. *Computer & Security*, Vol 49. s.70-94.

Roscini, M. (2014). *Cyber Operations and the Use of Force in International Law*. United Kingdom: Cambridge University Press.

Roscini, M. (2019). Gravity in the statute of the international criminal court and cyber conduct that constitutes, instigates or facilitates international crimes. *Criminal Law Forum*, Vol 30, s.247,255

Rosenzweig, P. (2011). From Worms to Cyber War, *Hoover Institution*, <https://www.hoover.org/research/worms-cyber-war>, (Erişim Tarihi: 07.06.2024)

Rosenzweig, P. (2013). *Cyber Warfare: How Conflicts in Cyberspace Are Challenging America and Changing the World*. California: Praeger Publishing.

Ruys, T. (2010). *'Armed Attack' and Article 51 of the UN Charter: Evolutions in Customary Law and Practise*. Cambridge University Press

Schmitt, M. (2013). *Tallinn Manual on The International Law Applicable to Cyberwarfare*. United Kingdom: Cambridge University Press.

Schmitt, M. (2017). *Tallinn Manual on The International Law Applicable to Cyber Operations*. United Kingdom: Cambridge University Press.

Sen, K. (2023). List of Cybersecurity Regulations in the European Union, *UpGuard*, <https://www.upguard.com/blog/cybersecurity-regulations-in-the-european-union#:~:text=New%20NIS%20Directive,-,The%20EU%20Cybersecurity%20Act,ENISA%20as%20its%20main%20core> (Eriřim Tarihi:07.06.2024)

Senden, L. (2004). *Soft Law in European Community Law*. America: Hart Publishing

Shaffer, G.ve Pollack, M. (2010). Hard vs Soft Law: Alternatives, Complements, and Antagonists in International Governance, *Minnesota Law Review*, Vol (94), s.717-721

Steele, Jonathan, (2023). Compare Iraq with Ukraine. It's clear the era of US global supremacy is. *The Guardian*, [overhttps://www.theguardian.com/commentisfree/2023/mar/20/iraq-ukraine-us-global-supremacy-washington-power-china-global-south](https://www.theguardian.com/commentisfree/2023/mar/20/iraq-ukraine-us-global-supremacy-washington-power-china-global-south) (Eriřim Tarihi 28.10.2023)

Strategic Studies Institute. (2011). On the New Breed of Denial of Service (DOS) Attacks in the Internet.

Switzer, M. ve Park, T. (2020). R2P & Cyberspace: Sovereignty as a Responsibility. International Conference on Cyber Conflict. *2020 12th International Conference on Cyber Conflict*. Estonia: CCDCOE, s.113-127

řentuna, T. (2019). Libya Askeri M¼dahalesinin Uluslararası Hukuka Uygunluęu ve Koruma Sorumluluęu Kavramı Çerçevesinde Meřruiyeti. *The Turkish Yearbook of International Relations*, Volume (50), s.215-239.

Thornburg, Nathan, (2005). Inside the Chinese Hack Attack, *TIME*, <https://content.time.com/time/nation/article/0,8599,1098371,00.html> Eriřim Tarihi: 07.02.23

Tosun, F. (2009). Uluslararası Hukukta “Kuvvet Kullanma ve Karıřma” Kavramlarının Deęiřen Anlamı. *G¼venlik Stratejileri Dergisi*, Cilt (5), Sayı:9, s.89-93

T¼rkay, ř. (2017). Siber Savař Hukuku ve Uygulanma Sorunsalı. *İstanbul Hukuk Mecmuası*, Cilt 71, Sayı 1, s.1195-1197.

Uluslararası Adalet Divanı Statüsü, <https://www.icj-cij.org/statute>, Erişim Tarihi: 05.04.23

United Nations (Mahkeme Kararı) (International Tribunal for the Prosecution of Persons Responsible for Serious Violations of International Humanitarian Law Committed in the Territory of the Former Yugoslavia since 1991) 15 Temmuz 1999 tarihli, IT-94-1-A Case nolu karar

Ünal, K. (2022). Siber Güvenlikte Devletlerarası Saldırı, *Hukuk ve Bilişim Dergisi*, <https://www.hukukvebilisimdergisi.com/siber-guvenlikte-devletlerarasi-siber-saldiri/>, (Erişim Tarihi: 07.06.2024)

Valeriano, B. ve Maness, R. (2015). *Cyber War versus Cyber Realities*. New York: Oxford University Press.

Verbruggen, Y. (2023). Cybercrimes under consideration by the ICC, *Uluslararası Barolar Birliği*, <https://www.ibanet.org/cybercrimes-under-consideration-by-the-ICC> Erişim Tarihi: 30.01.2024

Wagner, H. (2002). *People At Odds Israel and The Arab World*. America: Chelsea House Publishers

Weber, V. ve Toriser, V. (2021). *Strategic Foresight and the EU Cyber Threat Landscape in 2025*. German Council on Foreign Relations

Westerman, P., Hage, J., Kirste, S. ve Machor, A. (2018). *Legal Validity and Soft Law*. Switzerland: Springer International Publishing

Williams, J. (1935). Recent Interpretations of the Briand-Kellogg Pact. *International Affairs*, Vol 14, No:3, s.346-348

Wingfield, T. Michael, J. ve Wijesekera, D. (2003). Measured Responses to Cyber Attacks Using Schmitt Analysis: A Case Study of Attack Scenarios for a Software-Intensive System. *Twenty-Seventh Annual Int. Computer Software and Applications Conference 'dan alınmış bildiri*. <https://ieeexplore.ieee.org/document/1245406> (Erişim Tarihi: 02.03.23)

Yener Y. (2015). 8. Yılında Estonya Saldırılarına Çok Boyutlu Bir Bakış, *Siber Bülten*, <https://siberbulten.com/siber-saldirilar-2/8-yilinda-estonya-saldirilarina-cok-boyutlu-bir-bakis/>, (Erişim Tarihi: 07.06.2024)

Sciacca, G. (2020). Cybersecurity in the EU: An introduction. Jean Monnet'te sunulan bildiri, <https://blogs.uned.es/digitaleconomy/wp-content/uploads/sites/253/2022/01/Cybersecurity-in-the-EU-an-introduction.pdf> (Erişim Tarihi:15.07.2024)

Bertuzzi, L. (2020). EU sets out plan for Cyber Defence Policy, *EURACTIV*, <https://www.euractiv.com/section/cybersecurity/news/eu-sets-out-plan-for-cyber-defence-policy/> (Erişim Tarihi: 17.07.2024)

Martinez, C. (2018). Game Over? Europe's Cyber Problem, *Centre For European Reform*, <https://www.cer.eu/publications/archive/policy-brief/2018/game-over-europes-cyber-problem> (Erişim Tarihi: 18.07.2024)

Jensen, E. (2017). Tallinn Manual 2.0 Highlights and Insights. *Georgetown Journal of International Law*, Vol 48, No:17-10, s.737-739

Cornell, S. ve Starr, F. (2009). *The Guns of August 2008 Russia's War in Georgia*. New York: Silk Road Studies Program Joint Center

(23.11.2010) BBC News, https://www.bbc.com/persian/iran/2010/11/101123_127_iran_nuclear_setback_stuxnet Erişim Tarihi:22.04.2023

(30.05.2018) "Cryptojacking: Kullanıcıları kripto para madencisine çeviriyor", <https://www.hurriyet.com.tr/teknoloji/cryptojacking-kullanicilari-kripto-para-madencisine-ceviriyor-40852254> Erişim Tarihi: 03.03.23

(06.09.2021) Patrick Jackson, (2021, Eylül 6). 11 Eylül Saldırıları 2001'de Nasıl Düzenlendi ve Ne Oldu, BBC NEWS, <https://www.bbc.com/turkce/haberler-dunya-58462900> Erişim Tarihi: 13.11.2021

(03.03.2022), Özkan, Y. (2022). Rusya'nın Ukrayna'yı işgali: Uluslararası Ceza Mahkemesi, Ukrayna'da savaş suçları işlendiği iddiaları hakkında soruşturma başlattı.

BBC News, <https://www.bbc.com/turkce/haberler-dunya-60597557> (Eriřim Tarihi:05.05.2024)

(30.04.2022) “Kuzey Kutup Bölgesinde Hangi Ülkeler Hak İddia Ediyor “
<https://www.bbc.com/turkce/haberler-dunya-61269408> (Eriřim Tarihi: 18.12.2022)

(24.02.2023) Kirby, Paul. (2023). Has Putin's war failed and what does Russia want from Ukraine? *BBC News*, <https://www.bbc.com/news/world-europe-56720589> (Eriřim Tarihi:18.12.2022)

http-1: <https://www.ncsc.gov.uk/section/about-ncsc/what-is-cyber-security> (Eriřim Tarihi:05.05.2024)

http-2: <https://purplesec.us/resources/cyber-security-statistics/#Malware> (Eriřim Tarihi:05.05.2024)

http-3: <https://ccdcoe.org/research/tallinn-manual/> (Eriřim Tarihi: 05.05.2024)

http-4: <https://ccdcoe.org/news/2020/ccdcoe-to-host-the-tallinn-manual-3-0-process/> (Eriřim Tarihi: 05.05.2024)

http-5: IHL Treaties - Hague Convention (III) on the Opening of Hostilities, 1907 ([icrc.org](http://www.icrc.org)) (Eriřim Tarihi: 07.06.2024)

https-6:
<https://www.europarl.europa.eu/news/en/headlines/security/20221103STO48002/fighting-cybercrime-new-eu-cybersecurity-laws-explained> (Eriřim Tarihi: 05.05.2024)

https-7 : <https://eur-lex.europa.eu/legal-content/EN/LSU/?uri=CELEX:32019R0881> (Eriřim Tarihi: 05.05.2024)

http-8:
[https://www.ikv.org.tr/images/files/Siber_Dayaniklilik_Yasasi_Bilgi_Notu\(1\).pdf](https://www.ikv.org.tr/images/files/Siber_Dayaniklilik_Yasasi_Bilgi_Notu(1).pdf) (Eriřim Tarihi: 05.05.2024)

http-9: <https://digital-strategy.ec.europa.eu/en/policies/nis2-directive#:~:text=The%20NIS2%20Directive%20is%20the,of%20cybersecurity%20in%20the%20EU.> (Eriřim Tarihi: 07.06.2024)

http-10:

[https://www.ikv.org.tr/images/files/Siber_Dayaniklilik_Yasasi_Bilgi_Notu\(1\).pdf](https://www.ikv.org.tr/images/files/Siber_Dayaniklilik_Yasasi_Bilgi_Notu(1).pdf)

(Erişim Tarihi: 05.05.2024)

http-11: <https://russiancouncil.ru/en/analytics-and-comments/analytics/time-for-an-international-cyber-court/> (Erişim Tarihi: 05.05.2024)

http-12: <https://l24.im/hdDMkv> (Erişim Tarihi: 05.05.2024)

http-13: <https://www.cfr.org/cyber-operations/titan-rain> (Erişim Tarihi: 05.05.2024)

http-14: <https://eadaily.com/ru/news/2022/08/27/v-otvet-na-snos-sovetskih-pamyatnikov-na-estoniyu-obrushilis-kiberataki> (Erişim Tarihi: 05.05.2024)

http-15: <https://www.radware.com/security/ddos-knowledge-center/ddospedia/duqu/> (Erişim Tarihi: 05.05.2024)

http-16: <https://securelist.com/the-mystery-of-duqu-2-0-a-sophisticated-cyberespionage-actor-returns/70504/> (Erişim Tarihi: 05.05.2024)

http-17: <https://l24.im/b83eJW> Erişim Tarihi: 05.05.2024