

HUKUK FAKÜLTESİ

INDIVIDUAL CRIMINAL LIABILITY AND RESPONSIBILITY OF THE COUNTRY FOR THE GENOCIDE
Soykırım Açısından Ülke Sorumluluğu ve Bireysel Cezai Sorumluluk
Doc. Dr. Sadmir KAROVIĆ

TÜRK TİCARET KANUNU VE VERGİ USUL KANUNU ÇERÇEVESİNDE TİCARİ KÂR MALİ KÂR AYRIMI
The Dichotomy Of Commercial Profit And Fiscal Profit In Turkish Commercial Act And Tax Procedure Act
Ahmet Emrah GEÇER

CYBER SECURITY AN INTEGRAL PART OF NATIONAL SECURITY
Milli Güvenliğin Bütünleyici Bir Parçası Olarak Siber Güvenlik
Benazir BANU

CYBER SECURITY AND HUMAN RIGHTS
Siber Güvenlik ve İnsan Hakları
Sanaz YOUSEFI

SİBER SALDIRILAR KARŞISINDA MEŞRU MÜDAFAA HAKKI
The Right of Self Defence Against Cyber Attacks
Oğuz Kaan PEHLİVAN

AVRUPA İNSAN HAKLARI SÖZLEŞMESİ VE AVRUPA KONSEYİ
(Convention for the Protection of Human Rights and Fundamental Freedoms and Council of Europe)
Mehmet ÇATLI

KAMU HUKUKU ARŞİVİ (KHUKA) 1998'DEN BERİ YAYIMLANAN VE YÖK KRİTERLERİNİ YERİNE GETİRMİŞ, ULUSAL HAKEMLİ BİR KAMU HUKUKU DERGİSİDİR.

ISSN NO: 1303-6076 **Web ISSN:** 1304-2416

KHukA
Kamu Hukuku Arşivi – 2016/1-2
Archiv des öffentlichen Rechts – 2016/1-2
L'Archive du droit Public – 2016/1-2
Archive of Public Law – 2016/1-2

Altı ayda bir yayımlanır. (Haziran ve Aralık aylarında)
Die Zeitschrift erscheint halbjährlich.
Cette revue se publie deux fois par ans.
Bi-annual.
Cilt XV, Sayı 1-2
Band XVI, Nummer 1-2
Volume XVI, Numéro: 1-2
Volume XVI, Number: 1-2

Editör **:** Dr. Öğr. Üyesi Murat TUMAY
Editör Yrd. **:** Arş. Gör. Mustafa Gökhan ERTİN
Sahibi **:** İstanbul Medeniyet Üniversitesi Hukuk Fakültesi
Sorumlu **:** Arş. Gör. Abuzer ZENGİN
Adres **:** D100 Karayolu 6/1, Kadıköy- İSTANBUL
Tel **:** 444 42 43 / Dahili: 1364
E-posta **:** khukadergisi@gmail.com

YAYIN KURULU / SCHRIFTLEITUNG / COMITÉ DE L'ÉDİTİON / ASSOCIATED EDITORS
Prof. Dr. Mustafa AVCI
Prof. Dr. Refik KORKUSUZ
Prof. Dr. Hakan HAKERİ
Prof.Dr. İlyas Doğan
Prof. Dr. Andrzej BISZTYGA
Dr. Mohd Iqbal ABDULWAHAB
Dr. Öğr. Üyesi Murat TUMAY
Dr. Öğr. Üyesi Saliha Okur GÜMRÜKÇÜOĞLU

Kamu Hukuku Arşivi (KHukA) 1998'den Beri Yayımlanan ve
YÖK Kriterlerini Yerine Getirmiş,
Ulusal Hakemli Bir Kamu Hukuku Dergisidir.

E-MAIL: kamuhukukuarsivi@gmail.com

YAYINCI / VERLAG / PUBLISHER

A D A L E T Y A Y I N E V İ
Strazburg Caddesi 10/B Sıhhiye / Ankara
Tel: (0 312) 231 17 00 – 231 17 94 / Faks: (0 312) 231 77 04
web: adaletyayinevi.com / e-mail: adalety@adaletyayinevi.com

Baskı: Ay-bay Kırtasiye İnş. Gıda Paz. ve Tic. Ltd. Şti. **Baskı Tarihi:**
Sertifika No: 33365 Tel: (0 312) 472 58 55 - Ankara Ağustos, 2018

YAYIN İLKELERİ ve AÇIKLAMALAR:

1. Dergide yayımlanması istenen çalışmalar **Murat Tümay** adına **murattumay@yahoo.com** elektronik posta adresine gönderilmelidir. Gelen çalışmalar editör ve editör yardımcılarımız tarafından bir **ön incelemeye** tabi tutulduktan sonra yayın kurulu tarafından değerlendirilerek ilgili hakem kurulu üyesine gönderilir. Çalışmanın, hakemlerin incelemesi ve düzeltmelere olanak tanınması amacıyla yayın tarihinden **en az üç ay önce** gönderilmesi tavsiye edilir. Hakem kurulu üyesine gönderilecek çıktıda yazarın adı yer almaz (Kör hakemlik usulü).

2. Yayınlanan çalışmadaki dil, üslup, görüş ve hukuki sorumluluk yazara/yazarlara aittir. Gönderilen yazıların, yazım bakımından **son denetimlerinin yapılarak** tarafımıza ulaştırıldığı ve dilbilgisi kurallarına uyulduğu ve bu hali ile basılması istendiği kabul edilir. Yayın kurulu çalışma üzerinde esasını bozmadan değişiklik yapma hakkını saklı tutar. Editör çalışmanın özüne dokunmaksızın ifade ve biçimle ilgili değişikler yapabilir.

3. Gönderilen çalışma yayınlandığı takdirde telif haklarının Editörün tasarrufunda olmak üzere derginin yayımlandığı tarihteki sahibine devredilmesine rıza gösterildiği anlamına gelir. Yazar bu çalışmasını başka bir süreli yayında yayınlamama taahhüdünde bulunmuş sayılır. Çalışmalar için telif ücreti ödenmeyecektir. Yazara, ilgili sayı basılı olarak 3 adet gönderilecektir.

4. Başka yerde yayınlanmış çalışmalar kabul edilmez.

5. Çeviri eserlerde; çeviren, eser sahibinden ya da yayın hakkına sahip kişi ya da kurumdan yazılı yayım izni almak ve bu izin belgesini istendiği zaman ibraz etmek durumundadır. Bu hususstaki her türlü sorumluluk çeviren yazara aittir.

6. Yayınlanmak üzere gönderilen çalışmalar "Office Word" (en az 2003) programında, yazı karakteri "Arial" ve 9 punto, tek aralık, dipnotları ise 8 punto ve sayfa altında gösterilerek hazırlanmalıdır.

7. Her çalışma Başlık/Title, Öz/ Abstract, anahtar kelimeler/Keywords, Giriş/Introduction, Sonuç/ Conclusion içermelidir.

8. Dergimizde "Dipnotlu Kaynak Gösterme Yöntemi (Klasik Sistem)" kullanılması tavsiye edilmektedir. Yabancı dilde yayınlanmak üzere gönderilen çalışmalarda "Metin İçi Kaynak Gösterme Yöntemi (APA Sistemi)" de kullanılabilir.

9. Dipnotta verilen literatür "Kaynakça/Yararlanılan Kaynaklar" olarak çalışmanın sonunda verilmelidir.

10. Çalışmalar ile birlikte, yazarın iletişim bilgileri (açık adresi ve telefon numaraları, elektronik posta adresi) editöre gönderilmiş olmalıdır. Ayrıca **güncel e-posta adresi ve ünvan ve çalışılan kurum bilgisi ilk dipnotta mutlaka verilmelidir.**

11. ÇALIŞMANIN BAŞLIĞI TÜRKÇE'NİN YANINDA İNGİLİZCE OLARAK DA İFADE EDİLMELİDİR.

MAKALENİN BAŞLANGICINA 150-200 KELİMELİK İNGİLİZCE ÖZET VE AYNI ÖZETİN TÜRKÇESİ; İNGİLİZCE VE TÜRKÇE ANAHTAR KELİMELER EKLENMELİDİR.

ATIF İÇİN ÖNERİLER:

Altındağ, H. Anayasa Mahkemesinin (02.04.2014 Tarihli) Twitter Kararı, KHukA, 2014; 14 (1): 1-4.

HAKERİ, Hakan, Ceza Hukuku Genel Hükümler, 17.Baskı, Ankara 2014, s.35.

INFORMATION TO CONTRIBUTERS

1. The manuscripts is send to the address of the editorial board. The received work is send to peer related reviewers after a brief check by editorial board. The manuscripts should be sent as early as there months before publication for the completion of refeires' suggestions and required corrections. The manuscripts send to refeires will not include the identities of the authors.

2. The editorial board finds itself abstained from all legal responsibilities that the ideas, style and format disclosed in the manuscript after publication.

3. Buy submitting the manuscript, the Authors is accepting that copyright of the manuscript will be trasferred to IMUHF after publication in KHukA, and will not be published in any journal.

4. The published manuscript in any journal is not accepted for consideration.

5. The submission should have an compatible CD including a copy written by Office Word 2003 or above, the body text with Arial-8. the editorial committee reserves all the right for any change in the manuscript.

Hakem / Danışma Kurulu / Beirat / Comité de Consultant / Consulting Board *

Prof.Dr. Ömer ANAYURT, Gazi Üniversitesi
Prof. Dr. Dr. h.c. Hakan HAKERİ, *İstanbul Medeniyet Üniversitesi*
Prof. Dr. Bahtiyar AKYILMAZ, *Gazi Üniversitesi*
Prof. Dr. Gül AKYILMAZ, *Gazi Üniversitesi*
Prof. Dr. Mehmet Emin ARTUK, *Medipol Üniversitesi*
Prof. Dr. Mustafa AVCI, *Selçuk Üniversitesi*
Prof. Dr. Meltem Dikmen CANİKLİOĞLU, *Dokuz Eylül Üniversitesi*
Prof. Dr. Ahmet CİHAN, *İstanbul Medeniyet Üniversitesi*
Prof. Dr. M. Emin ÇAĞIRAN, *Gazi Üniversitesi*
Prof. Dr. İlyas DOĞAN, *Gazi Üniversitesi*
Prof.Dr. Halil KALABALIK, Türkiye İnsan Hakları ve Eşitlik Kurumu
Prof. Dr. Yusuf KARAKOÇ, *Dokuz Eylül Üniversitesi*
Prof. Dr. Bernhard KEMPEN, *Köln Üniversitesi / ALMANYA*
Prof.Dr. Yüksel Metin, *Süleyman Demirel Üniversitesi*
Prof. Dr. Hayrettin ÖKÇESİZ, *Akdeniz Üniversitesi*
Prof. Dr. İzzet ÖZGENÇ, *Gazi Üniversitesi*
Prof. Dr. Bahri ÖZTÜRK, *İstanbul Kültür Üniversitesi*
Prof. Dr. Doğan SOYASLAN, *Çankaya Üniversitesi*
Prof. Dr. Makoto TADAKI, *Chuo Üniv. Tokyo/ JAPONYA*
Prof. Dr. A. Mete TUNÇOKU, *Onsekiz Mart Üniversitesi*
Prof. Dr. Feridun YENİSEY, *Bahçeşehir Üniversitesi*
Prof. Dr. Javier F. REVORIO, Universidad de Castilla- La Mancha, İspanya
Prof. Dr. Sandra THOMPSON, University of Houston, ABD
Prof. Dr. Marco VENTURA, University di Parma, İtalya
Doç. Dr. Farid SHUAIB, International Islamic University of Malaysia, Malezya
Dr. Öğr. Üyesi Gülay Arslan Öncü, *İstanbul Üniversitesi*
Dr. Öğr. Üyesi Saliha Okur GÜMRÜKÇÜOĞLU, *İstanbul Medeniyet Üniversitesi*
Dr. Öğr. Üyesi Murat TUMAY, *İstanbul Medeniyet Üniversitesi*
Dr. Öğr. Üyesi Tülay YILDIRIM, *İstanbul Medeniyet Üniversitesi*
Dr. Pardis Moslemzadeh TEHRANİ, University of Malaya, Malezya
Dr. Sadmir KAROVİÇ

* Hakem Kurulu üyelerinin isimleri akademik unvan ve alfabetik soyadı sıralamasına göre düzenlenmiştir.

İÇİNDEKİLER

INDIVIDUAL CRIMINAL LIABILITY AND RESPONSIBILITY OF THE COUNTRY FOR THE GENOCIDE 1

Soykırım Açısından Ülke Sorumluluğu ve Bireysel Cezai Sorumluluk

Doc. Dr. Sadmir KAROVIĆ

TÜRK TİCARET KANUNU VE VERGİ USUL KANUNU ÇERÇEVESİNDE TİCARİ KÂR MALİ KÂR AYRIMI 13

The Dichotomy Of Commercial Profit And Fiscal Profit In Turkish Commercial Act And Tax Procedure Act

Ahmet Emrah GEÇER

CYBER SECURİTY AN INTEGRAL PART OF NATİONAL SECURİTY..... 29

Milli Güvenliğin Bütünleyici Bir Parçası Olarak Siber Güvenlik

Benazir BANU

CYBER SECURITY AND HUMAN RIGHTS 41

Siber Güvenlik ve İnsan Hakları

Sanaz YOUSEFI

SİBER SALDIRILAR KARŞISINDA MEŞRU MÜDAFAA HAKKI 55

The Right of Self Defence Against Cyber Attacks

Oğuz Kaan PEHLİVAN

AVRUPA İNSAN HAKLARI SÖZLEŞMESİ VE AVRUPA KONSEYİ 67

(Convention for the Protection of Human Rights and Fundamental Freedoms and Council of Europe)

Mehmet ÇATLI

SİBER SALDIRILAR KARŞISINDA MEŞRU MÜDAFAA HAKKI

(The Right of Self Defence Against Cyber Attacks)

Oğuz Kaan PEHLİVAN

ÖZET

Bu çalışmada, siber saldırıların meşru müdafaa hakkını tetikleyecek nitelikte olup olmadığı tartışılacaktır. Siber saldırılar, öncelikle, değerli fikri mülkiyet ürünlerinin, şirket sırlarının ve planlarının, ekonomik açıdan değer ifade eden verilerin kaybedilmesini sonucu doğurduğu gibi hedef alınan sistemin güvenliğini ihlal ettiği için yeniden güvenliğin sağlanması için yapılacak harcamalar gibi yan zararlara da sebebiyet vermektedir. Ancak bundan daha önemlisi, siber saldırılar sonuçları itibariyle ağır ve telafi edilemez felaketler doğurabilme potansiyeline sahiptir. Uçakların yazılımlarını ve havalimanlarını hedef alan bir saldırı ölümlere yol açacak felaketler doğurabilir.

Bu bilgiler ışığında bu çalışma şu sorulara cevap aramaktadır. Böylesi senaryolarda siber saldırılara nasıl karşılık verilecektir? Yerleşik normlar siber saldırılara etkili cevap vermek için yeterli midir? Yoksa devletler self-help kurumu çerçevesinde herkesin kendi hakkını aradığı bir sistemi mi tercih edecekler? Şimdiden söylemek gerekirse, devletler yerleşik normların sınırlarını genişletmekte ve yeni yöntemler aramaktadır.

I. Giriş

Çeşitli motivasyonlarla geniş bir yelpazedeki hedeflere karşı gerçekleştirilen siber saldırılar bugün pek çok ülkenin kamusal ve özel bilgisayar ağlarına zarar veriyor. Bu çalışmada siber saldırıların etkisi ve boyutları ile saldırı sonrasında meşru müdafaa hakkının kullanılabilirliği tartışılacaktır. Siber saldırı kavramı ve bu kavramın içerdiği unsurlar ile saldırı öncesinde atılması gereken adımlar etrafında dönen tartışmalara yer verilmeyecektir.

Devletler, kurumlar ve bireyler her geçen gün artan bir şekilde siber saldırı tehdidiyle karşı karşıya kalmaktadır (Pehlivan, 2013). Fırsatların ve tehditlerin iç içe yer aldığı bu yenidünyada, uluslararası sistemin en temel aktörü olan devletleri siber casusluk ve siber terörizm; kurumları ve bireyleri ise siber casusluk ve siber suçlar mağduru olarak görmekteyiz. (Pehlivan, 2014) Yapılan araştırmalar, şirketlerin devletlere ait kamusal ağlardan daha fazla hedef alındığını göstermektedir.

Siber saldırılar karşısında, mevcut hukuki kavramların uygulanabilir olup olmadığı tartışması bir yana, devletlerin ve ekonomik değeri olan dijital varlıklarını korumak için şirketlerin nasıl bir hareket alanına sahip olduğunun incelenmesi önem taşımaktadır. Zira dijital zenginliğin muhafaza edilmesi ve enerji, finans, iletişim, ulaşım, sağlık gibi kritik altyapıların korunması, koruma için alınacak önlemleri ve bu önlemlerin hukukiliğini gündeme getirmektedir.

Devletlerin, dijital alanda egemenlik sınırlarını belirleyerek birtakım tedbirlere başvurduğunu görüyoruz. Bu bağlamda, siber saldırıya maruz kalan bir devletin meş-

ru müdafaa hakkını kullanıp kullanamayacağını ele almak gerekmektedir. Öte yandan şirketler de dijital varlıklarını korumak için belirli adımlar atmaktadır. Bu yazının ilk bölümünde, devletlerin siber saldırıya maruz kalması durumunda uluslararası hukuka uygun olarak meşru müdafaa hakkını kullanıp kullanamayacağı incelenecektir. İkinci bölümde ise devletlerden daha fazla saldırıya maruz kalan şirketlerin, bir saldırı karşısında yapabilecekleri ve bu tedbirlerin hukukiliği tartışılacaktır.

II. Siber Saldırılar Karşında Devletler

a) Devletlerin Meşru Müdafaa Hakkı

Meşru müdafaa kavramının kaynağını oluşturan Birleşmiş Milletler Antlaşması'nın 51. Maddesi uyarınca "*Bu antlaşmanın hiçbir hükmü, Birleşmiş Milletler üyelerinden birinin silahlı bir saldırıya hedef olması halinde, Güvenlik Konseyi uluslararası barış ve güvenliğin korunması için gerekli önlemleri alıncaya kadar, bu üyenin doğal olan bireysel ya da müşterek meşru müdafaa hakkına halel getirmez."* (BM Kurucu Antlaşması, 1945). Bu maddeyle, meşru müdafaa hakkının sınırları çizilmektedir. Bu kavrama ancak şu iki farklı şart var olduğu durumlarda başvurulabilecektir: i) *sınır aşan nitelikli bir silahlı saldırının* var olması, ii) BM üyelerinden birinin, *bir devletin hedef olması*.

Hukuk, karşılaşılan problemlerin çözümünde uygulanması gereken bir form/kalıp belirler ve sınırlar çizer. Bu açıdan normlar yapısı itibariyle belirli bir çerçeveye sahip kavramların ya da şartların bir araya getirilmesiyle oluşturulur. Öncelikle söylemek gerekir ki, meşru müdafaa hakkı kinetik ve klasik savaşların devam ettiği bir dönemde oluşturulmuştur (Dinstein, 2005; Walker, 2014). Öyle ki, meşru müdafaanın uluslararası teamül hukukunda yer alması 1837 yılında Amerika Birleşik Devletleri (ABD) ile Birleşik Krallık arasında sivillerin öldüğü Caroline isimli geminin batırılmasıyla gerçekleşmiştir. İkinci Dünya Savaşı'ndan sonra Birleşmiş Milletler Kurucu Antlaşması'nın kabulüyle meşru müdafaa, pozitif hukukun bir parçası haline gelmiştir. Dolayısıyla bu hak, tanımında barındırdığı birtakım kavram ve şartlarla o dönemim özelliklerini yansıtan bir form/kalıp belirler, sınırlar çizer. Bu form/kalıp ve sınırlar, günümüzde siber saldırıların giderek yoğunlaştığı, bulanık savaş stratejisi olarak adlandırılan topyekûn savaşların sona erdiği, vekâlet savaşlarının arttığı, düşük yoğunluklu askerî grupların aktif olduğu, altyapılara yönelik siber saldırı ve savaşların yoğunlaştığı bir dönemde tekrar tartışmaya açılmıştır.

Bu bağlamda Birleşmiş Milletler Antlaşması'nın 51. maddesinde yer bulan meşru müdafaa kavramının kapsamı içerisine siber saldırıların dâhil edilip edilmeyeceği tartışmaya açık bir nokta olarak durmaktadır. Dolayısıyla öncelikli olarak bir siber saldırıda, bu saldırının devleti hedef alması ve sınır aşan nitelikte olması şartlarının var olup olmadığının incelenmesi gerekmektedir.

b) Silahlı Saldırı

Birleşmiş Milletler (BM) Antlaşması'nın 51. maddesinde yer alan meşru müdafaa hakkının temel unsurlarından birisi "*silahlı bir saldırının*" var olmasıdır. Silahlı saldırının varlığının tespiti, hukuka uygun verilecek olan karşılığın niteliğini ve sınırlarını belirleyecektir. Peki, bu silahlı saldırının kapsam ve sınırları nelerdir? Silahlı saldırının mutlak bir şekilde kinetik mi olması gerekmektedir? Ya da silahlı saldırı sadece belirli araçlarla gerçekleştirilince mi var olacaktır?

NATO Siber Savunma Mükemmeliyet Merkezi öncülüğünde Uluslararası Bağımsız Uzmanlar Grubu tarafından hazırlanan, bağlayıcı olmayan yumuşak hukuk olarak kabul edilen, Siber Savaşa Uygulanacak Hukuk Hakkında Tallinn Manuel, silahlı saldırı seviyesine yükselen bir siber saldırı karşısında, bireysel ya da topyekun meşru müdafaa hakkının kullanabileceğini vurgular. (Talinn Manuel, 2013, 54)

Silahlı saldırıların niteliği konusunda, Uluslararası Adalet Divanı'nın (UAD) Birleşmiş Milletler Genel Kurulu'nun isteği üzerine 1996 yılında verdiği nükleer silahlara ilişkin danışma görüşü önemli bir yer tutmaktadır (Alpkaya, 1997, 105). UAD bu kararında, BM Antlaşması 51. maddesinin sadece belirli silahlara atıf yapmadığını, saldırı araçlarına bakılmaksızın her türlü kuvvet kullanımında uygulanacağını belirtmektedir (Dinstein, 2013, 280). Bu noktada artık literatürde siber silah kavramına yer verildiğine ve devletlerin belirli hedefler için özel olarak tasarlanmış siber silahlar geliştirdiğine değinmek de faydalı olacaktır. Öte yandan milletlerarası teamülün oluşması için gerekli olan genel, tutarlı ve sürekli devlet uygulamaları da bu yorumu destekler mahiyettedir (Öktem, 2013). UAD, 1969 Kuzey Denizi Kıta Sahanlığı davasında, uluslararası bir teamülün oluşması için devlet uygulamasının gerekli ve kaçınılmaz bir şart olduğunu belirtiyor (Germany/Denmark; Germany/Netherlands, 1969). Hatta, devletler kimyasal ve biyolojik saldırıları, felaket sonuçlar doğurabileceği için meşru müdafaa hakkının kapsamı içerisinde ele almaktadır (UAD Danışma Görüşü, 1996, 245). Dolayısıyla, silahlı saldırının varlığı, sadece kullanılan silahlı araçlarla değil, bu araçların doğurabileceği sonuçlarla da yakından ilgilidir. Talinn Manuel'de de ifade edildiği üzere bir siber saldırının, silahlı saldırı olup olmadığının tespiti bu saldırının boyut ve etkisine bağlıdır.

Benzer şekilde, UAD ilk olarak, Nikaragua kararında silahlı saldırı düzeyine ulaşmış "en ağır" kuvvet kullanımı ile "daha az ağır" kuvvet kullanımı ayrımı yaparak, silahlı saldırının tespitinde boyut ve etki testini (*scale and effect test*) kullanmıştır (Nicaragua v. United States of America, 1986, 101). Petrol Platformları davasında ise, BM Antlaşması'nın 51. Maddesi kapsamında meşru müdafaa hakkının kullanılabilmesi için "*saldırının ciddi boyutlarda*" olması gerektiğini vurgulamıştır (Islamic Republic of Iran v. United States of America, 2003, 187).

Siber saldırıları incelediğimizde, bu saldırıların sonuçları ve etkileri itibariyle yıkıcı nitelikte oldukları görülmektedir. 2007 yılında Estonya'nın karşı karşıya kaldığı siber saldırı bu yaklaşımı kullanabileceğimiz en belirgin örnek olmaktadır. Dijital işgal olarak tanımlanan siber saldırılarda İkinci Dünya Savaşı'nda ölen Rus askerlerin anısına dikilen Bronz Asker Heykeli'nin olduğu yerden kaldırılması saldırıların temel sebebi olarak gösterilmektedir (Davis, 2007; Ruus, 2008). Heykelin yerinden kaldırıldığı 26 Nisan 2007 tarihinden bir gün sonra Rusya, Estonya'yı kınamış ve Talinn'de gösteriler başlamıştır. Ertesi günlerde, bazı resmi sitelerin ele geçirilmesi, küçük çaplı DDoS saldırıları ve başlangıç düzeyinde spam e-posta saldırıları düzenlenmiştir. 30 Nisan-18 Mayıs tarihleri arasında ise saldırıların yoğunluğu giderek artmış ve ulusal bilgi sistemleri, internet hizmet sağlayıcıları, finansal sisteme yönelik daha geniş katılımlı ve koordineli DDoS saldırıları gerçekleştirilmiştir. Bu saldırılar sonrasında internet bant genişliği büyük oranda saldırılar tarafından doldurulmuş ve ülkenin internet altyapısı çökme noktasına gelmiştir. Bu saldırıların en dikkat çeken yanı ise sonuçları ve etkileri gözlemlendiğinde açığa çıkmaktadır. 1.3 milyon nüfusa sahip olan Estonya'da 1 milyondan fazla dijital kimlik kartı kullanılmakta, vergi beyanlarının yüzde 80'i, bankacılık işlemlerinin yüzde 97'si internet üzerinden gerçekleştirilmektedir (Ruus, 2007; Schnurer, 2015). Ayrıca ülkedeki sağlık kayıtlarının tamamı dijital ortamda tutulmakta ve dahası ülkede kurulan her 4 şirketten 1 tanesi internet üzerinden kurulmaktadır. Tüm bunlar göz önüne alındığında Estonya'ya gerçekleştirilen siber saldırı, boyut ve etki testi bağlamında değerlendirilecek olduğunda bu saldırının sonuçlarının kinetik saldırıların neden olacağı sonuçlarla benzerlik taşıdığı görülmektedir.

Bu bilgiler ışığında, silahlı saldırının her türlü araçla gerçekleştirilebileceği ve siber saldırıların doğurabileceği felaket sonuçlar dikkate alındığında, siber saldırıların silahlı saldırı kapsamında değerlendirilmesi mümkün gözükmektedir.

c) Sınır Aşan Nitelik

BM Şartının 51. maddesi uyarınca meşru müdafaa hakkının varlığından söz edebilmek için bir diğer kavrama daha ihtiyaç vardır: "BM üyelerinden birinin, bir devletin hedef olması". Bu ifade bir yandan "bir devletin" hedef alınmasını diğer bir yandan ise saldırının "sınır aşan boyutta" olması gerektiğini belirtmektedir.

Bu açıdan, saldırının BM üyesi olan bir devletten BM üyesi olan bir devlete ya da devlet dışı bir aktörden BM üyesi olan bir devlete karşı gerçekleşmesi gerekmektedir. Siber saldırılar doğaları gereği sınır aşan niteliği sahip olmaktadır. Bu noktada dijital dünyada sınır kavramının olup olmadığı tartışılmaya açıktır. Her ne kadar dijital dünyada sınırların belirlenmesi imkansız olsa da, dijital dünya birtakım fiziksel yapılardan meydana gelmektedir. Bu fiziksel yapılar ise günümüz uluslararası düzenin temelini oluşturan "ülkesel sınırlar" içerisinde yer almaktadır. Ülkeler kendi sınırları içerisinde yer alan yapıları, kurumları, varlıkları hakimiyetleri gereği hukuk vasıtasıyla düzenleyebilir. Talinn Manuel'de de ifade edildiği gibi "*Devlet, kendi egemenlik bölgesi dahilinde, siber altyapı ve siber eylemler üzerinde kontrol yetkisini kullanabilir*." (Talinn Manuel, 2013, 15) Dolayısıyla, siber saldırıların sınır aşan nitelikte olduğuna ilişkin bir tereddüt bulunmamaktadır. Ancak diğer bir sorun olan atfedilebilirlik gündeme gelmektedir. Bir devletin sınırları içerisinde yer alan fiziksel yapılardan kaynaklanan saldırılar, ne ölçüde o devlete yada devlet organlarına atfedilebilir? (Tsagourias, 2012, 5). Talinn Manuel'e göre, bir devletin sınırları içerisinde yer alan altyapılardan kaynaklanan bir siber saldırı doğrudan bu devlete atfedilemez, ancak bu altyapı resmi nitelikteyse (örneğin, askeri bir altyapı) bu taktirde saldırının o devlet tarafından düzenlendiği karine olarak kabul edilir. Ancak bu karinenin aksini ya da temelsiz olduğu saldırının kaynaklandığı devlet ispat edebilir.

Bu bilgiler ışığında sivil ya da kamusal bilgisayar ağları silahlı saldırı seviyesinde bir siber saldırıya uğrayan devletler, *minimum, gerekli ve orantılı* şiddet içeren bir kuvvet kullanarak meşru müdafaa haklarını kullanabilir. Uluslararası Bağımsız Uzmanlar Grubu da bir siber saldırı gerçekleşmişse veya gerçekleşmesi yakın ise ya da acil bir karşılık verildiği taktirde saldırı gerçekleşecekse devletlerin gerekli ve orantılı olmak kaydıyla karşılık verebileceğini belirtiyor. (Talinn Manuel, 2013, 61-66)

III. Siber Saldırılar Karşısında Şirketler

Günümüzde devlet dışı aktörler hızla çoğalmakta ve buna paralel olarak devlet dışı aktörlerin sahip olduğu dijital varlıkları giderek büyümektedir. Dolayısıyla sınırların anlamını yitirdiği dijital alanda devletlerin yanı sıra devlet dışı aktörlerin siber saldırı karşısında neler yapabileceğini tartışmak gerekmektedir.

a) Devlet Dışı Aktörler

Uluslararası kişiliğe yani "uluslararası hukuktan kaynaklanan haklara ve yükümlülüklere sahip olma" ve "uluslararası hukuktan doğan haklarını uluslararası düzeyde doğrudan koruyabilme yeteneklerine sahip olma" durumu uluslararası hukukun süje-

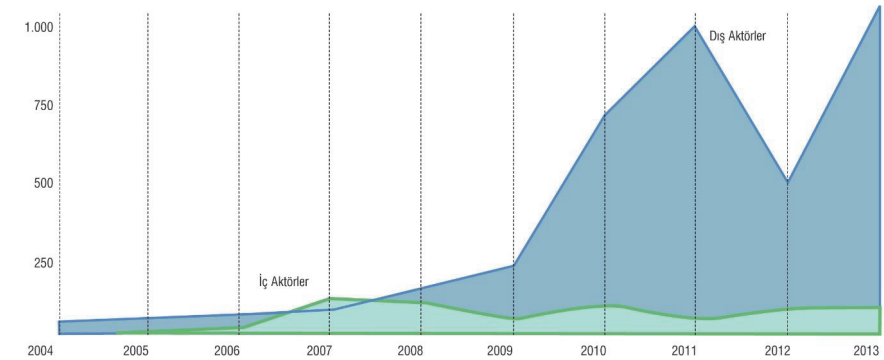
lerini belirlemek için kullanılan iki kriter olarak belirtilmektedir (Pazarcı, 2013, 15). 19. yüzyıl boyunca sadece devletler bu iki kriter bağlamında uluslararası hukukun süjesi olarak değerlendirilmekteydi. İkinci Dünya Savaşı sonrasında ise devletler tarafından oluşturulan hükümetler arası kuruluşlar, bireyler tarafından oluşturulan STÖ'ler, çokuluslu şirketler ve bireyler de uluslararası hukukun süjesi olarak ortaya çıkmaya başlamıştır (Hofmann and Geissler, 1999).

Çokuluslu şirketlerin hukuksal statüsü konusunda tartışmalar devam etmektedir. Ancak, eylem ve işlemlerinden dolayı devletlerce sorumlu tutulmalarının zorluğu karşısında şirketlere uluslararası hukuk kişiliği verilmesi gerekli görülmüştür. (Shaw, 2003, 224). Dijital dünyanın genişlemesiyle birlikte klasik egemenlik ve sınır kavramlarının giderek anlamsızlaşmasıyla şirketlerin güçlü bir aktör olarak ortaya çıkışının hızlanması beklenmektedir. Öyle ki, Google, Dropbox, Amazon gibi şirketler, bireylere, diğer şirketlere ve kendilerine ait büyük verileri bulut sistemlerinde korumaktadır. Şirketlerin hak ve yükümlülüklerini belirleyen -sadece Belçika, Fransa ve Hollanda tarafından kabul edilen- 1956 tarihli Lahey Sözleşmesi yeterli sayıda ülke tarafından kabul görmediği için yürürlüğe girememiş, bu sebeple davranış yasaları (*code of conducts*) oluşturulmaya başlanmıştır (Convention, 1956). Ancak uluslararası düzeyde olmasa da ülkesel ve bölgesel düzeyde, şirketlerin altyapılarında veya veri tarlalarında bulundurdukları verileri korumalarına ilişkin hukuki metinler çıkarılmıştır. Avrupa Birliği ve ABD sınırları içerisinde, veri işleyen veya depolayan şirketlerin alması bir takım yükümlülükler belirlenerek, uygun güvenlik düzeyini sağlamaya yönelik gerekli tedbirleri almaları zorunlu tutulmuştur. Öte yandan şirketler, sahip oldukları şirket sırlarını ve ticari sırlarını korumak amacıyla güvenlik tedbirleri alma ihtiyacı duymaktadır.

b) Saldırıların Anatomisi

Günümüzde siber saldırıya en fazla devletlere ait bilgisayar ağları değil özel teşebbüslere ait bilgisayar ağları maruz kalmaktadır. Öyle ki, siber suçlar ve siber casusluğun dünya ekonomisine yıllık maliyeti, 445 milyon dolar olarak hesaplanmaktadır (CSIS, 2014). Bu maliyet içerisinde fikri mülkiyet hırsızlığı büyük bir yer tutmaktadır (Ibid). Bu tür hesaplamalar her ne kadar tartışmalı olsa da siber tehdidin büyüklüğünün anlaşılması açısından bir fikir vermektedir.

Grafik 1: Veri Kaybı Gerçekleşen Saldırılarda Aktörler

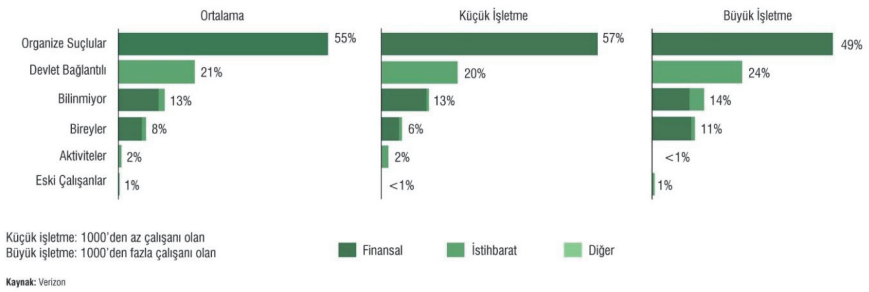


Kaynak: Verizon

Öte yandan 95 farklı ülkeden 50 şirketin katkı sunduğu, 63.437 siber olayın incelendiği *Verizon 2014* Data *Breach Investigation* raporuna göre siber saldırıların büyük bir bölümü dış aktörlerden kaynaklanmaktadır (bknz: Grafik 1) (Verizon, 2014).

Aynı firmanın 2013 raporu verilerine göre ise dış aktörler, organize suç örgütleri, devlet bağlantılı gruplar, bireyler, aktivistler ve eski çalışanlar olarak göze çarpmaktadır (bknz: Grafik 2) (Verizon, 2013).

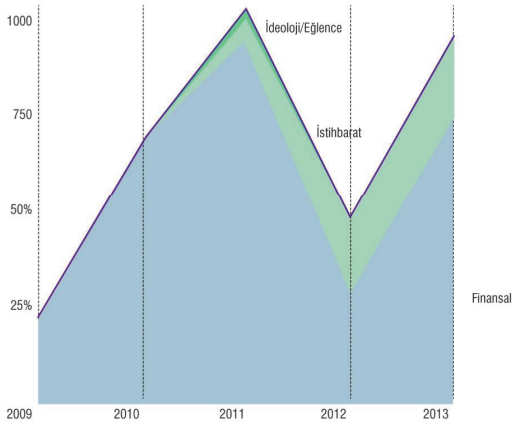
Grafik 2: Dış Aktörler



Kaynak: Verizon

Bu rapora göre 1000'den az çalışanı olan küçük işletmelerin ve 1000'den fazla çalışanı olan büyük işletmelerin maruz kaldığı siber saldırıların yarısından fazlası ekonomik çıkar elde etme motivasyonuyla hareket eden organize suç örgütleri tarafından gerçekleştirilmektedir. Devlet bağlantılı olduğu düşünülen aktörlerin oranı ise ortalama yüzde 21 olarak gözükmektedir. Dolayısıyla, şirketlerin giderek artan oranda sınır aşan boyutlu siber saldırılara maruz kaldıkları anlaşılmaktadır.

Grafik 3: Veri Kaybı Gerçekleşen Saldırılarda Motivasyon



Kaynak: Verizon

Öte yandan siber saldırıları gerçekleştiren aktörlerin ana motivasyonu ekonomik kazanç sağlamak olarak göze çarpmaktadır (bknz: Grafik 3). Dış aktörlerin ikincil motivasyonlarının ise istihbarat toplamak olduğu görülmektedir. Bu kapsamda *Mandiant* firmasının APT1 raporu önemli bilgiler içermektedir. Rapor, Çin Halk Cumhuriyeti ordusu altında yer alan bir birimin, *Advanced Persistent Threat (APT)* olarak adlandırılan bir saldırı yöntemiyle 2006-2010 yılları arasında, askeri ve teknoloji alanında çalışan kritik öneme sahip farklı sektörlerden 141 ABD menşeli şirketin sistemlerinden veri sızdırdığını iddia ediyor. (Mandiant, 2014) Devlet bağlantılı/destekli olarak ifade edilen bu uzun süreli saldırı sonrasında gerek şirketler gerekse de devlet kurumları nezdinde gerekli güvenlik tedbirlerinin alınması için çalışmalar yapılmıştır.

c) Şirketlerin Aldığı Tedbirler

Çokuluslu şirketler, ekonomik kazançlarını ve yatırımlarını koruyabilmek adına askerî güç kullanabilmekte, paralı askerler tutabilmekte çıkarlarını korumak doğrultusunda devlet yönetimlerine müdahale edebilmektedir (Başlar, 2005, 194). Günümüzde ise, şirketler sadece ekonomik kazanç ve yatırımlarını değil, şirket ve ticari sırlarını ve altyapılarında depoladıkları başkalarına ait verileri korumak için çeşitli yöntemlere başvurmaktadır.

Birçok büyük şirketin kendi siber olaylara müdahale ekiplerini (*Incident Response Teams*) oluşturdukları, pasif savunma uygulamalarının yanı sıra aktif siber savunma uygulamalarını da hayata geçirdikleri görüyoruz. İlk olarak aktif siber savunma kapsamında şirketler ve devletler, bal küpü (*honeypot*) uygulamalarıyla saldıranı şaşırtarak başka bir hedefe yönlendirebilmekte, sistem içerisine giren saldırganın "kontrol altında" hareket etmesini sağlayarak kendileri hakkında bilgi toplanmasını önleyebilmektedir (ENISA, 2014). Ayrıca bu uygulamayla, olası bir siber saldırgan ve saldırı önceden tespit ederek sonlandırabilmektedir (Ibid). Bu ve benzeri uygulamalarla hedef alınan sistem içerisinde, hangi dosyaların hedefte olduğu, daha çok ne tür verilerin arandığını belirlemek; sistem dışında ise saldırının nereden geldiğini tespit etmek, saldırı kaynağına erişmek, saldıranın bilgisayarına girmek ve taramak, hatta veri silmek ve değiştirmek mümkün olmaktadır.

Bu yazıda dış aktörlerin sınır aşan nitelikte olduğu bir ön kabul olarak ele alındı. Ancak bu aktörlerin bir bölümü ülke içerisinde yer alabilir. Ülke içerisinde yer alan bu aktörlere ulusal ceza hukuku hükümleri çerçevesinde cevap verilirken, sınır aşan boyutta uluslararası hukuk hükümleri devreye girecektir. Örneğin, *Akbank* finansal sistemine, THY altyapılarına, ASELSAN sistemlerine karşı düzenlenen organize bir siber saldırıda, saldırıyı düzenleyen kişilerin bir kısmı Türkiye'de ele geçirildiğinde, Türk Ceza Kanunu'nun bilişim alanında suçlar başlığı altındaki hükümleri uygulanacaktır. Yurt dışında yer alan ve yerleri tespit edilen kişiler hakkında o ülke yetkilileriyle iletişime geçilecek, gerekli adımların atılması talep edilecektir. Ancak klasik hukuk terminolojisinin kavramsallaştığı dönem sahip olunan "zaman algısı" artık geçerli değildir. Siber dünya, hukukun çok daha hızlı bir şekilde harekete geçmesini zorunlu kılmaktadır. Bu açıdan, bu firmalar kendi siber olaylara müdahale ekibiyle, saldırı karşısında bazı önlemler alamaz mı? Ele geçirildiğini düşündüğü kendi verilerini kurtarmak amacıyla karşı-hack (hack back) ya da saldırı öncesinde ön alıcı hack gibi hamlelerde bulunabilir mi?

Benzer bir olayda, 2010 yılında veri tabanları siber saldırıya uğrayan *Google*, Tayvan'da yer alan saldıranın bilgisayarına karşı bir saldırıyla erişim sağlamıştı (Worthen, 2014). Ancak *Google* yetkilileri, saldıranın bilgisayarında aralarında *Symantec*, *Yahoo*, *Adobe Systems*, *Northrop Grumman* ve *Juniper Networks* gibi

kurumların bulunduğu 33 şirketin bazı kritik verilerinin ele geçirildiğini de fark etti. Sonrasında *Google* Çin pazarından çekilme kararı almıştır (Vascellaro, Dean ve Gorman, 2014). Her ne kadar Google, büyük çaplı bir saldırının izlerini tespit etmiş ve durumu yetkililerle paylaşmış olsa da üzerinde durulması gereken iki nokta bulunmaktadır: i) Google'ın böylesi bir karşı saldırı düzenleme hak ve yetkisi bulunuyor mu? ii) Google karşı saldırıda ele geçirdiği verilerle diğer şirketlerin pek çok gizli verisine de ulaşmış ve bir bakıma saldırının ortağı olmuş oluyor mu?

d) Hukuka Uygunluk Tartışması ve Self-Help

Öncelikle belirtmek gerekir ki, gerek Türk Ceza Kanunu kapsamında gerekse de Amerika'daki federal kanunlar ya da Avrupa ülkelerindeki yerel mevzuat uyarınca bir kişinin bir bilişim sisteminin bütününe veya bir kısmına, rızası dışında hukuka aykırı olarak girmek suçtur. Dolayısıyla açık bir şekilde karşı hack bir suç olarak anlaşılmaktadır. Öte yandan ceza kanunları bir kimsenin, kendisinin veya bir başkasının herhangi bir hakkına yönelen bir saldırıyı def etmek amacıyla, saldırı ile orantılı biçimde, saldırı sürerken kuvvet kullanmaya izin vermektedir (Türk Ceza Kanunu, 2004). Bu düzenlemelerin uluslararası hukuk literatüründe yer alan meşru müdafaa ile uyumlu ve paralel olduğunu belirtmek gerekiyor.

Bu bakımından Google ya da bir Türk şirketi ceza hukuku bağlamında meşru müdafaa kavramına, ABD ya da Türkiye ise uluslararası hukuk bağlamında meşru müdafaa hakkına dayanarak birtakım adımlar atabilir. Zira Google, sahip olduğu dijital varlığa yöneltilen bir saldırıyı, Roma Hukukunun temel prensibi *dominium'a* dayanarak, savuşturmak isteme hakkına sahiptir. Dominium prensibi, bir eşya üzerindeki herkese karşı ileri sürülebilen sahiplik hakkını ve bu eşyanın korunması için gereken tedbirleri alabilmeyi ifade etmektedir (Burdick, 2007, 325) Ancak alınan önlemler, (örneğin saldırganın teknik altyapısının etkisiz hale getirilmesi, internet kör vb. karşı hack uygulamaları) sınır aşan boyutta, uluslararası nitelikte ve zarar verici mahiyettedir. Dikkat edilmesi gereken nokta, karşılık vererek saldırıyı durdurmanın zorunlu olması ve orantılı, asgari bir kuvvet kullanarak sorunun çözülmesi esastır. Benzer şekilde internet güvenlik şirketlerinin, karşı hack düzenleyerek saldırganları internet kör duruma getirdikleri belirtilmektedir (Condron, 2007, 410-411).

Bir devlet olarak ABD ise dijital alanına yapılan bu saldırıyı, -her somutta olayın şartlarına göre- egemenlik ihlali, güç kullanma ya da silahlı saldırı olarak niteleyebilir ve gerekli önemleri alabilir (Halberstam, 2013). Pandoranın kutusunun açıldığı yer tam olarak da burasıdır. Zira Google, saldıranın bilgisayarına zarar da verebilecek zamana, kapasiteye ve imkâna sahiptir. Aksine ABD'nin bir devlet olarak saldıranın ağına erişmesi uzun ve zahmetli bir yol olacaktır. Bu durum, şirketlere haklarını korumak için rahatça tedbirler alabileceği bir serbestiyet de sağlamaktadır. Öte yandan bir şirketin yapacağı karşı saldırının, yol açacağı etkiler tahminlerin ötesinde olabilir. Uluslararası krizlere yol açabileceği gibi, topyekûn ekonomik ve finansal ağların savaş alanına dönmesine, kimin kime ne için ve ne gerekçe ile saldırdığının tespit edilemediği bir kaosa yol açabilir.

Bu durumda, devletler ile devlet dışı aktörler arasında bir denge kurabilecek güçlünün hukuku olarak da adlandırılan kendi kendine yardım (self-help) kurumu *de facto* gerçekliği ifade etmek için kullanılmaktadır. Kendi kendine yardım kurumunun en dikkat çeken örneği olarak 1992 yılında sonuçlanan *United States v. Alvarez-Machain* davası gösterilebilir. Narkotik bölümünde çalışan bir memurun 1985 yılında Meksika'da öldürülmesi sonrasında, suça karışan kişilerin yakalanması ve mahke-

mede yargılanması için Amerikan hükümeti girişimler başlatmıştır (Semmelman, 1992, 811-820). Meksika ile ABD arasında suçluların iadesi anlaşması kapsamındaki prosedürün işletilmesi uzun bir zaman alacağı için, Amerikan hükümeti, suça karışan Alvarez Machain derdest edilerek mahkeme önüne çıkarılmasını sağlamıştır (Ibid). Yüksek Mahkeme, Alvarez'in, Meksika'dan derdest edilip mahkeme önüne getirilmesini, -her ne kadar uluslararası hukukun prensiplerine aykırı gibi gözükse de- Meksika-ABD arasındaki iade anlaşmasına ve hukuka uygun olarak nitelemiştir (Ibid).

IV. Sonuç

Her ne kadar pek çok hukuki ve siyasi probleme neden olacak olsa da kendilerine bir saldırı yöneltilen şirketler, dijital varlıklarını korumak için birtakım aktif savunma mekanizmaları kurabilmelidir. Ancak bu sınırsız bir hareket alanı sağlamamaktadır. Gerek uluslararası hukuk gerekse ulusal hukuk, şirketlerin hak ve yükümlülüklerini düzenleyen kurallar geliştirmektedir. Devletlerin, siber saldırıların birincil hedefinde olan şirketleri bir yandan korumak diğer yandan ise sınırlandırmak için tedbirler almaları gerekmektedir. Aynı zamanda ekonomik ve siyasal bir alan olan siber dünyanın giderek askerîleşmesi (Cavelty, 2012) şirketleri ve özel ağları çeşitli riskler altında bırakmıştır. Bu risklerle baş edilebilmesi için devlet-özel şirketler işbirliği zorunlu hâle gelmektedir. Bu bağlamda şirketler, 19. yüzyıl benzeri bir ortamda *self-help* tedbirleri alabilmeli ancak elde ettikleri bilgileri hukukun sınırları içerisine taşıyarak resmi kurumlarla paylaşmalıdır.

Son tahlilde, 'kendine yardım' niteliğindeki aktif savunma mekanizmalarıyla, makul ve orantılı bir kuvvet kullanarak, suçun işlenmesinin, devam etmesinin ve tamamlanmasının önlenmesi hukuk mantığın uygun olmaktadır. Benzer şekilde siber uzayın güvenliğinin artırılması noktasında kamu kurumları ile özel sektör arasında sağlanacak işbirliği (*whole of government approach*) en ideal çözüm olarak önerilmektedir (NATO, 2014). Bu yaklaşımla, şirketler ile resmi yetkililer arasında üst seviyede iletişim kanalları kurulacak ve saldırı öncesinde, anında ya da sonrasında hızlı bir cevap verilmesi mümkün olacaktır.

KAYNAKÇA

Alpkaya, G. (1997) *Nükleer Silah Tehdidi ya da Kullanımının Hukuka Uygunluğu*, Ankara Üniversitesi Siyasal Bilgiler Fakültesi Dergisi, Cilt: 52 Sayı: 1.

Başlar K. (2005) *Uluslararası Hukukta Hükümet Dışı Kuruluşlar*, Nobel.

Birleşmiş Milletler Kurucu Antlaşması, (1945) Birleşmiş Milletler, New York*, http://www.uhdigm.adalet.gov.tr/sozlesmeler/coktaraflisoz/bm/bm_01.pdf,* [erişim tarihi 14.02.2016].

Burdick, William Livesey. (2007) *The Principles of Roman Law and Their Relation to Modern Law,* New Jersey: The Lawbook Exchange.

Cavelty Myriam Dunn (2012) *The Militarisation of Cyberspace: Why Less May Be Better*, 2012 4th International Conference on Cyber Conflict, C. Czosseck, R. Ottis, K. Ziolkowski (Eds.), NATO CCD COE Publications, Tallinn.

Cavelty Myriam Dunn (2012), *The Militarisation of Cyber Security as a Source of Global Tension*, Strategic Trends Analysis, Center for Security Studies.

Center for Strategic and International Studies (CSIS) (2014) *Net Losses: Estimating the Global Cost of Cybercrime: Economic Impact of Cybercrime http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf,* [erişim tarihi 14.02.2016].

Convention (1956), *The Recognition of the Legal Personality of Foreign Companies, Associations and Institutions*, http://www.hcch.net/index_en.php?act=conventions.status&cid=36, [erişim tarihi 14.02.2016].

Condron M. (2007) *Getting It Right: Protecting American Critical Infrastructure in Cyberspace*, Harvard Journal of Law and Technology, Vol. 20.

Davis, J. (2007) *Hackers Take Down the Most Wired Country in Europe* Wired: *http://archive.wired.com/politics/security/magazine/15-09/ff_estonia?currentPage=all*, [erişim tarihi 14.02.2016].

Dinstein Y. (2013) *Cyber War and International Law: Concluding Remarks at the 2012 Naval War College International Law Conference*", International Law Studies, Sayı 89.

Dinstein Y. (2012) *War, Aggression and Self-Defence* 5th ed. Cambridge University Press.

ENISA, (2014) *Proactive Detection of Security Incidents*, *https://www.enisa.europa.eu/activities/cert/support/proactive-detection/proactive-detection-of-security-incidents-II-honeypots,* [erişim tarihi 14.02.2016].

Germany/Denmark; Germany/Netherlands (1969) *North Sea Continential Shelf Case* http://www.icj-cij.org/docket/files/52/5563.pdf [erişim tarihi 14.02.2016].

Hofmann ve Geissler (1999) *Non-State Actors as New Subjects of International Law: International Law - From the Traditional State Order Towards the Law of the Global Community*, Duncker & Humblot.

Halberstam Manny (2013) *Hacking Back: Reevaluating the Legality of Retaliatory Cyberattacks*, The George Washington International Law ReviewVol. 46.

Islamic Republic of Iran v. United States of America, (2003) *Case Concerning Oil Platforms* http://www.icj-cij.org/docket/files/90/9715.pdf [erişim tarihi 13.02.2016].

Mandiant (2014) *APT1: Exposing One of China's Cyber Espionage Units http://intelreport.mandiant.com/,* [erişim tarihi 13.02.2016].

Nicaragua v. United States of America, (1986) *Case Concerning Military and Paramilitary Activities in and against Nicaragua, http://www.icj-cij.org/docket/files/70/6503.pdf* [erişim tarihi 13.02.2016].

Öktem Emre, (2013) *Uluslararası Teamül Hukuku*, İstanbul: Beta Yayınları.

Pazarcı H. (2013) *Uluslararası Hukuk*, Ankara: Turhan Kitapevi.

Pehlivan, Oğuz Kaan. (2013), *Siber Güç Kapasitesi, Asimetrik Savaşın Parametreleri,* Analist Journal Vol. 32.

Pehlivan, Oğuz Kaan. (2014), *Yeni Dünya'nın Keşfi: Siber Fırsatlar ve Tehditler*, Analist Journal Vol. 40.

Ruus, K. (2008) *Cyber War I: Estonia Attacked from Russia* European Affairs: Volume number 9, Issue number 1-2.

Ruus, K. (2007) *E-Stonia: Pioneer of Internet Innovation and e-Goverment,* European Affairs: Volume number 8, Issue number 1.

Schnurer, Eric. (2015) *E-Stonia and the Future of the Cyberstate* Foreign Affairs https://www.foreignaffairs.com/articles/eastern-europe-caucasus/2015-01-28/e-stonia-and-future-cyberstate [erişim tarihi 13.02.2016].

Semmelman J. (1992) *United States v. Alvarez-Machain* The American Journal of International Law (American Society of International Law) Sayı: 86 (4).

Shaw M. (2003) *International Law*, Cambridge University Press, 2003

Siber Savaşa Uygulanacak Hukuk Hakkında Tallinn El Kitabı, Milli Güvenlik Kurulu Genel Sekteterliği, http://www.mgk.gov.tr/index.php/siber-savasa-uygulanacak-hukuk-hakk-nda-tallinn-el-kitab-uluslararas-siber-guevenlik-hukuku# [erişim tarihi 13.02.2016].

Talinn Manuel. (2013), Talinn Manuel on the International Law Applicable to Cyber Warfare, Cambridge University Press.

Tsagourias Nicholas (2012) *Cyber Attacks, Self-Defence and the Problem of Attribution* Journal of Conflict and Security Law.

Türk Ceza Kanunu. 2004/25611, http://www.mevzuat.gov.tr/MevzuatMetin/1.5.5237.pdf [erişim tarihi 05.09.2014].

Walker, R. (2014) *Other Ways Than By (Kinetic) Warfare,* CS Monitor*, http://www.csmonitor.com/The-Culture/The-Home-Forum/2009/0123/p18s01-hfes.html*, [erişim tarihi 01.09.2014].

UAD Danışma Görüşü (1996) *Legality of the Use of Nuclear Weapons*, *http://www.icj-cij.org/docket/files/95/7495.pdf,* [erişim tarihi 24.09.2014].

United States v. Alvarez-Machain (1992) 504 U.S. 655 http://caselaw.lp.findlaw.com/scripts/getcase.pl?navby=CASE&court=US&vol=504&page=655, [erişim tarihi 05.09.2014].

Vascellaro J., Dean J. ve Gorman S. *Google Warns of China Exit Over Hacking* Wall Street Journal *http://online.wsj.com/articles/SB126333757451026659* [erişim tarihi 05.09.2014].

Verizon, (2014) *Data Breach Investıgatıons Report http://www.verizonenterprise.com/DBIR/2014/* [erişim tarihi 24.09.2014].

Verizon, (2014) *Data Breach Investıgatıons Report* http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2013_en_xg.pdf, [erişim tarihi 24.09.2014].

Worthen B. *Researcher Says Up to 100 Victims in Google Attack* Wall Street Journal, http://online.wsj.com/news/articles/SB10001424052748704625004575090111817090670 [erişim tarihi 05.09.2014].