Araştırma Makalesi
Research Article

Siber Güvenliğin Uluslararası Politikada Etki Aracına Dönüşmesi ve Uluslararası Aktörler

Transformation of Cyber Security into an Effect Tool in International Politics and International Actors

Vahit GÜNTAY*

Öz

Değişen dünyanın önemli unsurlarından biri haline gelen siber alan sahip olduğu özellikler ile dikkat çekmektedir. Çıkar mücadelesi açısından bir parametre oluşturan siber saldırılar farklı aktörlerin ilgisini çekerek uluslararası ilişkiler içerisinde tartışma alanına dâhil olmuştur. Uluslararası politikada etki aracı haline gelen siber güvenlik, sahip olduğu özelliklerin birçoğunu saldırı konseptine dönüştürmeye de başlamıştır. Bu çerçevede uluslararası ilişkiler temelindeki yaklaşımlar ve kavramsal bütünlük de siber alanı teorik olarak incelenir hale getirmiştir. Çalışma dâhilinde siber saldırılar ve siber istihbarata ilişkin birtakım veriler uluslararası politika içerisinde ele alınmış; aktörlere ilişkin değerlendirmeler teorik ve pratik örnekleriyle analiz edilmiştir.

Anahtar Kelimeler: *Siber Güvenlik, Uluslararası İlişkiler, Uluslararası Politika, Siber Saldırı, Siber Caydırıcılık.*

Abstract

Cyber area, which becomes one of the important factors of changing world, attracts attention with its qualities. Cyber attacks that create a parameter in terms of interest struggle are included into the discussion field of international relations through attracting different actors. Cyber security, which became an effect tool in international policy, has started to transform many of its components

* Dr. Öğr. Üyesi, Karadeniz Teknik Üniversitesi, İİBF, Uluslararası İlişkiler Bölümü, e-posta: vahitguntay@gmail.com.

Geliş Tarihi/Received: 31.07.2017
Kabul Tarihi/Accepted: 03.01.2018

into attacking concept. In this context, approaches and conceptual unity within international relations have also made cyber area to be researched theoretically. In this study, cyber attacks and data about cyber intelligence are evaluated in terms of international policy; and evaluations on actors are analyzed theoretically and through practical examples.

Keywords: *Cyber Security, International Relations, International Policy, Cyber Attack, Cyber Deterrence.*

Giriş[1]

Uluslararası ilişkiler temel olarak göstermiş olduğu disiplinler arası özellikle beraber politik alanın tüm araçlarıyla tartışılır hale gelmiştir. Uluslararası anlamda aktörlerin birbirleriyle olan mücadeleleri, bu araçların çeşitlenmesindeki en önemli sebeplerin başında gelmektedir. Uluslararası güvenlik temelinde tartışma aritmetiği bulan siber güvenlik ve çıktıları, değişen dünya açısından politik arenada kendisini fazlasıyla hissettirmektedir. Çıkar mücadelesinin merkezde olduğu düzey, siber güvenlik ve temelindeki araçlarla güç mücadelesinin ana aktörleri olma özelliğini koruyan devletlerin ajandasında üst sıralara yükselmiştir. Özellikle nükleer ve konvansiyonel unsurlara dayalı caydırıcılık; fiziksel unsurlara dayalı zararı düşük yoğunluklara indiren fakat etkili bir araç bütünlüğü sunan siber saldırıları bir tercih haline de dönüştürmüştür.

Siber mücadelenin devletler arasındaki ilişkilere etki ettiğine dair birçok veri mevcuttur. Siber alanın uluslararası ilişkiler boyutunda tartışıldığı ve artık "siber politikalar" adıyla çalışma bütünlüğüne kavuşan bu veriler bütünü güncel çalışmalar açısından ciddi bir artış göstermektedir. Siber savaş kavramı ne kadar tartışmalı bir kavram olursa olsun uluslararası aktörlerin siber alan içerisinde çeşitlendiği ve bu durumun uluslararası ilişkilerde etki araçlarına dönüştüğü bir gerçekliktir. Bu etki araçları içerisinde, uluslararası politika açısından yükselen siber

[1] Çalışma; Ponemon Institute, McAfee Labs. ve Kaspersky Lab. üzerinden yararlanılan verilerin güncel halini içermektedir. Bu kurum ve şirketler arasında benzer verilere ilişkin eşzamanlı bir etkileşim yoktur ve farklı zamanlarda ortaya konulan veriler belirli zaman dilimlerinde güncellenmektedir.

alan, caydırıcılık konseptiyle de bir seçenek haline dönüşmüştür.

Uluslararası ilişkiler boyutuyla ele alınan siber güvenlik ve onun özelindeki siber savaş kavramı, kendi içerisinde gizemli olmaktan çıkmıştır. Saldırı niteliklerinin nereden geldiği ile ilgili tespitler yapılabilmekte ve bu durum uluslararası aktörler açısından uluslararası sistemi olumsuz etkilemektedir. Uluslararası politika açısından sorun, devlet merkezli yaklaşımlardan kaçınılması gerekliliğidir. Çalışmanın temelinde bu merkeziliğin kendi içerisindeki çeşitliliği vurgulanmıştır.

Siber tehditlerin uluslararası sistem açısından varlığı, devletleri sıcak çatışmalara sürükleyecek düzeye gelmiştir. Bu konudaki en önemli gelişmeler ise söylemler ve verilen karşılıklardır. Soğuk Savaş ve sonrasında güvenlik algılamalarındaki farklılık, tehdit parametrelerinin değiştiğini ortaya koymaktadır. Devletlerin siber uzayda bir aktör haline gelmesi, farklı aktörlerle ilişkilendirildiğinde günümüz gelişmeleri açısından artık bir gerçekliktir ve uluslararası ilişkiler temelinde daha çok gündeme gelmektedir. Bu temel dâhilinde çalışma içerisinde siber güvenliğin etki aracı olarak karşımıza çıktığı düzey tartışılmıştır. Bu konudaki dönüşüm kullanılan araçlarla birlikte siber istihbaratın yönüne dair tespitlerle şekillendirilmiş ve siber saldırılar başta devletler olmak üzere uluslararası aktörlerle birlikte ele alınmıştır.

1. Siber Güvenliğin Uluslararası İlişkilerde Etki Araçlarına Dönüşmesi

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

Siber uzayın tartışıldığı ve konumlandığı alanda, artık siber müdahale araçları olarak siber saldırı yöntemleri ve siber silahlar geliştirilmiştir. Siber silahların kullanımına ilişkin verilerin toplanması ve bunların politik boyuta taşınmasıyla birlikte, siber istihbarat dediğimiz

bir çalışma alanı oluşmuş ve bu alanda nitelikli personele ihtiyaç duyulmaya başlanmıştır. Siber saldırıların hazırlık ve savunma aşamalarına ilişkin ise devletler kimi zaman iş birliği içerisinde hareket ederken, kimi zaman da kendi öz imkânları ve kabiliyetleri doğrultusunda bu alanda etkili olmaya çalışmaktadır.

1.1. Genel Olarak Siber Silahlar

Siber saldırının hangi tür yazılım ve donanımlar ile gerçekleştirileceği konusunda, bir başka deyişle ne gibi zararlı bilişim unsurlarının siber saldırı silahı olarak nitelenebileceği hakkında literatürde kesin mutabakat sağlanmış değildir. Bunun bir nedeni, muhtemelen bilişim alanındaki gelişmelerin olağanüstü hızı ve silah olarak sınıflandırılabilecek yazılım ve programların konvansiyonel silah sistemlerine göre resmî şekilde açıkça tasnif edilmemiş olmasıdır.[2] Her ne kadar bu tasnif, nitelendirme olarak siber silah algısını geliştirmemiş olsa da, uluslararası alandaki olayların seyrine etki eden bu türden araçlar alanın müdahale unsurları haline dönüşmüştür.[3]

Siber silahlara örnek olarak zararlı yazılımlar bakteri, solucan, virüs, trojan, arka kapı ve sistemleri etkilemeye yönelik saldırılar, hizmet dışı bırakma saldırıları verilebilir. Başka programlarla ilişkili olup olmamasına bağlı olarak da gruplandırmalar yapılabilir. En temel siber silahlarını, gelişmişliği ya da geçmişine bakılmaksızın, Çifçi şu şekilde gruplandırmıştır:[4]

- Bakteri: Bağımsız, kendi kendine çoğalabilen, bir bilgisayarda birçok türünü kendi kendine yaratabilen bir programdır; çoğalan türlerini çalıştırırken, daha fazla disk alanı ve işletim zamanı işgal ederler.

---

[2] Şener Çelik, "Stuxnet Saldırısı ve ABD'nin Siber Savaş Stratejisi: Uluslararası Hukukta Kuvvet Kullanmaktan Kaçınma İlkesi Çerçevesinde Bir Değerlendirme", ***Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi***, 2013, 15(1), 137-175, s.141.

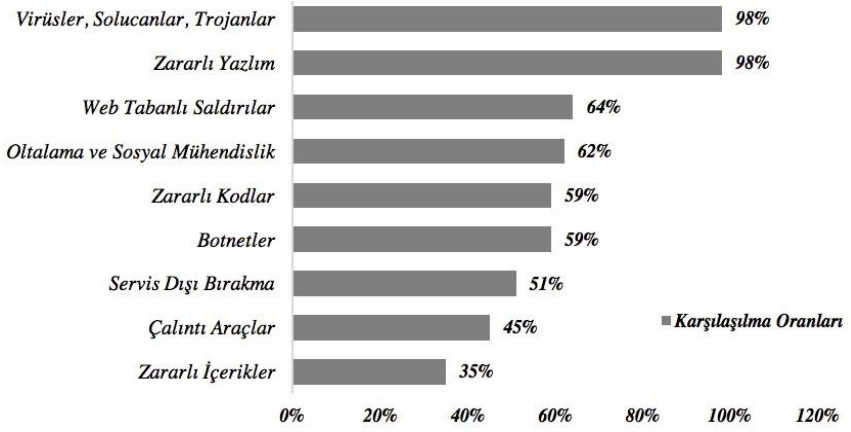
[3] Dale Peterson, "Offensive Cyber Weapons: Construction, Development and Employment", ***Journal of Strategic Studies***, 2013, 36(1), 120-124, s. 121.

[4] Hasan Çifçi, ***Her Yönüyle Siber Savaş***, TÜBİTAK Bilim Kitapları, Ankara, 2013, s. 150.

- Solucan (*Worm*): Kurt da denmektedir; bağımsız, kendi kendine çoğalabilen, ağda bir bilgisayardan diğerine yayılma yollarını araştıran ve yayılan bir programdır. Saniyeler içinde milyonlarca bilgisayara ulaşabilir.
- Virüs: Başka programlara bağımlı, kendi kendine çoğalabilen, yerleşebileceği bir programa ihtiyaç duyan bir programdır. İçine gizlendiği program çalıştırıldığı anda veya sistemde istenen herhangi bir işlemin yapılmasından sonra başka programlara bulaşır.
- Truva Atı (Trojan): Normalde yararlı bir program gibi gözüken, ancak gizli bir şekilde, yerleştiği bilgisayara zarar vermeye yönelik olarak kullanılan programlardır. Truva atı, genelde kötü niyetli fonksiyonu harekete geçirmek için duruma bağlı bir test içerir.
- Mantık Bombası (*Logic Bomb*): Belirli bir zamanda veya belirli bir durum oluştuğunda çalışan programlardır. Mantık bombası, bilgisayarda gizli bir şekilde çalışacağı günü bekleyebilir veya kullanılan bir programda zamanı geldiğinde zararlı işlemleri yapacak şekilde ayarlanabilir.
- Arka Kapı (*Backdoor, Trapdoor*): Tuzak kapı olarak da bilinmektedir. Sadece saldırgan tarafından bilinen, normal kimlik kontrol mekanizmalarını kullanmadan karşıdaki sisteme gizli bir kanalla ulaşmayı sağlayan yöntem veya giriş noktasına verilen isimdir.
- Köle Bilgisayarlar (*Botnet, Zombie*): Bilgisayarlar, yüklenen bir program vasıtasıyla uzaktan kontrol edilebilmektedirler. Kullanıcı bilgisayarına gizlice yüklenen ve saldırganın hedef sistemi, internet bağlantısı üzerinden uzaktan kontrol edilmesine imkân sağlayan programlar aracılığıyla köle bilgisayarlar kontrol edilir.
- Kök Kullanıcı Takımı (*Rootkit*): Bilgisayarda çalışan işlemleri, dosyaları veya sistem bilgilerini işletim sisteminden gizlemek suretiyle varlığını gizlice sürdüren zararlı programlara verilen isimdir. Genellikle işletim sisteminde çekirdek düzeyinde (*kernel level*) çalıştıkları için tespit etmek ve kurtulmak çok zordur.

- Tuş Dinleyiciler (*Keylogger*): Temel olarak klavyede basılan tuşları sürekli olarak kayıt etmekte ve bunları belli bir metin dizisi haline getirerek ağ üzerinden saldırgana iletmektedir. Tuş dinleyiciler özellikle siber istihbaratçılar tarafından kullanılmaktadır.
- *Script*: *Script*'ler web sayfalarında çalışan kod topluluklarıdır. Bot desteği ve *script*'ler kullanılarak toplu saldırılar gerçekleştirmek mümkündür.
- Sahte web sitesi: İnternette popüler web sitelerinin birebir kopyalarının yapılması ve benzer adlarıyla yayınlanan web siteleridir. Sahte web sitelerindeki hareketler izlenerek kişisel verilere ulaşılabilmektedir.
- Taklit e-posta hesabı: Taklit hesaplarla istihbarat çalışmaları yapılabilmektedir.

Siber silahların kullanımında amaç ve hedeflenilen yer genelde mevcuttur. İstisnasını özellikle virüs, solucan ve trojan gibi zararlı yazılımların yayıldığı türler bozsa da bazı çalışmalarda karşılaşılma sıklıkları ile ilgili veriler de mevcuttur. Grafik 1'de siber saldırı türlerinin karşılaşılma sıklığına ilişkin oranlar verilmiştir. Karşılaşılma sıklığı açısından karakteristik olarak en yüksek oranlara sahip olan virüs, solucanlar, trojanlar ve zararlı yazılımlar ön planda olsa da, verdikleri zarar açısından diğer siber saldırı türleri spesifik olaylarda ön plana çıkabilmektedir. Bu spesifik olaylardaki maddi kayıplardan ve zararlardan bireyler, kâr amacı güden unsurlar ve uluslararası aktörler etkilenebilmektedir. Devletlerin operasyonel unsurlarını oluştururken bu türden saldırı türlerinden hangilerine başvuracaklarına ilişkin bir tasnif bulunmamaktadır. Bu durum siber saldırılara ilişkin teorik çalışmalarda sorun oluşturmaktadır.



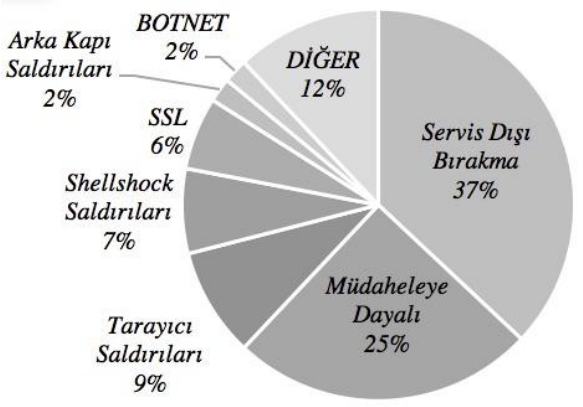
Grafik 1. Siber Saldırı Türlerinin Karşılaşılma Sıklığı[5]

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

Grafik 2'de, 2015 yılı genelinde, en yüksek ağ saldırı türü olarak servis dışı bırakma saldırıları ön planda gözükmektedir. Daha önce vurguladığımız hususlar arasında, birimlerin işleyişini bozmak ve yeri geldiğinde psikolojik bir harp stratejisi izleme adına tercih edilen servis dışı bırakmada maddi kayıplar da doğabilmektedir. Devlet kurumlarının çevrimiçi erişim kanallarına yönelik tercih edilen servis dışı bırakma saldırılarında ciddi bir prestij kaybı da doğabilmektedir. Her ne kadar bu konuda önlemler alınsa da hangi kurumun, ne zaman

[5] Ponemon Institute, ***2015 Cost of Cyber Crime Study: Global***, Ponemon Institute Research Report, Michigan, 2015, p. 11. (Grafik 1 üzerindeki veriler, 252 şirket üzerinden ölçülerek elde edilmiştir. Dağılım olarak saldırı türlerinin sıklığı ve oranları bu şirketlerden elde edilen verilere dayandırılmıştır.)

ve ne şekilde bu türden bir saldırıya uğrayacağı kestirilmesi imkânsız bir durumdur. Kritik kurumların bu konuda tedbirli olması yerinde olacaktır. Bu tür saldırıları örgütleyen devletlerin genellikle kendilerine yönelik benzer saldırılara ilişkin daha az mağduriyet yaşadığı gözlenmiştir.



Grafik 2. En Yüksek Ağ Saldırı Türü Oranları[6]

Siber silahlar açısından bugün ortaya çıkan silahlanma yarışları, Soğuk Savaş dönemine benzerlikten uzaktır. Siber silahların gelişimi bakımından kıyaslandığında, özellikle siber silahların kullanımına ilişkin ilk adımlarda, ilk evreler benzer şekilde tehlikelidir. Siber silahlara ilişkin herhangi bir yarışta büyük stratejik üstünlükler kısa süreli olabilmektedir. Bunun en önemli sebeplerinden biri, karşı tarafın kullanacağı siber silahlara ilişkin manevraların beklenmedik bir şekilde gerçekleşmesidir.[7]

[6] McAfee Labs, ***Threats Report May 2015***, Santa Clara, 2015, p. 44.
[7] P.W. Singer ve Allan Friedman, ***Siber Güvenlik ve Siber Savaş***, çev. Ali Atav, Buzdağı Yayınları, Ankara, 2015, s. 218.

1.2. Siber İstihbarat ve Siber Casusluk

İstihbarat günün şartlarına uygun olarak gelişmektedir ve çeşitli sözlüklerde "akıl, zekâ, malumat, haber, bilgi, havadis, bilgi toplama, haber alma" şeklinde tanımlanmaktadır.[8] Teknolojinin gelişmesiyle ise sadece bilgisayarlar değil; telefonlar, tabletler, evdeki televizyonlar ve hatta buzdolabı gibi eşyalar dahi siber uzaya bağlı hale gelmiştir ve tüm bu dijital verilere ulaşmak amacıyla yapılan istihbarata "siber istihbarat" adı verilmektedir.[9] Siber istihbaratın tanımsal özelliklerinde bu faaliyeti kimin yürüttüğü ve neyi amaçladığı belirleyici olmaktadır ve kavramın kapsayıcılığını genişletmektedir. Uluslararası hukukun da dâhil olduğu siber istihbarat faaliyetleri, Birleşmiş Milletler (BM) Sözleşmesi'nin 2. Maddesi'ndeki egemenlik ve iç işlerine dair hususlarla birlikte tartışma konusudur.[10]

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

İstihbaratçıların işini de saha çalışmalarından kurum içi gelişmelere ve bilgisayar ekranlarına taşıyan, bu gelecek kurgusu olmuştur. Bilgisayarların istihbarat ve araştırma yapmalarını olanaklı kılan teknolojik gelişmeler, bunun baş döndürücü hızına ivme katmıştır. Günümüzde küresel iletişim ağlarından yararlanan gizli servisler, neredeyse istedikleri bütün kapalı veri bankalarına girerek gizli ve özel

---

[8] CIA resmî sitesindeki açıklamada istihbarat, basit ve ilginç bir şekilde, "Ulusumuzun liderlerinin, ülkemizi güvende tutmak için duyduğu bilgi" olarak tanımlanmıştır. Siber istihbaratla elde edilen bilginin genişliği teknolojik gelişmelerle birlikte ciddi bir öneme sahip olmuştur.

[9] Atalay Keleştemur, ***Siber İstihbarat***, Level Kitap, İstanbul, 2015, s. 74.

[10] Victoria Ekstedt vd., "Commitments, Mechanisms & Governance", Alexander Klimburg, (ed.), ***National Cyber Security: Framework Manual***, NATO CCD COE Publication, Talinn, 2010, 146-190, p. 157.

bilgilere ulaşabilmektedir.[11] Birçok güvenlik laboratuarının yapmış olduğu testler ve analizlerde saldırı merkezlerinin kesin tespitleri ise oldukça zor gözükmektedir.[12] Modern terörizmin yıkıcı etkiler bırakacak saldırıların yanında para, silah, bilgi ve doküman transferleriyle ilgilenerek verilere yönelmiş olması istihbaratın karakteristik niteliğini değişime uğratmıştır. Gerek 11 Eylül saldırıları esnasında, gerekse yükselişe geçtiği dönemde, El-Kaide terör örgütünün internet ve "hackleme" teknolojilerinde ciddi bir yol kat etmesi dikkat çekicidir.[13]

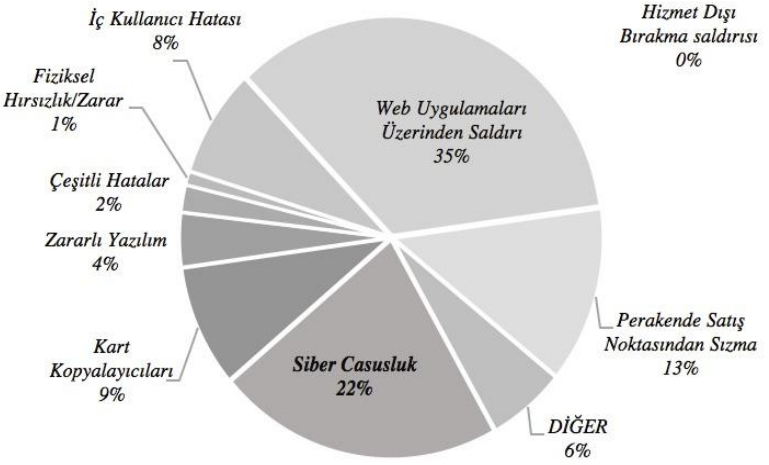
Siber istihbarat açısından uluslararası aktörlerin caydırılması amacıyla bir tercih önceliğine dönüşen "siber casusluk", veri kaybının oluşumunda, Grafik 3'te görüldüğü üzere, önemli bir orana sahiptir. Siber casusluk alanına ilişkin veriler, fiziksel birtakım unsurlara göre daha dikkatli izlenmektedir. Devletlerin nitelikli personel ihtiyacı ve bu konuda kurumsallaşmaya gidilmesi gibi hususlar benzer örneklemlerle de çoğaltılabilir. Özellikle savunma kısmında, devletlerin veya mağdurun eli oldukça zayıflamaktadır. Gelişen saldırı biçimleri ve anlık olarak güncellenebilen siber silahlar, bu konudaki en büyük açığı oluşturmaktadır.

---

[11] Sait Yılmaz ve Olay Salcan, ***Siber Uzay'da Güvenlik ve Türkiye***, Milenyum Yayınları, İstanbul, 2008, s. 18.

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

[13] Luigi Vellone, "From Data to Knowledge: How Intelligence and Security Tools can Help", Fernando Duarte Carvalho ve Eduardo Mateus da Silva, (ed.), ***Cyberwar-Netwar: Security in the Information Age***, IOS Press, Amsterdam, 2006, 115- 130, p. 119.



Grafik 3. Veri Kaybına Yol Açan Saldırıların Dağılımı[14]

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

Farklı kurumlar ve birimlerin oluşturulmasıyla, savaş zamanında casusluğa benzer biçimde siber casusluk da farklı değerlendirmelere tabi tutulmuştur. Siber savaş alanında önemli çalışmalardan biri olan ***Tallinn El Kitabı (Tallinn Manual)***, siber casusluğun insancıl hukuka

[14] Alper Başaran, "Verizon Bilgi Güvenliği Olayları Raporu", 4 Aralık 2014, http://securitist.blogspot.com.tr/2014/12/verizon-bilgi-guvenligi-olaylar-raporu.html, (Erişim Tarihi: 28.07.2017).

aykırı olmadığını ve siber casusların da savaş esiri statüsünü kaybedeceğini belirtmektedir.[15] Uzaktan bilgi toplama operasyonu, düşmanın kontrol ettiği bölgenin dışında gerçekleştirildiği için siber casusluk rejimi burada uygulanmayacaktır. Siber istihbarata yönelik uluslararası uygulamalarda ve devletlerarası boyuttaki gelişmelerde hukuki düzenlemelere bu yüzden ihtiyaç vardır. Yapılacak düzenlemelerin uygulanabilirliği konusunda tartışmalar, düzenlemelerin niteliğinden daha çok tartışılmaktadır.

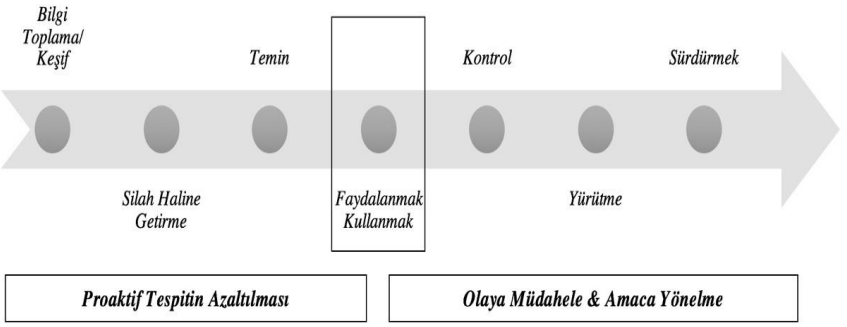
1.3. Siber Saldırılarda Hazırlık Aşaması

Siber saldırı, siber korsanlar tarafından yapılabileceği gibi yetkili resmi kurumların bilgisi dâhilinde de gerçekleştirilebilmektedir. Dolayısıyla siber saldırılar gerek yasal anlamda, gerekse teknik anlamda farklılıklar gösterebilmektedir. Siber saldırı, siber ortam üzerindeki yazılım, donanım ve altyapıları hedef almaktadır. Saldırılar amaçlarına, saldırı şekillerine, etkilerine göre farklılık içermektedir. Kimi saldırganlar ideolojik ya da tamamen kişisel tatmin amaçlı saldırılar düzenleyebilmektedir. Tüm bu saldırı tiplerine ve saldırgan karakterlerine göre bir analiz yapılmakta ve buna göre saldıran kişi ve grupların kimler olduğu tespit edilebilmektedir.[16] Siber saldırıların hazırlık aşaması, bu noktada, genelde saldırıyı düzenleyecek birimin hedeflerine göre şekillendirilmektedir.

Siber saldırıların hazırlık aşaması, saldırı sürecinin aldığı yolu belirleyici en önemli unsurdur. Sürekliliğin kalitesi bu süreçte hazırlık aşamasındaki ciddiyete bağlıdır. Şekil 1'de siber saldırı süreci döngüsü gösterilmiştir. Siber saldırılardaki keşif unsurlarının siber silah haline getirilmesi ve oluşturulabilmesi, sürecin faydaya dönüşmesindeki ilk unsurlardır.

---

[15] Michael N. Schmitt, ***Talinn Manual on the International Law Applicable to Cyber Warfare***, Cambridge University Press, Cambridge, 2013, p. 159.
[16] Atalay Keleştemur, ***a.g.e.***, s. 267.



Şekil 1. Siber Saldırı Süreci/Yaşam Döngüsü *(Lifecycle)*[17]

Her grubun farklı bir saldırı becerisi bulunmaktadır. Uluslararası anlamda bireylerin ya da devletlerin ve kâr amacı güden grupların bu konuda çevrimiçi halde devamlı olarak iletişimde olduğu bir gerçektir. Siber saldırıların ortaya çıkışında karşı tarafa zarar verilme istemi haklı veya haksız olsun, işbirliği yapanlar açısından belli düzeyde samimiyet ve güvene de ihtiyaç duymaktadır. Bu yüzden saldırıların niteliğine ilişkin samimiyetin yanında elde edilecek kazanç, sürekliliği beraberinde getirebilmektedir.

Siber saldırıların ortaya çıkışında ve hazırlanışında, siber uzayın, zayıf olanın güçlü üzerinde üstünlük kurabileceği gibi garip bir avantajı beraberinde getirdiği söylenebilir; fakat siber saldırı yeteneklerinin geliştirilmesine yönelik engeller oldukça düşüktür. Örneğin; insansız uçak sistemi Amerika Birleşik Devletleri'ne (ABD) yaklaşık 45 milyon dolara ve bu sistemin kayıtlarının aktarıldığı uzay uydu şebekesi milyarlarca dolara mal olmuştur. Bu sistemleri çökertmek için *skygrabber* olarak bilinen bir program ise 25,95 dolara mal olmuştur. ABD gibi

[17] Sean Barnum, ***Standardizing Cyber Threat Intelligence Information with the Structured Threat Information eXpression (STIX)***, The Mitre Corporation, Version 1.1, Revision 1, 2014, p. 5.

devletler için gerçek kaygı, diğerlerinin artık siber tehdit oluşturabilmeleri değil, geleneksel kuvvetlerin hassas noktalar oluşturmalarıdır.[18]

Siber saldırıların hazırlık aşamasında, birimler ya da aktörler, tekil hareket etmenin yanında ortak harekât kabiliyetine de sahiptir. Siber ortamın dünyanın her yerinden ulaşılabilirliği, bu alana ilişkin saldırıların hazırlık boyutunu ve birimlerin birbirlerine ulaşma alanını sınırsız hale getirmektedir. Keleştemur,[19] siber saldırı yapanları, sahip oldukları kapasite açısından ayırt etmeksizin, şöyle gruplandırmıştır:

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

1.4. Siber Savunma ve Tehditler

Bir tehdit ile başa çıkabilmenin birinci şartı, onu doğru tanımlayabilmekten geçmektedir. Herhangi bir siber tehdidi tanımlayabilmek için öncelikle saldırıyı kimin yaptığını ve nasıl bir saldırı olduğunu belirlemek gerekmektedir. Siber tehditler, bilişim teknolojisi kullanılarak bir toplumun iç ve dış düzenini muhafaza etme refleksini zayıflatmak veya tamamen yok etmek amacıyla kullanılmaktadır. Dünyanın herhangi bir yerinden başka bir bölgeye yönlendirilen saldırı, küreselleşme sonucunda sınırların ortadan kalkması olgusunu pekiştirmektedir.[20] Verilerin toplamda her yönüyle birbirine bağlı olduğu siber ortam bu sınırları boyutsuzlaştırmıştır. Siber politikalarda temel

---

[18] P.W. Singer ve Allan Friedman, ***a.g.e.***, s. 2015.
[19] Atalay Keleştemur, ***a.g.e.***, s. 267.
[20] Taner Altunok ve Zeynep Kaya, "Siber Tehditlerle Mücadele", Haydar Çakmak ve Taner Altunok, (ed.), ***Suç, Terör ve Savaş Üçgeninde Siber Dünya***, Barış Platin Kitabevi, Ankara, 2009, 137-162, s. 138.

dikotomi olan "saldırı ve savunma" ikilisinde, siber saldırıya ve siber savunmaya ilişkin politikaların oluşturulması hususunda tartışılmaktadır.[21]

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

Siber ortamın merkezî ve sınırları olmayan ağ biçimindeki yapısı, onun herhangi bir devletin veya herhangi bir hukuk düzeninin altında yer almasına engel olmaktadır. Siber ortamda hâkimiyetin kimlerin elinde olacağı veya egemenlik yetkisinin sınırlarının nasıl çizilebileceği sorusu karışık ve yanıtlanması zorunlu bir soru olarak karşımıza çıkmaktadır. Siber ortam; ulusal güvenlik ve siyasi iktidarların askerî saldırıları için bir ortam olarak kullanılabilmektedir. Siber ortam teröristler açısından propaganda aracı olarak da kullanılabilmektedir. Tüm bu unsurlar içerisinde savunmaya yönelik karşı hareketler zorunlu hale gelmektedir.[22] Harekâtın boyutları ele alınırken kaçırılmaması gereken nokta, ön savunmanın oluşturulması gerekliliğidir. Siber saldırılara ve tehditlere karşı ön savunmanın teknik zemini kesin ve net bir çerçeve ile oluşturulamasa da, olası saldırı türlerine karşı tedbirler her zaman mümkün gözükmektedir.

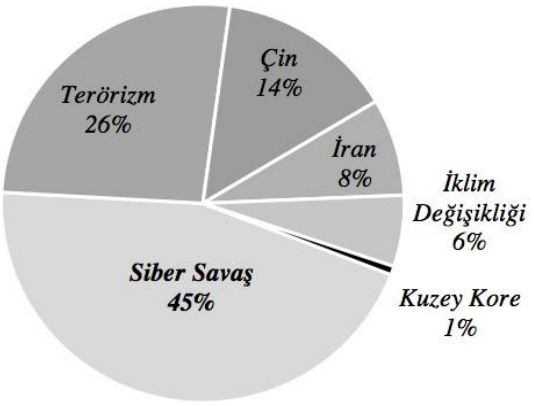
Tehdit olarak algılanan siber saldırılar, birçok toplum için diğer tehdit algılarının önüne geçmiştir. Grafik 4'te görüldüğü üzere, siber savaş tehdidi ABD toplumu için terörizm, Çin ve İran gibi unsurların da önündedir ve savunma sistemi oluşturulması açısından bu algının

---

[21] Alexander Klimburg ve Jason Healey, "Strategic Goals & Stakeholders", Alexander Klimburg, (ed.), ***National Cyber Security: Framework Manual***, Tallinn, NATO CCD COE Publication, Tallinn, 2012, 66-107, p. 74.

[22] Taner Altunok ve Engin Avcı, "Siber Tehditlerin Geleceği ve Alınması Gereken Önlemler", Haydar Çakmak ve Taner Altunok, (ed.), ***Suç, Terör ve Savaş Üçgeninde Siber Dünya***, Barış Platin Kitabevi, Ankara, 2009, 209-232, s. 215.

yönlendirilmesi önemli bir göstergedir. ABD'de çoğu zaman ciddi sıkıntılara yol açan iklimsel sorunlar dahi siber savaş tehdidi yanında tehlike boyutu açısından daha az bir algı düzeyi oranına sahiptir.



Grafik 4. ABD'nin Çıkarları Açısından Hangisi Daha Tehlikeli?[23]

Farklı tehditler ve siber savunma açısından diğer bir tehdit gelişimi ise, siber uzaya artan bağımlılık ve hem devletlerin hem de bireylerin bu konudaki bilgi yetersizliğidir. Karar alıcılar açısından iyi oluşturulmamış kurumsal bir yapı ciddi sorunsala dönüşmektedir ve tehdit oluşturmaktadır. Verilerin korunmasına ilişkin alınabilecek tedbirlerde prosedürel bir yaklaşım yoktur; fakat özellikle fiziksel çevrenin temel unsurları haline gelen iletişim ağları ve bunlara bağlı

[23] Michael Pizzi, "Cyberwarfare greater threat to US than terrorism, say security experts", 7 Ocak 2014, Aljazeera America, http://america.aljazeera.com/articles/ 2014/1/7/defense-leaders-saycyberwarfaregreatestthreattous.html, (Erişim Tarihi: 12.06.2017). Toplam 293 katılımcının yer aldığı araştırmada "Siber Savaş" ilk sırada yer almıştır. Kendisini "Demokrat" olarak tanımlayanlar "İklim Değişikliği" tehdidini ikinci sıraya koyarken; herhangi bir siyasi yaklaşımdan bağımsız düşünenler "Terörizmi" seçmiştir. "Cumhuriyetçiler", "Terörizm" ile "Siber Savaşı" eşit tehditler olarak görmüştür.

cihazların etkinliği her geçen gün artmaktadır. "Siber alana artan bağımlılık düzeyi" olarak da adlandırabileceğimiz bu durum devletlerin korkulu rüyası haline gelmektedir. Siber alandaki altyapının anlık değişimler göstermesi, bu durumun oluşmasında temel neden olarak dikkat çekicidir. Artan bağımlılık düzeyi kısa ve uzun vadede geri çekilememektedir.

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

2. Uluslararası Aktörler ve Siber Mücadeledeki Yerleri

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

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

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

2.1. Devletler

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

Günümüzde savaş teknolojisindeki gelişmeler ve siber uzaya artan bağımlılık, ülkesel devletin siyasal sınırlarının geçit vermezliğini ve bu sınırlar içerisinde söz konusu olan mutlak egemenlik olgusunu aşındıran sonuçlar doğurmuştur.[24] Gelişmişlik düzeylerine göre devletlerin kendi aralarındaki karşılıklı bağımlılık olgusu, ulusal devletin klasik özellikleri üzerinde bazı önemli değişiklikler meydana getirmiştir.[25]

Bu değişiklikler içinde, özellikle siber ortamın kendi yapısal özellikleriyle birlikte devletlere zarar vermesi, belirleyici olan kıstastır. Karşılıklı bağımlılık, egemenlik haklarına müdahale eden saldırgan bir boyuta ulaşmıştır. Siber uzayın nüfuz etme ve sanallaştırma karakteri, geleneksel olarak belirli bir arazinin kontrolünden türemiş olan devlet güçlerinin gerçek sınırlarının olduğu anlamına gelmeye başlamıştır.[26]

Karşılıklı bağımlılık ve egemenlik konsepti içinde ise devletlerin aktör olarak belirginleşmeye başladığı siber uzayda, güç, tam olarak

---

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

[25] Faruk Sönmezoğlu, ***Uluslararası Politika ve Dış Politika Analizi***, Filiz Kitabevi, İstanbul, 2000, s. 34.

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

hesaplanıp tahmin edilememektedir. Kimin daha güçlü olduğunun belirlenmesi adına ortaya çıkan savaşlar öncesinde, taraflar kendini güçlü görüp baskın olacağını hissettiği için girişimlerde bulunmaktadır. Devletler siber güvenlik ortamında, yine siber savaşlar bağlamında, benzer bir düşünceyle hareket etmektedir.[27] Siber ortamda karşılığın nasıl ve ne şekilde olacağını kestiremeyen devletler, kapasite hesaplaması ve rakibi tanıma gibi unsurları masaya koyamamaktadır. [28]

Daha önce değindiğimiz siber savaş konsepti içersinde günümüz için devletlerin temel aktör olduğunu ya da baskın bir tarzda savaş etkileşimi içerisinde olduğunu söylememiz çok güçtür. Bunun en önemli sebebi, sorunların çözümünde devletler arasında ciddi bir gelişmişlik farkı ve güven eksikliğidir. Özünde çatışmalı olan uluslararası sistem, geçmişi bilinmeyen ve geleceği tahmin edilemeyen bir ortamda daha da şüpheci hale gelmektedir.

Devletler kendi aralarında olmasa da farklı aktörlerin devreye girmesiyle siber ortamdan etkilenmekte ve bu etkilenme düzeyi siber ortama bağlılık düzeyine göre farklılık göstermektedir.[29] Şekil 2'de devletlerin web tabanlı saldırılardan etkilenme dağılımı verilmiştir. Uluslararası ilişkiler açısından sınırları belirli olan devletler, etkilenme açısından coğrafi, kültürel ve sosyal unsurlara bakılmaksızın, ciddi bir farklılığa sahiptir. Bu saldırılardan etkilenme oranlarının birbirleri arasındaki çatışma kültürüyle doğrudan alakalı olmadığı olgusu, dağılımın yüzdeleriyle de açıkça ortaya çıkmaktadır. Rusya ve çevresindeki devletlere ait oranların yüksek olmasında bankalara ve finansal kuruluşlara saldırılar, devlet kurumlarına ait verilere

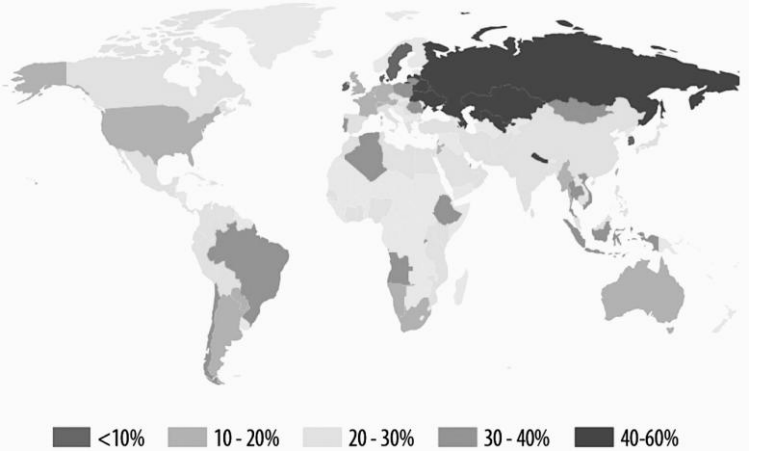
---

[27] Michael G. Roskin ve Nicholas O. Berry, ***Uluslararası İlişkiler, Uİ'nin Yeni Dünyası***, çev. Özlem Şimşek, Adres Yayınları, Ankara, 2014, s. 29.

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

[29] Alexander Klimburg ve Jason Healey, ***a.g.m.***, s. 68.

ulaşılmaya çalışılması ve illegal faaliyetlerin siber ortamda yoğunlaşması gibi unsurlar belirleyici olmuştur.

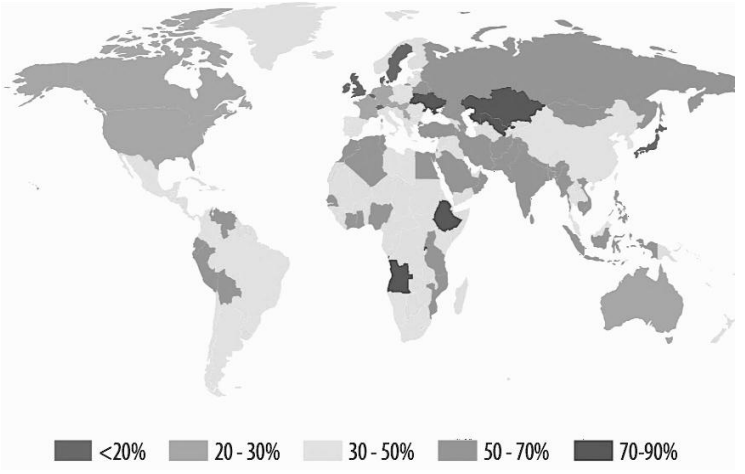


Şekil 2. Web Tabanlı Saldırılarda Devletlerin Küresel Etkilenme Oranları[30]

Uluslararası alanda güç ilişkisinin her şeyiyle etkili olmadığı siber ortam, sadece dış dinamiklerin etkisiyle devletler üzerinde baskı oluşturmamaktadır. Küresel bir aktör olarak devletin sınırları içerisinde olan ve dolaşan siber tehditler farklı fiziki araçlarla da etkinliğini artırabilmektedir. Şekil 3'te yerel siber tehditlerin küresel dağılımı devletlere göre oransal olarak verilmiştir. Web tabanlı saldırılara göre, yerel siber tehditler, etkinlik açısından daha dengeli durmaktadır. Bunun en temel sebebi, fiziksel olarak devletlerin bağlı olduğu teknolojik

[30] Kaspersky Lab., "Kaspersky Security Bulletin 2015", p. 31, https://securelist.com/files/2015/12/Kaspersky-Security-Bulletin-2015_FINAL_EN.pdf, (Erişim Tarihi: 28.07.2016). Kaspersky Laboratuarlarının ölçümlerine göre, 2015 içinde her üç bilgisayardan biri (tüm bilgisayarların %29'u), bir veya daha fazla web tabanlı saldırıya uğramıştır. Genel olarak yüksek oranlara sahip zararlı programlar rapor içerisinde ayrıca belirtilmiştir.

araçların ve altyapının her geçen gün etkinliğini arttırması ve bu araçların varlığının kimi zaman bir caydırıcılık dahi oluşturmasıdır.



Şekil 3. Yerel Siber Tehditlerin Küresel Dağılımı[31]

Farklı güvenlik şirketlerinin yaptığı araştırmalar, devletlerin küresel bir aktör olarak siber güvenlik konsepti içinde maruz kaldıkları etkinin güç ilişkisiyle bağlantılı olmadığını gözler önüne sermektedir. Özel olarak belirli hedeflere yönelmiş devletler veya diğer aktörler, amaçladıkları sonuçlar ve etki açısından farklılık göstermektedir. Son yıllarda artan siber suçlar ve saldırılar siber güvenlik adına en önemli aktörlerden biri haline gelen devletleri uluslararası politika açısından ön

[31] Kaspersky Lab., ***a.g.e.***, p. 32. Kaspersky tarafından test edilen tehditler her ülkenin kurumsal kullanıcılarının yüzdeleriyle elde edilmiştir. "Antivirüs tespit dosyası", kurumsal bilgisayar kullanıcılarının %41'inden etkilenmiştir. Tespit edilen unsurlar bilgisayarların yanında flaş bellekler, hafıza kartları, telefonlar, harici diskler ve ağ araçları üzerinde konumlanmıştır. Genel olarak yüksek oranlara sahip zararlı programlar ve virüsler rapor içerisinde ayrıca belirtilmiştir.

plana çıkarsa da, temel olarak belirli sınıflandırmalardan kaçınılması ve zayıf-güçsüz ayrımına gidilmemesi gerekmektedir.

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

2.1.1. Siber Ordular

"Siber ordu" ülkeyi ya da kurumu siber dünyadan gelebilecek tehdit ve saldırılara karşı koruyacak ve gerektiğinde karşı siber saldırılar gerçekleştirebilecek yetenekteki bilgi güvenliği uzmanlarından oluşturulmaktadır. Siber ordunun mensupları, hem saldırı, hem de koruma yöntemlerini çok iyi bilmek zorundadır. Bu konuda önde gelen ülkelerde genelde iki tür siber ordu bulunmaktadır:[32]

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

Devletin kendi eliyle oluşturdukları ordular içinde saldırı yapabilmek adına çok pahalı ve karmaşık silah sistemlerine ihtiyaç duyulmamaktadır. Resmî olmayan gruplarda olsun, devletlerin resmî siber ordularında olsun, bazen bir adet bilgisayar ve basit bir yazılım dahi bir grup için veya ordu için yeterli bir strateji aracı olabilmektedir. Orduların kapasitelerini de ölçmek bu yüzden bir o kadar zorlaşmaktadır.[33] Siber alandaki değişimin anlık olarak nasıl takip edildiği ve ordu düzeyinde nasıl programa alındığı bu hususta belirleyici

---

[32] İlk siber ordu, yıllar önce ABD tarafından gizli olarak kurulmuştur. ABD Savunma Bakanlığı siber uzayın kara, hava, deniz gibi yeni bir savaş alanı olduğunu doktrin olarak kabul etmektedir. ABD'de bu alandaki en önemli darboğazın bilgisayar güvenliği uzmanı sayısındaki yetersizlik olduğu vurgulanmaktadır. ABD, mevcut bir kaç bin kişi civarında olan uzman sayısını 20.000-30.000'e yükseltmek için gerekli eğitim programlarını uygulamaya almıştır.

[33] Hasan Çifçi, ***a.g.e.,*** s. 23.

olmaktadır. Özellikle siber orduların kapasitesi nasıl ve ne güçte olursa olsun, klasik anlamda savaş anlayışının ve orduların bilgi teknolojilerine bağımlı hale geldiği bir gerçektir. Komuta kontrol sistemleri, silah sistemleri, istihbarat, keşif ve gözetleme sistemleri ve savaş sistemleri gibi sistemlerin tamamı elektronik ortamda ve iletişim altyapısı üzerinde çalışmaktadır.[34]

Geniş bir şekilde, askerî kabiliyetlerin parçası olan sayısal ve elektronik ortamın korunması ve gerekli müdahalelerin yapılması adına atılacak adımlar, devletler adına nizami bir ordu oluşturulması açısından zorunluluk haline gelmiştir. Dünyada 100'den fazla askerî örgüt ve istihbarat birimi, çok sayıda birey, suç ve terör örgütü, bilgi sistemlerinden veri çalmaya ve bu bilgi sistemlerini çalışamaz hale getirme adına faaliyetlerini sürdürmektedir.[35]

Birçok devletin "beşinci muharebe alanı" olarak ilan edilen siber alanda güçlü olabilmek adına, siber ordular yanında, caydırıcılık gücünü artırmak için özel sektörle de iş birliği halinde olduğu gözlenmektedir. Bu devletlerin başında ABD gelmektedir. Siber orduları sadece nitelikli personel ile baş başa bırakmama arzusu içinde olan ABD gibi ülkeler, farklı çıkar konularında birleştikleri özel sektör güçleri ile ortak projelere imza atmakta ve ordularını takviye etmektedir. 2009 yılında ordu bünyesinde siber bir birim oluşturduğunu ilk açıklayan NATO üyesi olan Almanya, 76 kişi ile başlayan çalışma ve iş birliği gücünü,

---

[34] Ahmet K. Al-Rawi, "Cyber Warriors in the Middle East: The Case of the Syrian Electronic Army", ***Public Relations Review***, 2014, Vol: 40, 420-428, p. 421.

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

günümüzde 6000 kişilik bir siber ordu kapasitesine eriştirmiştir.[36] Siber savunmanın kapasitesi ve yöntemi açısından bir tercih halinden çıkıp zorunluluk haline gelen siber ordulara ilişkin yapılanmalar, ülkelerin gelişmişlik düzeyiyle ilgilidir; fakat başarısı ve sahip olduğu güç bu düzeyi geçersiz kılmaktadır.

2.2. Devlet Dışı Uluslararası Aktörler

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

Uluslararası politikanın analiz seviyesinde birey/grup ve uluslararası kuruluşlar düzeyinde analiz yapabilmek için siber saldırılar sonucunda tarafların kazançlarına ve kayıplarına ilişkin elimizde kesin veriler olması gerekmektedir.[37] Uluslararası politika analizlerinde, genel geçerliliği konusunda herkesin üzerinde anlaştığı genel, hatta kısmi bir teorik yaklaşımdan bahsetmek zaten güç bir husustur. Diğer taraftan, devletlerin kazanç sağlamaya çalıştığı siber müdahalelerde bu durum daha da güçleşecektir. Bu süreç, devlet dışı uluslararası aktörler olarak baskın bir şekilde illegal yapılanmaları ve manipülatif birimleri karşımıza çıkaracaktır.

---

[36] Minhaç Çelik, "Siber Ordu Kurmak için Devletler Özel Sektör ile Çalışıyor", ***TMMOB Bilgisayar Mühendisleri Odası Dergisi***, 2015, Sayı 5, 32-34, s.32.

[37] Analiz düzeyi sorununun uluslararası politika disiplini içerisinde bir inceleme başlığı olarak yer alması, farklı yaklaşımlarda dolaylı ve direkt olarak kimi çalışmalarda açıklığa kavuşturulmaya çalışılmıştır. Kenneth Waltz, ***Man, the State and the War: A Theoretical Analysis*** adlı çalışmasında savaşın sebeplerini, birey, devlet ve uluslararası sistem olmak üzere üç ayrı düzeyde analiz etmiştir. Özellikle birey ve devlet ilişkilendirilmesinde savaşın çehresinin değişimine ilişkin tespitler yakın dönemde birçok olaya ışık tutar niteliktedir. Bkz. Kenneth Waltz, ***Man, The State and The War: A Theoretical analysis***, Columbia University Press, New York, 1959.

2.2.1. Uluslararası İllegal Yapılanmalar

Aktör olarak illegal-yasadışı yapılanmaların varlığı ve uluslararası alandaki baskınlığı, devlet dışı gruplar olarak bir faaliyet alanı oluşturmuştur. Bilgisayar ve haberleşme teknolojileri alanında bilgi sahibi olan ve bu konularda ileri düzeyde beceriye sahip olan yapılanmalar, devletlerle ve kimi özel kuruluşlarla iş birliği halinde uluslararası sistemin aktörleri haline gelmiştir.[38]

Son dönemlerde yaşanan siyasi olaylarla birlikte farklı gruplar, gündemde adlarından sıkça söz ettirmeye başlamıştır. "*Anonymus*" gibi yapılanmaların faaliyetleri ve "*Wikileaks*" ile "Panama belgeleri"nin sızdırılmasına ilişkin olaylarda farklı grupların faaliyetleri ciddi yankı bulmuştur. Sıradan birine sorulduğu zaman bile akıllara gelebilecek "*RedHack*" ve "*Anonymus*" gibi grupların kendi içerisinde dahi kimi zaman bölünebildiği ve farklı olaylarla ilişkilendirildiği bilinmektedir.

Başta NATO olmak üzere uluslararası örgütlerin ve ABD gibi ülkelerin uluslararası illegal yapılarla mücadele ve eylem planlarına ilişkin söylemleri ve askerî açıdan attıkları adımları, mücadele alanı oluşturan aktörler açısından önemli bir yere sahiptir. Uluslararası yapılanmaların faaliyet alanı ve kapasitesi, bu önemi ve gerçekliği de gözler önüne sermektedir.

2.2.2. Manipülatif Birimler ve Söylemler

Son yıllarda siber güvenliğe ilişkin gelişmelerin en önemlileri arasında olan manipülatif söylemler ve bunların doğurduğu sonuçlar dikkat çekicidir. Endüstriyel sistemlerin güvenlik zafiyetinin daha fazla ortaya çıkmasının ardından kurumların sahip olduğu verilerin değiştirilerek geri dönülemez şekilde gerçekleştirilen saldırıların yaygınlaşması beklenmektedir. Özellikle devletlerin günümüzde kırılgan noktaları olan krizler ve krizleri doğuran olaylara ilişkin manipülatif söylemler ciddi maddi kayıplara da sebep olmaktadır.

---

[38] Roderic Broadhurst vd., "Organizations and Cyber Crime: An Analysis of the Nature of Groups Engaged in Cyber Crime", ***International Journal of Cyber Criminology***, 2014, 8(1), 1-20, s. 3.

Krizlerin gelişiminde siber saldırı araçları ve hizmetleri her geçen gün olağan bir hal almakta; herhangi bir organizasyona saldırmanın maliyeti önemli ölçüde düşmekte ve bu da birincil odak noktası olarak daha fazla sayıda saldırının yapılabilmesini sağlamaktadır. Devletlerin alana ilişkin verecekleri kararlar bu gelişme dâhilinde işlemektedir. Veriler bilinçli ya da bilinçsiz olarak manipüle edilirse, söz konusu kararlara ilişkin yanlış adımlar atılabilir ve zorlayıcı unsurlara da başvurulabilir. Kontrol sistemlerindeki ve üretim süreçlerindeki verilerin yanlış yorumlanması, yıkıcı sonuçlar doğurabilir.[39]

Devletleri ve sahip olduğu verilere ilişkin karar alıcıları zorlayabilecek, hatta etki altına alabilecek manipülatif gelişmeler, medyanın değişimiyle ve siber ortamdaki etkinliğiyle birlikte söylemler boyutuyla uluslararası arenayı zorlamaktadır. Sosyal ağlar ve siber ortam üzerinden etkinliğini artıran illegal yapılanmalar, manipülasyon ile kaos ortamı oluşturabilmekte ve hatta finansal krizlere neden olabilmektedir. Günümüzde siber ortam araçlarıyla uluslararası sisteme etki edebilecek ve toplumları etkileyebilecek bir algı operasyonunun varlığı her fırsatta dile getirilmektedir. Farklı terör yapılanmalarının da bu algı operasyonlarını kullandığı bilinmektedir. Bilişim teknolojilerinin en belirgin değişimi, devletlerin ciddi güvenlik sorunlarıyla karşı karşıya kalmasıdır.

2.3. Siber Savaşçılar

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

---

[39] Sanghamitra Nath, "What Military Deterrence can not Do, Cyber Deterrence can Do to Iran: Exploring the Implications of Manipulative Incessant Usage of the Term 'Pre-Emptive'", ***International Journal of Social Sciences and Humanity Studies***, 2012, 4(1), 313-323, p. 314.

bu düzlemdeki önemi ve varlığını da kabul etmiştir.[40]

Siber savaşların harekâtı yönünde ve kazanç elde edilebilmesinde, bireyler gerek yasal, gerekse yasa dışı yollarla farklı amaçlarla uluslararası arenada yer almaktadır. Özellikle siber anlamda harekâtların yürütülmesinde karşı tarafın olanakları ve kabiliyetleri tam olarak bilinemediği ya da tespit edilemediği için ortak hareket edilecek bireylerin veya grupların karakteristik özellikleri doğru tahlil edilmelidir. Bu grupları şu şekilde özetleyebiliriz:[41]

- Bilgisayar Korsanları: Yaptıkları saldırılar neticesinde hedef bilgisayardaki verileri okuyabilir, kopyalayabilir ve değiştirebilirler. Farklı topluluklar oluşturabilen bilgisayar korsanları, bireysel ve gruplar halinde çalışabilmektedir. Sürekli olarak işletim sistemlerinde, yazılımlarda ve internet teknolojilerinde açık arayan bilgisayar korsanları açık buldukları anda durumdan faydalanarak saldırılarını gerçekleştirebilmektedir.
  - Siyah Şapkalı Bilgisayar Korsanları: Kötü amaçlı olarak sistemlere sızan, genelde kişisel bilgileri ele geçirmek, tamamen yok etmek gibi saldırgan faaliyetler yürütenlerdir.
  - Gri Şapkalı Bilgisayar Korsanları: Sistemlere sadece merak amaçlı sızmakta, herhangi bir kötü amaç taşımamaktadır; fakat yine de yapılan suç teşkil edebilmektedir.
  - Beyaz Şapkalı Bilgisayar Korsanları: Siyah şapkalı bilgisayar korsanlarının yapacakları potansiyel tehditleri savuşturmakla yükümlüdür.

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

[41] Keleştemur, ***a.g.e.***, s. 209.

- Siber Casuslar: Siber casuslar aslında birer bilgisayar korsanı türevidir. Klasik istihbarat yöntemleri ve anlayışıyla hareket edip siber uzayda etkili olmaya çalışmaktadır. Siber casuslar sızdıkları sisteme zarar vermemekte ve bağlı oldukları yere hizmet etmektedir.
- Toplum Mühendisleri: Toplum mühendisleri ya da sosyal mühendisler olarak da bilinen kişiler, ileri seviyelerde psikoloji ve sosyoloji bilgisine sahiptir. Genellikle istihbarat servisleri tarafından tespit edilmiş kişilere yönelmektedirler. Toplum mühendisleri yazılımsal alandan daha çok insanlar üzerindeki açıklara yönelmektedir.
- Kripto Analizciler: Kriptografik sistemleri ve algoritmaları analiz etmekle görevlidir.
- Ağ ve Sistem Uzmanları: Bir kurum içinde tesis edilmiş olan ağ ve sistemlerin etkin ve sorunsuz çalışmasından sorumlu olan kişilerdir. Bu kişiler aynı zamanda herhangi bir problem olması durumunda problemin kaynağını tespit etme ve kısa sürede çözüm bulma özelliklerine sahiptir.

Siber savaşçılar konusunda en profesyonel girişimler geliştiren ülkelerin başında ABD gelmektedir. 2012 yılında bilgisayar korsanlarının ABD merkezli enerji şirketlerinin bazı kilit mekanizmalara girişi düzenleyen şifreleri elde etmek amacıyla saldırılar düzenlediği ortaya çıkmıştır.[42] Bilgisayar korsanlarının söz konusu şifrelerle hayati önem taşıyan endüstriyel altyapı sistemlerinin kontrolünü elde etmeyi amaçladığı belirlendikten sonra, bütçe planlarında ciddi bir değişiklik yapan ABD, siber savaşçı statüsünde istihdam edilen personel sayısını kademeli olarak artırma yoluna gitmiştir.

[42] Srisakdi Charmonman ve Chatpawee Trichachawanwong, "Training of Interdisciplinary Cyber Warriors", ***International Journal of the Computer, the Internet and Management***, 2014, 22(2), 7-12, p. 8.

Sonuç

Siber güvenlik ve uluslararası ilişkiler içerisindeki siber caydırıcılık kavramı, farklı aktörlerle birlikte gelişimini sürdürecektir. Bu gelişimin temelinde tehditlerle ilgili durumun ne yönde artacağını, devletlerin merkezinde yer aldığı uluslararası aktörler belirleyecektir. Özellikle siber güvenlik açısından farklı teorik yaklaşımların uluslararası ilişkiler içerisindeki boyutu tutarsızlaşmaya da başlamıştır. Bunun en önemli sebebi, siber alandaki saldırı ve savunma yeteneklerinin tam ve net bir şekilde tespit edilemeyişidir.

Siber alanda yaşanan atılımın politik düzeyi rasyonel bir şekilde kurgulanmamaktadır. Bireysel ve toplumsal beklentiler ve dalgalanmalar, siber güvenlik alanındaki strateji düzeyinde çoğu zaman belirleyici olabilmektedir. Strateji düzeyinde oluşturulacak ajandalar, bu alanda atılım yapmak isteyen aktörler adına kaçınılmaz gözükmektedir. Farklı aktörlerin yer aldığı siber alan uzun vadeli politikalarla desteklenmezse, veri kayıplarının olması ve ekonomik zararların hissedilmesi kaçınılmaz gözükmektedir.

Siber güvenlik ve siber güvenliğin özüne ilişkin çalışmaların varlık boyutu sadece uluslararası politika temelinde değerlendirilmemelidir. Akademik ve profesyonel düzlemde farklı alanlarda oluşmaya başlayan baskınlık, bir güç mücadelesine dönüşmüştür. Teknik alandaki gelişim ve baş döndürücü hız, devletleri karşı karşıya getirmekte ve ciddi bir veri trafiği oluşmaktadır. Disiplinler arası bir yön gösteren bu çeşitlilik, siber suç olgusunu beraberinde getirerek, uluslararası hukuk boyutunda bir farkındalığı oluşturmuştur.

Siber silahların, fiziksel etki doğuran silahlara göre sınıflandırılması sorunsalı ve devletlerin siber alanda gelişiminde caydırıcılık oluşturmasına ilişkin veriler, bir bütünlüğün oluşumunu zorlaştırmaktadır. Silahlanma yarışının siber alanda teknik bir boyutta geliştiği süreç, devletleri yeni bir savaş alanına iterek "siber savaşları" gerçekçi kılmaktadır. İç politikanın etkilenmesi ve oluşturulması konusunda "güvenlikleştirme kuramları" gibi yaklaşımlarla siber alanı açıklama isteği artar hale gelmiştir. Ulusal çıkarların tehdit algısına dönüştüğü siber savaş ortamı etkileşimi artırmıştır.

Siber savaş ortamındaki etkileşim, ekonomik açıdan yük getirmeyen zararlı yazılımların ortaya çıkışını ve nitelikli personelin tedariki hususundaki süreci hızlandırmıştır. Uluslararası güvenlik adına siber tehditler, güvenlikleştirme modeli açısından iç politikanın etkilenmesinde kendisine yer edinmeye başlamıştır. İç politikanın etkilenmesiyle ve ulusal çıkarın farklılaştırdığı tehdit algısıyla birlikte, siber caydırıcılık açısından dış politikada çıktılar üretilmektedir.

Summary

Being inherent of international relations, power struggle and conflicts maintain its alteration with its qualitative characteristics. One of the most important points of this alteration is cyber security and cyber deterrence area, which have some effects on international politics and which have been differentiated from power concept in this area.

Historical approaches and progress of international security have indicated that cyber security has some arguments at the level of international politics with the concepts like deterrence, war, and asymmetry. If we assumed that periodical conflicts are dealt with cyber attacks and alliances among the states, maximizing the interest of international actors could provide an important logical framework with regard to perspective of literature.

There are many different data sets for activating the relations among the states under the name of cyber struggle. With its dimension in international relations and apart from its interdisciplinary area, economic data of argued dimension have been assisted with different analysis at international politics. In this subject, some of the cyber politics and theoretical approaches with regard to regional characteristics reveal a necessity in terms of application area. Through the comparison of theoretical framework and data which have been dealt with coupling international alliances and interest groups, it is purposed for strengthening the research question of study. States as an important actor of international area and their interest dividedness have been focused with special approach for clarifying the problem of cyber conflicts.

Kaynakça

Kitaplar

ÇİFÇİ, Hasan, ***Her Yönüyle Siber Savaş***, TÜBİTAK Bilim Kitapları, Ankara, 2013.

KELEŞTEMUR Atalay, ***Siber İstihbarat***, Level Kitap, İstanbul, 2015.

ROSKIN, Michael G. ve O. BERRY, Nicholas, ***Uluslararası İlişkiler, Uİ'nin Yeni Dünyası***, çev. Özlem Şimşek, Adres Yayınları, Ankara, 2014.

SCHMITT Michael N., ***Talinn Manual on the International Law Applicable to Cyber Warfare***, Cambridge University Press, Cambridge, 2013.

SINGER, P.W. ve Friedman Allan, ***Siber Güvenlik ve Siber Savaş***, çev. Ali Atav, Buzdağı Yayınları, Ankara, 2015.

SÖNMEZOĞLU, Faruk, ***Uluslararası Politika ve Dış Politika Analizi***, Filiz Kitabevi, İstanbul, 2000.

WALTZ, Kenneth, ***Man, the State and the War: A Theoretical analysis***, Columbia University Press, New York, 1959.

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

Makaleler ve Kitap Bölümleri

AL-RAWI, Ahmet K., "Cyber Warriors in the Middle East: The Case of the Syrian Electronic Army", ***Public Relations Review***, 2014, Vol: 40, 420-428.

ALTUNOK, Taner ve Avcı, Engin, "Siber Tehditlerin Geleceği ve Alınması Gereken Önlemler", Haydar Çakmak ve Taner Altunok, (ed.), ***Suç, Terör ve Savaş Üçgeninde Siber Dünya***, Barış Platin Kitabevi, Ankara, 2009, 209-232.

ALTUNOK, Taner ve Kaya, Zeynep, "Siber Tehditlerle Mücadele", Haydar Çakmak ve Taner Altunok, (ed.), ***Suç, Terör ve Savaş Üçgeninde Siber Dünya***, Barış Platin Kitabevi, Ankara, 2009, 137-162.

BROADHURST, Roderic, vd., "Organizations and Cyber Crime: An Analysis of The Nature of Groups Engaged in Cyber Crime", ***International Journal of Cyber Criminology***, 2014, 8(1), 1-20.

CHARMONMAN, Srisakdi and Trichachawanwong, Chatpawee, "Training of Interdisciplinary Cyber Warriors", ***International Journal of the Computer, the Internet and Management***, 2014, 22(2), 7-12.

ÇELİK Minhaç, "Siber Ordu Kurmak için Devletler Özel Sektör ile Çalışıyor", ***TMMOB Bilgisayar Mühendisleri Odası Dergisi***, 2015, Sayı 5, 32-34.

ÇELİK, Şener, "Stuxnet Saldırısı ve ABD'nin Siber Savaş Stratejisi: Uluslararası Hukukta Kuvvet Kullanmaktan Kaçınma İlkesi Çerçevesinde Bir Değerlendirme", ***Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi***, 2013, 15(1), 137-175.

EKSTEDT Victoria, vd., "Commitments, Mechanisms & Governance", Alexander Klimburg, (ed.), ***National Cyber Security: Framework Manual***, NATO CCD COE Publication, Talinn, 2010, 146-190.

KLIMBURG, Alexander ve Healey, Jason, "Strategic Goals & Stakeholders", Alexander Klimburg, (ed.), ***National Cyber Security: Framework Manual***, Tallinn, NATO CCD COE Publication, Tallinn, 2012, 66-107.

NATH, Sanghamitra, "What Military Deterrence cannot Do, Cyber Deterrence can Do to Iran: Exploring the Implications of Manipulative Incessant Usage of the Term 'Pre-Emptive'", ***International Journal of Social Sciences and Humanity Studies***, 2012, 4(1), 313-323.

PETERSON, Dale, "Offensive Cyber Weapons: Construction, Development and Employment", ***Journal of Strategic Studies***, 2013, 36(1), 120-124.

VELLONE Luigi, "From Data to Knowledge: How Intelligence and Security Tools can Help", Fernando Duarte Carvalho ve Eduardo Mateus da Silva, (ed.), ***Cyberwar-Netwar: Security in the Information Age***, IOS Press, Amsterdam, 2006, 115-130.

Raporlar

BARNUM Sean, ***Standardizing Cyber Threat Intelligence Information with the Structured Threat Information eXpression (STIX)***, The Mitre Corporation, Version 1.1, Revision 1, 2014.

Kaspersky Lab., "Kaspersky Security Bulletin 2015", https://securelist.com/files/2015/12/Kaspersky-Security-Bulletin-2015_FINAL_EN.pdf, (Erişim tarihi: 28.07.2016).

McAfee Labs, ***Threats Report May 2015***, Santa Clara, 2015.

Ponemon Institute, ***2015 Cost of Cyber Crime Study: Global***, Ponemon Institute Research Report, Michigan, 2015.

İnternet Kaynakları

BAŞARAN Alper, "Verizon Bilgi Güvenliği Olayları Raporu", 4 Aralık 2014, http://securitist.blogspot.com.tr/2014/12/verizon-bilgi-guvenligi-olaylar-raporu.html, (Erişim Tarihi: 28.07.2017).

PIZZI, Michael, "Cyberwarfare greater threat to US than terrorism, say security experts", 7 Ocak 2014, Aljazeera America, http://america.aljazeera.com/articles/2014/1/7/defense-leaders-saycyberwarfaregreatestthreattous.html, (Erişim Tarihi: 12.06.2017).