SİBER UZAYDA GÜÇ VE SİBER SİLAH TEKNOLOJİLERİNİN KÜRESEL ETKİSİ*

Ersin ÇAHMUTOĞLU[1]

ÖZET

Teknolojinin gelişmesiyle birlikte ortaya çıkan tehditler ve imkanlar devletlerin ulusal güvenlik politikalarının güncellenmesine neden olmuştur. Aynı zamanda özel şirketlerin de üretim imkanlarını geliştirmiştir. Bu kapsamda siber uzayın kapsamının genişlemesiyle birlikte siber silah adı verilen yazılımların bir saldırı aracı olarak kullanılması söz konusu olmuştur. Etkileri bakımından ele alınan siber silahlar fiziksel zarar verme ve istihbarat amaçlı da kullanılmışlardır. Devletlerin güç kapasitesini artırma konusunda da siber silahlar önemli bir kuvvet çarpanı olmuştur. Genel manada bir saldırı aracı olan siber silahlar hem devletleri hem de birey ya da grupları hedef almıştır. Bu çalışmada söz konusu siber silahların etkileri, siber silah üreticilerinin ve büyüyen siber silah teknolojisi pazarının küresel anlamda önemi ve devletlerin bu konudaki tutumları incelenmiştir.
Anahtar Kelimeler: Devlet, Güç, İstihbarat, Siber Silah, Siber Uzay

THE POWER IN CYBERSPACE AND GLOBAL IMPACT OF CYBER WEAPON TECHNOLOGIES

ABSTRACT

Threats and opportunities that have emerged with the development of technology have caused to be updated national security policies of the states. At the same time, it has improved the production facilities of private companies. In this context, with the expansion of the scope of cyberspace, the use of software that called cyber weapons as an attack tool has been in question. In terms of their effects, cyber weapons were also used for physical damage and intelligence purposes. Cyber weapons have also been an important force multiplier on increasing the power capacity of the states. Cyber weapons, which are a means of attack tool in generally, targeted both the states and individuals or groups. In this study, the impacts of the cyber weapons in question, the global importance of cyber weapon manufacturers and the growing cyber weapon technology market and the attitudes of the states on this issue are examined.
Keywords: Cyberspace, Cyber weapon, Intelligence, State, Power

GİRİŞ

Uluslararası alanda realist perspektif açısından bakıldığında esas aktör olarak devletlerin ele alındığı varsayılırsa, güç konusunda mücadelelerin de yine devletler arasında olduğunu söylemek gerekmektedir. Devletlerin çıkarlarını korumak ve ulusal güvenliklerini sağlamaları amacıyla güç elde etmeleri bir ihtiyaç halini almaktadır. Böylece sürekli olarak gücü farklı unsurlarla elde etme konusunda da çalışmalar yapılmaktadır.

Güç kavramının siber uzayın gelişimi sonrası geldiği boyutun ele alındığı bu çalışmada esas olarak siber silah adı verilen yazılımsal saldırı ve savunma araçlarının güce

---

* Bu çalışma, Milli Savunma Üniversitesi, Atatürk Stratejik Araştırmalar Enstitüsü (ATASAREN), Strateji ve Güvenlik programı için hazırlanan *"Hibrit Savaşın Bir Boyutu Olarak Siber Saldırılar ve Türkiye'nin Durumu"* başlıklı yüksek lisans tezinden türetilmiştir.
[1] Milli Savunma Üniversitesi, Atatürk Stratejik Araştırmalar Enstitüsü (ATASAREN), Strateji ve Güvenlik Araştırmaları Bölümü Yüksek Lisans Öğrencisi, ersincmt@gmail.com, https://orcid.org/0000-0001-6105-3083
Makalenin Gönderilme Tarihi: *14 Ocak 2020* ***Kabul Tarihi:*** *15 Şubat 2020*

olan katkısı incelenmektedir. Daha çok siber uzayda güç elde etmeye odaklanan bu çalışmada siber silahların devletler açısından önemi ve küresel siber silah pazarının devlet dışı aktörleri olan küresel firmaların faaliyetleri de ele alınmaktadır.

Siber silahların mevcut durumu gösterir ki gelecekte siber silahlar konusunda bir belirsizlik hali olması muhtemeldir. Siber uzayda güçlenen aktörlerin saldırı amaçlı yazılımsal bir güce, yani siber silaha sahip olması başka aktörleri de rahatsız etmektedir. Siber silahların devlet dışı aktörlere satışının olup olmadığı konusundaki karmaşık bilgi yığının varlığı ise belirsizlikleri daha da artırmaktadır.

Bu çalışmada söz konusu belirsizliklerle birlikte siber silahların hem devletlere hem de birey veya gruplara olan etkileri incelenmektedir. Ayrıca siber silah türlerinin detaylıca ele alınıp fiziksel zarar veren, istihbarat amaçlı çalışan, birey veya grupları hedef alan ve çeşitli kurumları hedef alan siber silahlar şeklinde kategorizasyonu da söz konusudur. Bunlara değinmeden önce meselenin teorik kısmının da realist bakış açısıyla incelenmesiyle birlikte devletlerin tutumlarının neye göre şekillendiği ve siber uzayın ne tür katkılar sunduğu da ifade edilmektedir.

1. REEL-POLİTİK PARADİGMA AÇISINDAN GÜÇ KAVRAMI

Reel-politik paradigmanın temsilcilerinin tarihsel süreç içerisinde ifade ettiği görüşlerin, güvenlik kavramının teorik alt yapısını oluşturduğu bilinmektedir. Bu kapsamda realizm, güvenlik kavramını "kesintisiz/süregelen bir güvensizlik ortamı" gibi tanımlar üzerinden ifade etmektedir. Başka bir görüşe göre de güvenliği "tehdidin olmaması durumu" olarak açıklayınca, nihayetinde güvenlik kavramının reel-politik perspektifte güç, tehdit ve güvensizlik sözcükleri üzerinden değerlendirildiğini söylemek mümkündür. (Sandıklı & Emekliler, 2011, s. 6)

Realizm görüşünü savunanlar, özellikle de klasik realistler, sıkça kullandıkları ulusal güvenlik söylemi üzerinden anlaşılacağı gibi sadece devletlerin güvenliği konusunu incelemektedir. Onlara göre ulusal güvenlik konusu her şeyin üzerindedir ve *"high politics (birincil politika)"* olarak üst düzeyde tutulur. Geri kalan her şey *"low politics (ikincil politika)*" olarak değerlendirilir. Realistlere göre bu söz konusu birincil politika askeri güç ve güvenlik konusunu, ikincil politika ise ekonomi, kültür vb. konuları göz önünde tutmaktadır. (Sandıklı & Emekliler, 2011, s. 8)

Morgenthau, Machiavelli ve Hobbes gibi öncü isimlere dayanan klasik realizme göre güç konusu ise politikanın temel amacı olmaktadır. Devletler sürekli olarak güce ulaşma arzusunda hareket etmektedirler. Kenneth Waltz, John Mearsheimer gibi yazarların temsil ettiği neo-realizme göre ise uluslararası sistemin anarşik yapıda olmasından dolayı devletler de bundan etkilenmekte ve savunma amaçlı güç elde etme arayışında olmaktadırlar. Onlara göre de esas olan güç değil, güvenliktir. (Arı, 2011, s. 165) Dolayısıyla klasik realizm için öncelikli olan güç elde etmek iken neo-realizme göre öncelikli olan güvenliği sağlamaktır.

Realist görüşü savunanlar, uluslararası sistemin genellikle uluslararası düzeni oluşturan ve bunu sürdüren baskın güçlerle birlikte hiyerarşik olarak sıralandığını savunmaktadırlar. Böyle durumda aktörlerin güç yarışında olduğu ve sürekli bir tehdit algısının oluştuğu ortam, savaş riskinin en yüksek olduğu ortam olarak değerlendirilir.

1.1. Klasik Realizm ve Neo-realizm Açısından Güç

Uluslararası ilişkilerde daha çok askeri ve ekonomik alanda değerlendirilen güç kavramına kültürel ve siyasi alanlar gibi çeşitli unsurları içeren yeni yaklaşımlar söz

konusudur. Reel-politik perspektife göre temel aktör olarak devletlerin amacının varlığını sürdürebilmek olduğunu, bunu sağlayabilmek için de güç elde edilmesinin gerekli olduğunu yukarıda belirtmiştik.

Burada güç konusunda önemli bir ayrım söz konusu olmaktadır. Klasik realistlere göre güç elde etmek temel amaç, neo-realistlere göre ise sadece bir araçtır. Klasik realizme göre devletlerin anarşik yapıda olmaları, uluslararası sistemi de anarşik yapıya sürüklemekte ve bu anarşiden doğan kaos ve güvensiz ortamda da devletler daha fazla güce ulaşma arayışına girmektedirler. Çıkarların maksimize edildiği böyle bir ortamda her aktör self-help (kendi kendine yetme) olgusuyla karşı karşıya kalmaktadır. (Burchill, 2005, s. 225)

Yine klasik realizme göre güç kavramı askeri güç esas olmak üzere ekonomik güçle de açıklanırken, neo-realizme göre güç kavramı sadece askeri ya da ekonomik faktörleri değil, siyasi ve kültürel güç gibi "silah" niteliğinde tanımlanan faktörleri de içermelidir. (Mcclory, 2017) Güç kavramına farklı bakış açısıyla yaklaşan ve ilgili alanda önemli çalışmalar yapan Joseph S. Nye'a göre güç kavramının unsurları içerisindeki bütün bu faktörler soft power (yumuşak güç) ve hard power (sert güç) gibi kategorilerde değerlendirilmelidir. (Nye, 2011, s. 81)

1.2. Nye Perspektifinden Güç Kavramı ve Gücün Unsurları

Yumuşak güç kavramını ilk kez 1990 yılında kullanan Nye, ABD'nin Soğuk Savaş sonrası tek kutuplu dünyanın hegemonik gücünü nasıl yeniden kuracağı sorusu üzerine güç unsurlarının değiştiğine kanaat getirmiştir. (Nye, 2011, s. 125) Nye, bilgi ve iletişimin geliştiği bir çağda kültür, eğitim ve ticari faaliyetler gibi yumuşak güç unsurlarının, askeri ve ekonomik güç gibi sert güç unsurlarına nispeten daha etkili olacağına inanmaktadır.

Bunun ötesinde Nye, hem yumuşak hem de sert gücün eş zamanlı ve uygun bir şekilde kullanımının, ilgili aktörlere smart power (akıllı güç) kavramını da kazandırdığını ifade etmektedir. Nye'a göre akıllı güç, gerçek dünyadaki etkili stratejileri belirleyen sert ve yumuşak gücün etkili yollarla birleşimidir. Nye, insanların çoğunlukla sadece sert gücün yeterli olduğunu düşündüklerini, nadiren de yumuşak gücün kalpleri ve akılları kazanmaya yeterli olduğunu düşündüklerini ifade eder. Ancak ona göre gücün etkili olması için hem sert hem de yumuşak gücün bir kombinasyonunu kullanmanız gerekmektedir. (Gavel, 2008)

Son olarak Nye, özellikle bilgi devrimi sonrası ortaya çıkan imkanlardan dolayı gücün dönüşüm geçirmesiyle birlikte karşımıza çıkan yeni bir tür olarak cyberpower (siber güç) kavramını da önemli bir unsur olarak ifade etmektedir. Nye'a göre siber güç, siber uzayda asimetrik savaş yöntemleriyle sınırlı fırsatlar açarak devletler arasında bazı güç kaymalarına neden olabilmektedir. (Nye, 2010, s. 19)

Nye'a göre siber uzayda bir devletin, başka bir devletin vatandaşlarında cazibe meydana getirecek bir yumuşak güç oluşturma imkanı bulması da söz konusudur. İnternet ve özellikle sosyal medya üzerinden yürütülen kamu diplomasisi kampanyası buna bir örnektir. Bununla birlikte siber uzay, herhangi bir ülkedeki fiziksel hedeflere zarar verebilecek sert bir güç kaynağı olarak da kullanılabilir. Örnek vermek gerekirse; birçok modern endüstri kuruluşu, diğer deyişle sanayi sektörünün modern işletmecileri, tesislerindeki üretim veya denetleme sistemlerine bağlı olan ve bilgisayarlar tarafından kontrol edilen özel işletim sistemlerine sahiptir. Bu sistemlere yönelik yapılacak bir siber saldırı, sistemin yok olmasına ve bunun yanında çevreye olası zararlar verilmesine neden olabilmektedir. Sonuç olarak siber uzayın kullanıcısına sunduğu imkanlar, hem sert hem de yumuşak güç kaynakları sağlayabilir.

Burada kullanıcıların hem devlet, hem devlet dışı aktör, hem de teröristler gibi suç örgütlerinden oluşabileceği göz önünde tutulmalıdır. (Nye, 2010, s. 6)

Bilgi çağında, devlet dışı aktörlerin geleneksel olmayan güce sahip olması, devletlerin esas aktör olarak kabul edilmesi önerisine meydan okumaktadır. Devlet dışı aktörler, Nye'ın güç dağılımı teorisinde savunduğu gibi uluslararası ilişkilerde giderek daha fazla önem kazanmaktadır. Bu durum, özellikle bireysel suçluların, örgütlerin ve terörist grupların, devletlerin egemenliğini tehdit etmek için internetin erişilebilirliğinden yararlanabileceği bir siber ortamı da oluşturmaktadır.

2. SİBER UZAY VE SİBER GÜÇ

Uluslararası sistemde birçok devlet ve devlet dışı aktör, geçmişten günümüze gelişen teknolojilerin neden olduğu tehdit ve imkanlardan dolayı ulusal güvenlik kapsamındaki politikalarını yeniden belirlemektedir. Özellikle son yıllarda, internetin kullanım alanının yaygınlaşmasıyla birlikte gelişen siber uzayın yeni harp sahası olarak değerlendirilmesi söz konusudur. Kara, deniz, hava ve uzaydan sonra siber uzayın da savaşlarda kuvvet çarpanı olarak etki göstermesi ve harbin beşinci boyutu (Bayraktar, 2014, s. 122) olarak nitelendirilen söz konusu siber alanın kapsamının genişlemesiyle birlikte devletlerin ve devlet dışı aktörlerin elde ettiği ya da etmek istediği güç unsurları çeşitlenmektedir.

Siber uzay konusu da burada öne çıkmaktadır. Devletlerin güç elde etme amacıyla girişimde bulunduğu faaliyetlere siber uzayda güçlenme arzusu da eklenmiştir. Siber uzayda güç konusuna girmeden önce siber uzay kavramına değinmek, konunun daha iyi anlaşılması bakımından önem arz etmektedir.

2.1. Siber Uzay Kavramı

Siber uzay kavramının ilk olarak 1982 yılında bilim kurgu yazarı William Gibson'ın *Neuromancer* adlı romanında kullanıldığı ve sibernetik ve uzay kelimelerinin bir araya getirilmesi ile elde edildiği belirtilmektedir. Gibson'ın siber uzayı "insanlık sistemindeki her bir bilgisayardan alınan verilerin grafik gösterimi, tasavvur edilemez karmaşa, verilerin küme ve takım yıldızları" gibi ifadelerle tanımladığı söylenmektedir. (P. W. Singer, 2015, s. 28)

Siber ortam ya da siber alan olarak da anılan siber uzay esasında bir bilgi ortamı olarak nitelendirilebilir. Siber uzay, bilgilerin oluşturulduğu, saklandığı ve paylaşıldığı çevrimiçi bilgisayar ağlarının yer aldığı, diğer bir deyişle dijital verilerin oluşturduğu alem olarak da tanımlanmaktadır. (P. W. Singer, 2015, s. 29) Devletler ve devlet dışı uluslararası aktörler de bu konuda çeşitli tanımlar yapmıştır.

ABD Savunma Bakanlığı'na göre siber uzay, *"internet, telekomünikasyon ağları, bilgisayar sistemleri ve gömülü işlemciler dahil olmak üzere, birbirine bağlı bilgi teknolojisi altyapı ağlarını ve dijital verilerini içeren küresel bir alandır."* (U.S. Deparment of Defense, 2013) Avrupa Birliği (AB) tarafından yapılan tanımlamaya göre siber uzay, *"bir telekomünikasyon ağı yoluyla uzaktan da erişilebilen nesneler arasındaki bağlantılar ve ilişkiler kümesi"*ni ifade etmektedir. (ENISA, 2015, s. 30) NATO'nun tanımına göre siber uzay, *"bilgisayar ağlarını kullanarak veri depolamak, değiştirmek ve iletmek suretiyle bilgi sistemleri arasında fiziksel ve fiziksel olmayan bileşenlerin oluşturduğu çevre"* olarak ifade edilebilmektedir. (Schmitt, 2013, s. 211) Türkiye Cumhuriyeti'nin yaptığı tanıma göre ise siber uzay, *"tüm dünyaya ve uzaya yayılmış durumda bulunan bilişim sistemlerinden ve bunları birbirine bağlayan ağlardan oluşan veya bağımsız bilgi sistemlerinden oluşan sayısal ortam"* şeklinde tanımlanmaktadır. (UAB, 2016, s. 7)

Görüldüğü üzere siber uzay konusunda alanında uzman isimlerin yanında ABD, AB ve NATO gibi uluslararası aktörler de farklı tanımlamalar yapmaktadır. Bu durum, siber uzay konusunda net bir tanımın olmadığının göstergesidir. Siber uzay ve dolayısıyla bu kavramdan türeyen diğer tüm tanımlar konusunda değişkenlikler bulunmaktadır. Özetle, uluslararası alanda kabul görmüş genel bir tanıma sahip olmayan siber uzayı, *"bilgi sistemlerinin birbiriyle ve diğer unsurlarla etkileşim içinde olduğu alan"* olarak tanımlamak mümkündür.

Siber uzay ile birlikte siber güç, siber savaş, siber güvenlik, gibi çeşitli kavramlar da hem devletler hem de devlet dışı aktörler tarafından dikkatle incelenmektedir. Bu tür kavramlarla birlikte siber uzaydaki tehdit unsurlarının neden olduğu güvenlik problemleri de üzerinde durulan önemli konulardandır.

2.2. Bir Tehdit ve Güç Unsuru Olarak Siber Uzay

Devletlerin ve devlet dışı aktörlerin ulusal güvenlik çalışmalarında tehdit değerlendirmeleri artık yeni dönemde teknolojik gelişmelerle birlikte ele alınmaktadır. Bu teknolojik gelişmelerin getirdiği en büyük risk de siber uzay alanında olmaktadır. Kara, deniz, hava ve uzaydan sonra, özellikle askeri anlamda operasyonel saha olarak tanımlanan alanlara eklemlenen siber uzay, birçok tehdit aktörü için kullanışlı bir araç olmaktadır. Böylece devletler ve devlet dışı aktörler, tehditlere karşı daha etkili/kapsamlı savunma stratejileri uygulamak için bu aracı da kullanmak istemektedirler. (Brantly, 2018, s. 23)

Siber uzayın getirdiği teknolojik imkanlara sahip olan devletler ya da devlet dışı aktörler, askeri güç kapasitelerine yeni bir kuvvet çarpanı eklemektedirler. Bilgisayar ürünü olan yazılımlar aracılığıyla dünyanın herhangi bir noktasına erişim imkanı söz konusu devletleri ve devlet dışı aktörleri defansif (savunmacı) ya da ofansif (saldırgan) bir siber aktör yapabilmektedir. (Brantly, 2018, s. 36)

Bu tür imkanlara sahip olan devletleri de Nye'ın tanımından yola çıkarak siber güç şeklinde nitelendirmek mümkündür. Nye tarafından davranışsal olarak tanımlanan siber güç, siber uzayın elektronik olarak birbirine bağlı bilgi kaynaklarının (ağlar, yazılımlar dahil) kullanımı suretiyle arzu edilen sonuçları elde etme yeteneğidir. Nye'a göre siber gücün içinde de yumuşak güç ve sert güç unsurları yer almaktadır.

Siber uzayın içinde yer alan bilgi araçları (propaganda, enformasyon aygıtları), siber alanda cazibe oluşturma ya da ikna etme amaçlı yumuşak güç üretmek için kullanılabilmektedir. Aynı şekilde siber kaynaklar, siber uzay içinde sert güç de üretebilmektedir. Örneğin, devletler veya devlet dışı aktörler, bir şirketin veya devletin internet sistemine bağlı cihazlarına ve altyapılarına fiziksel hasar verme amaçlı siber saldırı yapabilmektedir. (Nye, 2010, s. 9) Özetle siber güç, kullanım amacına ve yöntemine göre hem sert hem de yumuşak güç olarak değerlendirilmektedir.

Nye'a göre ulusal güvenliği sağlamak devletlerin klasik bir işlevidir ve pek çok devlet, siber uzayda egemenliklerini genişletmeyi ve bunu yapmak için de gelişmiş teknolojik araçlara sahip olmak istemektedir. Siber güce sahip olan devlet ya da devlet dışı bir aktör, kendi imkanlarıyla oluşturduğu ya da başka kaynaklardan temin ettiği siber güç kapasitesiyle diğer aktörler için tehdit olabilmektedir. Sistemde yer alan her bir aktör, güç kapasitesini (özellikle de askeri güç) artıran diğer aktörü bir tehdit unsuru olarak algılaması sonucu kendi güç kapasitesini de artırma yoluna gidecektir. Realizm teorisinde ifade edilen security dilemma (güvenlik ikilemi) kavramı burada karşımıza çıkmaktadır. (Arı, 2011, s. 192)

Realist görüşün savunduğu kötü olan insan doğasının bencil ve çıkarcı bir tutumla güç elde etme arzusunda olması, bir tehdit unsuru olarak diğer aktörleri de etkilemekte ve oluşan güvensizlik ortamıyla bir güvenlik ikilemi ortaya çıkmaktadır. Siber uzayda güç elde etme arzusu da yine bu kapsamda değerlendirilmelidir. Bütün bu güç elde etme yarışı ve tehdit algılamalarından doğan güvenlik problemleri, aktörler arasında siber çatışma ortamını hatta siber savaşa giden yolu da hazırlamaktadır. Bu durumda aktörler siber saldırı aracı olarak çeşitli unsurlar ve yöntemler kullanmaktadır. Bunlardan en önemli olanları da siber silah olarak nitelendirilen spesifik siber saldırı araçlarıdır.

3. SİBER SALDIRILAR VE SİBER SİLAH KAVRAMI

Siber uzay, devletler ya da devlet dışı aktörler için hem bir tehdit hem de bir güç kaynağı olabilmektedir. Siber uzayın imkanlarını kullanan devletler teknolojik güç kapasitelerini geliştirirken aynı zamanda siber uzayda var olan bütün tehditlerle de yüzleşmek zorundadır. Bu tehditler de genel anlamda siber saldırılar olarak karşımıza çıkmaktadır.

Tanım itibariyle bir siber saldırı, bir Bilgi Teknolojisi (BT) sistemi aracılığıyla, doğrudan ya da dolaylı olarak başka bir BT sistemini veya ağını zarara uğratma, engelleme veya istismar etme amacıyla yapılan eylemlerin tümü olarak nitelendirilebilir. Burada istismar etme tabiri, hedeften veri elde etme veya veriyi manipüle etme anlamında siber casusluk faaliyeti kapsamında kullanılmıştır. Bir başka tanıma göre ise siber saldırı, siber uzayda yer alan bütün bilgileri ve sistemleri bozmak, değiştirmek ya da istismar etmek suretiyle gerçekleştirilen eylemlerdir. (Çifci, 2012, s. 6)

Bir BT sistemine veya ağına karşı saldırgan eylemler temel olarak iki şekilde gerçekleşebilmektedir. Yukarıdaki tanımda bahsettiğimiz gibi birinci yol siber saldırı, ikinci yol da siber istismar olarak ifade edilebilir. Bir siber saldırı, hedef BT sistemlerini ve ağlarını veya bu sistemlerde bulunan ya da bu sistemlerden geçiş yapan bilgi ve programları değiştirmek, bozmak veya yok etmek için uygulanan kasıtlı eylemler olarak da tanımlanmaktadır. Siber istismar ise bilgi/veri elde etmek için siber uzaydaki birtakım teknik işlemlerin kullanılmasıyla gerçekleşmektedir. (Schreier, 2015, s. 85) Özetle, bir siber saldırı sadece hedefe zarar vermek amacıyla kuvvet uygulamak anlamına gelmemektedir. Bunlara ilave olarak casusluk faaliyetleri de bu kapsamda değerlendirilmelidir.

Siber casusluk eylemleri olarak da niteleyebileceğimiz bazı siber saldırıların, genellikle gizli yürütülmesi ve elde edilmesi istenen verinin mümkün olduğunca hedef tarafından fark edilmeden gerçekleştirilmesi beklenir. Siber saldırı ve siber istismar arasındaki temel teknik farkın, yürütülecek işlemin niteliğinden ibaret olduğunu ifade etmek mümkündür. Bir siber saldırı eylemi yıkıcı ve ciddi zarar verici bir eylem olabilir ama bir siber istismar eylemi, hedefte herhangi bir tahribata neden olmadan bilgi veya istihbarat elde etme amaçlı gerçekleştirilir. (Schreier, 2015, s. 49)

Buraya kadar, siber saldırının ne olduğu konusunda bilgi vermeye çalıştık. Bu noktadan sonra tarihsel olarak siber saldırıların nasıl gerçekleştiğini ve günümüze kadar var olan siber saldırı türlerinin ne olduğunu da anlatmak gerekmektedir.

Siber saldırı türlerine geçmeden önce literatürde kimi zaman bir yazılım olarak ifade edilse de nitelik olarak bir *cyber weapon* (siber silah) etkisi gösteren eylemlerden de bahsetmek gerekmektedir. Genel olarak siber silahlar, siber uzaydaki sistemleri ve bilgileri etkileyen, bozan veya tahrip eden yazılımlara veya yöntemlere verilen isimdir. (Çifci, 2012, s. 168)

3.1. Siber Silah Teknolojileri ve Genel Tartışmalar

Siber silah kavramı, esasında siber saldırı aracı olarak tercih edilen yazılımı ya da bir saldırı aracını nitelendirmek için kullanılmaktadır. Fakat burada basit yapıda bir yazılım ya da saldırı aracından değil de gelişmiş tekniklerle üretilmiş, spesifik amaçları olan ve karmaşık yapıya sahip bir yazılım ve saldırı aracından bahsedildiğinin altını çizmek gerekmektedir. Silah kavramına bakınca da bunun genellikle bir saldırı veya savunma aracı olarak tanımlandığı ve insanları öldürmek, yaralamak veya bir hizmeti devre dışı bırakmak, mülke zarar vermek, hedefi imha etmek için tasarlanmış bir araç olarak nitelendirildiği görülmektedir. (Smeets, 2018, s. 9)

Bu tanım, geleneksel silahları tanımlamaktadır ancak siber silah için bir belirsizlik söz konusudur. Çünkü bir siber silahın bileşenleri içinde yer alacak kötü amaçlı yazılımların çoğu, insanları öldürmek, yaralamak veya mülke zarar vermek veya yok etmek için tasarlanmamıştır. Sadece istihbarat toplama ya da veri elde etme amacıyla hedef sistemde çalışması için üretilen yazılımlar da mevcuttur. (Arimatsu, 2012, s. 97) Görüldüğü üzere, siber silah konusunda bir tanımlama problemi vardır ve kavramsal açıdan geleneksel silah kavramından farklı bir yaklaşımla yeni bir tanımlamaya ihtiyaç duyulmaktadır.

Yapı itibariyle bir siber silah, kimilerince balistik füzeye benzetilmektedir. Buna göre bir füze üç temel unsurdan oluşur: iletim aracı, yani roket motoru, hedefe nasıl ulaşacağını söyleyen bir navigasyon sistemi ve hasar verici bileşenler. Aynı üç unsurun, bir siber silahın içinde de var olduğu ifade edilmektedir. (Schreier, 2015, s. 66) Bir füzenin yükü, bir tür patlayıcı ile dolu olan savaş başlığıdır. Bir siber silahta ise yük, hedeften verileri kopyalayan, değiştiren, işleyen ve harici bir kaynağa gönderen bir yazılım olabilir. Aynı şekilde bir siber silah, uzaktan erişim sağlayan ve tek seferde kullanım amaçlı salt kalıcı hasar vermeye odaklı bir yazılım olarak da çalışabilmektedir. (Thomas Rid, 2012, s. 7)

Görüldüğü üzere siber silahlar, tanım itibariyle belirsizliğe sahip olmasına rağmen siber güvenlik çalışmalarında kabul görmüş bir kavram olarak karşımıza çıkmaktadır. Elbette konvansiyonel silahlar, ileri seviyede gelişmiş silahlar, nükleer başlık taşıyan füzeler gibi silah teknolojileri konusunda yapılan yasal düzenlemeler, siber silahlar konusunda henüz bir tartışma ortamı oluşturmamıştır. Ancak yine de siber silahların üretimi, dağılımı ve kullanımına dair bir kontrol mekanizmasına gerek olup olmadığına dair çalışmalar da ihtimal dahilindedir. (Denning, 2000, s. 47)

Siber uzayda başvurulan siber silahların karmaşık ve sofistike olduğunu söylemek mümkündür. Devletlerin bu konuda yatırım amaçlı siber uzayı kullanmaları ve siber silah kapasitelerini geliştirmeleri, esas olarak siber uzayın silahlandırılması ve askerileştirilmesi gibi bir kavramı da öne çıkarmaktadır. (Darıcılı, 2018, s. 321) Böylece siber tehditlerin çok boyutlu hale gelmesi ve siber silahların sürekli gelişim göstermesi önemli küresel güvenlik problemlerinden biri olmaktadır.

Burada ele alınan siber silahlar, hedefe kalıcı hasar verme kapasitesi olan ve özel hayatın gizliliğini ihlal eden casus yazılımları içermektedir. Bunlara ilaveten savunma amaçlı, saldırı amaçlı ve her iki amaca hizmet eden siber silahlar olarak üç farklı kategoride değerlendirmeler de yapılmaktadır. Devletler ve özel şirketler bu silahların üretiminde yasal düzenlemelerden ziyade ticari ve güvenlik temelli konuları göz önünde bulundurmaktadır. (Denning, 2000, s. 48) Böylece yapılan değerlendirmeler sonucunda devletlerin karşı karşıya kaldığı siber silah tehditlerinin esas olarak iki farklı türde ele alındığını, bunların da amaçlarına göre belirlendiğini söyleyebiliriz.

3.2. Siber Silah Türleri ve Hedef Odaklı Saldırılar

Siber silahların, üretim ve nihayetinde kullanım amaçlarına göre iki farklı türde ele alınması mümkündür. Birincisi, fiziksel zarar verme amaçlı üretilen silahlar ki bunlar daha çok kritik altyapıları (enerji, ulaşım, doğal kaynaklar gibi) ve devletlerin sistemlerini hedef almaktadır. İkincisi ise zarar vermekten ziyade istihbarat amaçlı veri toplama, gözetleme ve teknik takip amaçlı üretilmektedir. İstihbarat amaçlı üretilen siber silahlar devletlerden devlet dışı aktörlere, organizasyonlardan bireylere kadar çok daha geniş kitleleri hedefleyen silahlardır.

Yukarıda da bahsettiğimiz gibi siber silah olarak adlandırabileceğimiz yazılım ve programların özellikle son 10 yılda gözle görülür bir yükseliş eğiliminde olduğunu belirtmek gerekmektedir. Gerek doğrudan devlet eliyle, gerekse özel şirketler tarafından üretilen siber silahlar dünyada yeni bir tehdit unsuru olarak göze çarpmaktadır. Bir bilgi teknolojisi ürünü üzerinden küresel alanda herhangi bir hedeften veri toplanması veya bir hedefe zarar verilmesi kapasitesinin günden güne artması, durumun ciddiyetini ortaya koymaktadır. Bu çerçevede siber silah türlerini kurumları hedef alan ve birey ve grupları hedef alanlar olmak üzere iki şekilde incelemek mümkündür.

3.2.1. Kurumları Hedef Alan Siber Silahlar

Kurumları hedef alan siber saldırı operasyonlarının hem fiziksel zarar verme hem de istihbarat elde etme amaçlı olduğunu söylemek mümkündür. Fiziksel zarar veren siber silahların daha çok devletler tarafından kullanılması, istihbarat amaçlı üretilen siber silahların ise devlet, şirket ayrımı gözetmeden geniş bir kullanıcı kitlesine hitap etmesi söz konusudur. Her ne kadar üreticiler bu tür araçları sadece devletlere sattıklarını iddia etseler de devlet dışı bir aktörün bunları elde edip etmediği konusunda herhangi bir net bilgi bulunmamaktadır.

Fiziksel zarar veren ve istihbarat amaçlı çalışan siber silah türlerini incelerken, öncelikle literatürde ve güvenlik raporlarında en çok ele alınan örnekleri değerlendireceğiz. Daha sonra ise özel hedef olan birey ve gruplara karşı kullanılan siber silahlara kısaca değineceğiz.

a) Stuxnet

Stuxnet, endüstriyel kontrol sistemlerini hedefleyen ve çalışma düzenlerini sabote eden ilk siber silah tehdidi olarak bilinmektedir. İran'ın nükleer program kapsamında inşa ettiği Natanz'daki nükleer tesise yönelik uzun bir süredir siber saldırı gerçekleştiren ve 2010 yılında tespit edilen Stuxnet silahı, nükleer santrifüjlerin hasara uğramasına neden olmuştur. Devlet destekli bir operasyon kapsamında yürütülen Stuxnet saldırısının sadece İran'ı hedef aldığı bilinmektedir.

Stuxnet vakası, siber silahlar arasında makalelere, dergilere, haber ve çeşitli yayınlara en çok konu olan hedef odaklı saldırıdır. Bugün bilindiği kadarıyla Stuxnet operasyonu, Kasım 2005'te ilgili sistemdeki C&C (komuta ve kontrol) sunucularının incelenmesi sonucu kısmen fark edilmiştir. Ancak burada sadece anormal bir işleyişin varlığı söz konusudur. Bu tehdidin mekanizması ve işlevleriyle ilgili kapsamlı tespit işlemleri ise bundan 5 yıl sonra, yani Temmuz 2010'da yapılmıştır. Bu durumun nedeni, Stuxnet solucanının kendisini bu zamana kadar gizlemeyi başarmasının altında yatmaktadır. Stuxnet solucanı sıradan bir solucan ya da virüsten farklı olarak spesifik amaçlı oluşturulmuştur ve yalnızca Siemens Step-7 sistemini hedef almıştır.

Stuxnet, kendisini hedefe bulaştırmak ve operasyona başlamak için birkaç farklı güvenlik açığı kullanan sofistike bir kötü amaçlı yazılım olarak bilinmektedir. Solucanın en muhtemel sızma yöntemi ise USB flash bellek, diğer adıyla taşınabilir bellekler aracılığıyla hedefe etki etmesi olarak değerlendirilmektedir. Solucan, internetten izole edilmiş, dışarıdan girilmesi mümkün olmayan ağlara da bulaşmıştır. İşin nihayetinde, Stuxnet solucanı 155 ülkede 40.000'den fazla cihaza (bilgisayarlar da dahil) sızdığı tespit edilmiştir. Stuxnet operasyonunun arkasında ABD, İsrail ve Hollanda'nın olduğu düşünülmektedir. (Wueest, 2014, s. 11)

b) Night Dragon

Stuxnet'ten sonra 2009'da üretilip yayıldığı düşünülen Night Dragon, daha çok küresel petrol ve enerji şirketlerine karşı koordine edilmiş bir silah olarak nitelendirilmektedir. Bazı kamu kurumlarını da hedef alan bu saldırı çoğunlukla Windows işletim sistemlerindeki birtakım güvenlik açıklarından yararlanmak suretiyle gerçekleşiyordu.

Güvenlik araştırmacılarının Night Dragon olarak adlandırdığı bu gelişmiş saldırı yönteminde kullanılan araçların, tekniklerin ve ağ faaliyetlerinin Çin Halk Cumhuriyeti (ÇHC) kaynaklı olarak belirlendiği ifade edilmektedir. Kullanılan saldırı araçlarının Windows oturum açma isteklerini engelleyen ve kullanıcı adlarını ve parolaları ele geçiren araçlar olduğu tespit edilmiştir. (McAfee, 2011, s. 3)

c) Flame (Flamer/SkyWiper)

2010 yılında aktif olan ve 2012 yılında SkyWiper adıyla tespit edilen Flame ya da Flamer, Stuxnet'e benzeyen fakat çok daha karmaşık ve güçlü bir siber silah olarak nitelendirilmektedir. Karmaşık bir yazılım olarak Flame, belirli bir aktör tarafından değil birden fazla aktörün dahil olması sonucu oluşmuştur. Bu sebeple bugüne kadar tespit edilen en komplike yazılım olarak ifade edilmektedir.

Ayrıca Flame'in birçok bileşeninin zararlı yazılım değil faydalı yazılım olarak sistemlerde çalıştığı da belirtilmektedir. Stuxnet'ten farklı olarak hedefe zarar verme değil, hedeften bilgi çalma amaçlı oluşturulmuştur. İlk olarak İran'da keşfedilen bu silah, Doğu Avrupa ve Ortadoğu ülkelerinde de tespit edilmiştir. Çoğunlukla devlet kurumlarını hedef alan Flame'in kaynağı hakkında net bir bilgi elde edilememiştir ancak tıpkı Stuxnet gibi devlet destekli bir operasyon kapsamında yürütüldüğüne dair kanıtlar mevcuttur. (sKyWIper Analysis Team, 2012, s. 8)

d) Duqu

2010 yılında çalışmaya başlayan Duqu, tıpkı diğer siber silahlar gibi belirli bir süre sonra, 2011 yılında tespit edilmiştir. Stuxnet ve Flame yazılımlarının bir benzerini içerdiği belirtilen Duqu'nun Stuxnet'i oluşturan tehdit aktörleri tarafından veya Stuxnet'in kaynak koduna erişimi olanlar tarafından yazıldığı tespit edilmiştir.

Duqu'nun Stuxnet'ten farklı olarak amacının, hedef sistemden veri elde etmek, bilgi çalmak olduğu ifade edilmektedir. Ayrıca diğer amacının da gelecekte başka bir üçüncü tarafa karşı daha kolay bir saldırı gerçekleştirmek için endüstriyel altyapı ve sistem üreticileri gibi kuruluşlardan istihbarat verilerini ve varlıkları toplamak olduğu belirtilmektedir. Duqu'nun Avrupa ve Ortadoğu'daki yaklaşık 12 ülkeden çeşitli organizasyonları hedef aldığı bilinmektedir ve tıpkı Stuxnet ve Flame gibi devlet destekli bir operasyon kapsamında kullanıldığına dair iddialar söz konusudur. (Symantec, 2011, s. 3)

e) Gauss

Gauss, 2011'de tespit edilmiş siber silah araçlarından biridir. Flame ile benzer yapıda bileşenlere sahip olan Gauss'un, bilinmeyen bir saldırı aracı taşıyan Trojan (Truva atı) olarak çalıştığı ve devlet destekli bir operasyon kapsamında yürütüldüğü tespit edilmiştir. Gauss, Stuxnet, Flame ve Duqu'nun aksine kurumları veya belirli bir sektörü hedeflememiş, spesifik anlamda belirli şahısları üst düzey bir siber casusluk operasyonu kapsamında hedeflemiştir. Bunu da ilgili hedefin sisteminden veri çalma yoluyla yapmıştır. Gauss'un Stuxnet, Duqu ve Flame'i üreten aynı aktörler tarafından oluşturulduğuna dair önemli kanıtların olduğu da bilinmektedir.

Gauss'un Windows sistemlerinden çeşitli verileri çalmanın yanı sıra, bazı sistemlerde etkinleşen bilinmeyen şifrelenmiş bir yük de içerdiği görülmüştür. Tıpkı Duqu'nun Stuxnet platformuna dayandığı gibi, Gauss'un da Flame platformuna dayandığı söylenmektedir. Toplamda 2,500'den fazla sisteme bulaştığı tespit edilen Gauss'un çoğunlukla Ortadoğu ülkelerini hedef aldığı teknik dokümanlarda belirtilmiştir. (GReAT - Kaspersky Lab, 2018, s. 48)

f) Shamoon

2012 yılında, son derece yıkıcı etkiye sahip bir siber saldırı olarak değerlendirilen Shamoon, Suudi Arabistan'ın en büyük petrol rafinerisinde yaklaşık 30.000 bilgisayarı etkilemiştir. W32.Disttrack olarak da bilinen bu saldırıda kullanılan kötü amaçlı yazılım, diğer tüm siber silahlara göre farklı bir çalışma mantığına sahiptir. Buna göre Shamoon, öncelikle sızdığı sistemde gerekli tüm dosyaları oluşturmakta, eski dosyaları silmekte ve son olarak gerekli verileri yöneticiye gizlice iletmektedir ve bu süreç tespit edilmeden aylarca sürmüştür. Shamoon son olarak işlemleri bitirince sızdığı sistemde bozulmalara ve kesintilere neden olmaktadır.

Stuxnet, Duqu ve Flame gibi silahlara nazaran Shamoon'un halen aktif olarak çalıştığı düşünülmektedir. Çünkü 2016 yılında ve 2018 yılında Orta Doğu'daki hedeflere karşı yeni bir saldırı dalgasıyla Shamoon yeniden tespit edilmişti. Bu son iki Shamoon saldırıları ilk varyanta göre daha etkili saldırılar olarak değerlendirilmektedir. (Security Response Attack Investigation Team, 2018)

g) Duqu 2.0

2015 yılında tespit edilen Duqu 2.0 operasyonunun, tıpkı önceki Duqu silahında olduğu gibi aynı aktör tarafından detaylıca planlanmış bir operasyon olduğu keşfedildi. Devlet destekli bir kampanya olan Duqu 2.0'nin temel amacı, sızdığı sistemdeki kritik verileri çalmaktı. Saldırının benzersiz olduğu ve daha önce görülmemiş bazı özellikler içerdiği, ayrıca operasyon sonunda da neredeyse hiç iz bırakmadığı ifade edilmektedir. Hedefin ise İran'ın nükleer programını gözetlemek ve istismar etmek olduğu tespit edilmiştir. (GReAT, 2015, s. 9)

Duqu 2.0'nin diğer hedefleri arasında bazı Avrupa, Ortadoğu ve Asya ülkelerinin de bulunduğu belirtilmektedir. En dikkat çeken ayrıntı, hedeflerden bazılarının İran'la nükleer anlaşma konusuna ilişkin müzakereler yürüten P5 + 1 (Birleşmiş Milletlerin 5 daimi üyeleri ve ek olarak Almanya) aktörlerinin olduğudur. Duqu 2.0'nin arkasındaki tehdit aktörünün, bu nükleer program konusunda üst düzeyde gerçekleşen görüşmelerdeki mekanlara saldırılar başlattığı tespit edilmiştir. Siber casusluk amaçlı yapılan bu saldırının etkileri hakkında henüz detaylı bir sonuç elde edilememiştir. (GReAT, 2015, s. 46)

Buraya kadar bahsedilen siber silahlar hem fiziksel zarar verme hem de istihbarat amaçlı üretilen ve kullanılan siber silahlar olarak nitelendirilmektedir. Elbette bunların dışında daha onlarca siber silah olarak nitelendirilebilecek saldırılar ve operasyonlar da vardır ancak burada ele alınanlar en çok konuşulan ve güçlü etkiye sahip olan silahlardır. Geri kalanlar ise bir operasyon kapsamında gerçekleştirilen ve çoğunlukla birey ve grupları hedef alan saldırılardır. İstihbarat amaçlı çalışan yazılımlar, hizmet engelleme, ağ trafiğini dinleme gibi saldırılar da yine bu kapsamda değerlendirilmektedir.

3.2.2. Birey ve Grupları Hedef Alan Siber Silahlar

Özellikle son on yıl içerisinde spesifik olarak üretilmiş siber silahlar mevcuttur. Bunlar daha çok devlet destekli olarak üretilen silahlardır ve gözetleme, teknik takip ve veri elde etme gibi amaçlara hizmet etmektedir. Bu tarz silahları genellikle devletler değil, özel şirketler ya da belirli finans kurumları altındaki paravan şirketler üretmektedir. Bu ürünleri doğrudan siber silah olarak tanımlayanların yanında silahlandırılmış yazılımlar olarak tanımlayanlar da mevcuttur. Gerçek şu ki böylesi siber silahların hiçbiri savunma amaçlı değildir. Her biri, yapısı itibariyle sadece saldırı odaklı çalışmaktadır.

Söz konusu şirketler/firmalar, bu siber silahları bir çözüm ya da araç olarak nitelendirmekte ve sadece terörizmi veya kritik suçları önleme amacıyla devletlerin istihbarat servislerine ve kolluk kuvvetlerine sattıklarını iddia etmektedirler. Ancak bugüne kadar karşılaşılan olaylara bakıldığında gerçeklerin daha farklı olduğunu söylemek mümkündür. Zira bu araçlar sadece terör örgütü üyelerini ya da kriminal suçluları değil, gazeteci, politikacı ve muhalif gruplardan tanınmış ya da sıradan çok sayıda isimleri de hedef almıştır. (Marczak, Hacking Team's U.S. Nexus, 2014)

Bu kapsamda bilinen siber silahları maddeler halinde incelemek mümkündür. Ancak her birinin üreticisi ve menşei farklı da olsa bu silahlar genellikle aynı yapıda olup aynı nitelikte çalışmaktadırlar. Ayrıca bütün bunların aynı amaç doğrultusunda kullanımı da söz konusu olduğundan detaylara girmeden kısaca bahsetmek daha uygun olacaktır. Buna ek olarak adı geçen bütün siber silahlar hakkında elde edilen bilgilerin bazı spesifik kaynaklardan ve Wikileaks veya çeşitli hacker grupları tarafından sızdırılmış resmi dokümanlardan sağlandığını da belirtmek gerekmektedir.

İlk olarak 2011 yılındaki Wikileaks sızıntılarından sonra adı en çok duyulan İtalyan Hacking Team firmasından ve ürünlerinden bahsetmek mümkündür. Hacking Team'in iki amiral gemisi olarak nitelendirilen *Galileo* (Hacking Team, 2013) ve *Da Vinci* (Hacking Team, 2012 (Revision 1.1)), temel olarak birbirine muadil siber silahlardır fakat Galileo'nun da Vinci'den daha güncel ve gelişmiş yapıda olduğunu belirtmek gerekmektedir. Uzaktan kontrol sistemi olarak çalışan ve her türlü veriyi elde etme kapasitesine sahip bu siber silahların, daha sonraki dönemlerde başka firmalar tarafından üretilen siber silahlar için örnek ürünler olduğu söylenebilir.

Hacking Team firmasının bu iki ürün dışında başka ürünlerinin de olduğu tahmin edilmektedir ancak incelenen dokümanlara göre aktif kullanımda olan başka ürün mevcut değildir. Milan merkezli Hacking Team'in, Avrupa'da ve Ortadoğu'da birçok devletin kolluk kuvvetlerine ve istihbarat servislerine milyon dolarlarca değeri olan bu siber silah sistemlerini satarak aslında küresel siber silah endüstrisinin önemli yapı taşlarını oluşturduğu söylenebilir.

2019 yılına kadar faaliyet gösteren Hacking Team, skandal olaylar sonrasında değer kaybedince satıldı ve aylar sonra yeni bir isimle ortaya çıktı. Memento Labs adını alan yeni oluşum, kendisini hibrit savaş ortamında çözüm üreten bir siber istihbarat şirketi olarak

tanıtmakta ve Hacking Team'den daha etkili siber silahlar üreterek (RCS X ve KRAIT gibi) sektörde etkili olmaktadır. (O'Neill, 2019)

Siber silah şirketlerine ek olarak Fransız Amesys (yeni adıyla Nexa Technologies) firmasının *CasperT* (Amesys, 2009) ve *Eagle GLINT* (Amesys, 2009) ürünleri, İngiliz Gamma Group'un *FinFisher* (GammaGroup, 2010) ürünü ve son günlerde çok konuşulan İsrailli NSO Group'un *Pegasus* (NSO Group, 2014) adlı ürünü aynı amaca hizmet eden ve aynı niteliğe sahip olan casus yazılım ve gözetim araçlarına örnektir. Burada Pegasus isminin dünyada son zamanlarda daha çok konuşulduğunu belirtmek gerekmektedir. Pegasus'un geçtiğimiz aylarda WhatsApp'ta yer alan bir güvenlik açığını istismar etmesi sonrası başlayan tartışmalara ek olarak İstanbul'daki Suudi Arabistan başkonsolosluğunda öldürülen gazeteci Cemal Kaşıkçı'nın da bu siber silahın hedefi olduğunun ortaya çıkması, meselenin önemini ortaya koymaktadır. (Albabwa, 2019)

Anılan siber silahlara ek olarak dünya çapında yüzlerce siber silahın farklı adlarla üretildiğini ve satıldığını söylemek de mümkündür. Örneğin sadece İsrail'e ait 30'a yakın firma olduğu ve bunların aynı amaçla küresel pazara ürün sundukları çeşitli kaynaklarca tespit edilmiştir. (Privacy International, 2016, s. 23) İsrail burada önemli bir aktör olarak öne çıkmaktadır. Genellikle Kıbrıs ve Bulgaristan'ın üs olarak seçildiği İsrail devlet destekli WiSpear gibi firmalar, sahip oldukları milyon dolarlık cihaz, teknolojik donanım ve yazılımlarla sektörde önemli yer edinmektedir. Adı geçen bütün teknolojiler ve araçlar, genellikle birey ve grupları hedef alarak istihbarat toplama ve teknik takip uygulama amacıyla çalışmaktadır ve genellikle aynı işlem kapasitesine sahiptir.

Bütün bu siber silah sistemlerinin sadece yazılımdan ibaret olmadığını da belirtmek gerekmektedir. İlgili firmalar tarafından donanımsal bir yapının (özel bir ağ bağlantısı ve bilgisayar donanımı) da yazılıma dahil olarak müşterilere (devletlere) sunulduğu bilinmektedir. Bunlara ilaveten yine ilgili firma tarafından eğitim ve danışmanlık hizmetinin de bulunduğu periyodik bir ticari süreç söz konusudur.

Söz konusu siber silahların sızma yöntemi ise çoğu zaman dört farklı biçimde olmaktadır. En çok kullanılan yöntem ağ üzerinden sızma şeklindedir. Diğer yöntemler ise kısa mesaj (SMS), zararlı yazılım içeren bağlantılar/dokümanlar/uygulamalar, cihazlardaki zafiyetleri istismar ederek sızma ve fiziksel erişim ile sızma şeklindedir.

Bu araçların hedeflediği sistemleri de Pegasus örneğinden yola çıkarak ifade etmek mümkündür. Pegasus ve diğer siber silahların çoğunluğu, her türden Windows, Apple ve Linux gibi bilgisayar sistemi ve yine her türden Android, iOS, BlackBerry ve Symbian gibi akıllı telefon sistemi üzerinde çalışma kabiliyetine sahiplerdir. Elde ettikleri verilerin ise herhangi bir sınırı bulunmamaktadır ve çağrılar, konuşmalar, alınan/gönderilen mesajlar, anlık mesajlaşma uygulamalarındaki konuşmalar (uçtan uca şifreleme ile çalışan WhatsApp dahil), kamera, mikrofon, ekran görüntüsü, ağ trafiği izleme, cihaz teknik bilgileri, depolama, rehber, konum, adres ve kişi bilgileri gibi elde edilebilecek bütün verilere ulaşıp bunları ilgili kullanıcıya ulaştırmaktadırlar. (NSO Group, 2014, s. 14-20)

Neredeyse bütün casus yazılımlar, üreticileri tarafından bir kritik istihbarat-misyon sistemi olarak nitelendirilmektedir. Bu yazılımlar, diğer deyişle siber silahlar, sızdıkları telefon ya da bilgisayarlarda fark edilmeden gizlice çalışarak (en güçlü güvenlik duvarları ve anti virüs programlarını baypas ederek) elde edilmek istenen amaca ulaşıldıktan sonra iz bırakmadan kendi kendilerini imha etmektedirler.

Bunların dışında, özellikle otoriter rejimlerde, belirli bir şirket tarafından üretilmeyip tamamen devlet destekli üretilen araçlar da mevcuttur. Burada ÇHC ve Birleşik Arap Emirlikleri (BAE) örneği öne çıkmaktadır. Bir grup araştırmacı tarafından yapılan tespitlere göre Tibet-Uygur bölgesindeki önemli şahıslara yönelik Çin rejimi tarafından siber casusluk operasyonu yürütülmüştür. Poison Carp adı verilen casus yazılım ilgili hedeflere akıllı telefonlar üzerinden bulaşıp, sonrasında teknik takip ve gözetleme amaçlı çalışarak operasyon yürütmektedir. (Citizen Lab, 2019)

Diğer taraftan BAE rejimi, ülke genelinde WhatsApp gibi uygulamaları yasaklarken kendi ürünleri olan ToTok uygulamasını kullanıma sunmuştur. Milyonlarca kullanıcıya sahip bu uygulamanın aslında bir sohbet programı olarak hizmet vermesinden öte BAE rejimine casusluk yapan bir uygulama olduğu tespit edilmiştir. Teknik analizlere ve uygulamayı üreten şirketin bağlantılarına dair yapılan soruşturmalara göre ToTok uygulaması dolaylı yoldan BAE istihbarat servisine bağlı olarak çalışmaktadır. (Marczak, 2020)

Görüldüğü üzere siber silah türlerinin hem fiziksel hasar verebilmesi hem de istihbarat operasyonları çerçevesinde veri elde etmek ya da teknik takip amaçlı kullanılabilmesi mümkün olmaktadır. Hem devletlerin hem de devlet dışı aktörlerin bu tarz siber silahları üreterek ya da diğer aktörlerden satın alarak ulusal güvenlik ya da ulusal çıkarlar çerçevesinde silahlanmaları söz konusudur.

Uluslararası aktör olarak nitelendirilebilen küresel şirketler, tamamen yasal çerçevede ve sadece devletlerin istihbarat servisleri ve kolluk kuvvetlerine hizmet sunmak amaçlı bu siber silahları ürettiklerini iddia etmektedirler. Yukarıda bahsedilen şirketler dışında dünya çapında daha ismi haberlere konu olmayan yüzlerce siber silah üreten şirketin var olduğu tahmin edilmektedir. Bu durum uluslararası alanda hem devletler hem de devlet dışı aktörler açısından önem arz etmektedir.

SONUÇ

Siber uzayın imkanlarının gelişmesiyle birlikte devletler ulusal güvenlik politikalarını bu kapsamda güncellemektedirler. Güvenliğini sağlamak isteyen devletler güç konusunda yatırımlarını geliştirerek siber uzayda güç elde etme amaçlı çalışmalar yürütmektedir. Buradan hareketle siber savunma ve siber saldırı kapasitelerini güçlendirerek siber silah teknolojilerine de yatırım yapmaktadırlar.

Siber silahların son on yıldan bu yana yükseliş eğiliminde olmasıyla devletlerin çıkarları gereği bu teknolojiye başvurması ve dolayısıyla küresel siber silah pazarının büyümesi ihtimal dahilindedir. Sadece devletler değil, devlet dışı aktörlerin de bu kapsamda güç elde etmeleri mümkündür. Her ne kadar ilgili firmalar ürünlerini yalnızca devletlere sattıklarını ifade etseler de bu silahların bir başka aktör tarafından da elde edilebileceğini söylemek mümkündür. Nitekim sızdırılan dokümanlar bunu açık bir şekilde göstermektedir.

Uluslararası alanda özellikle devletlerin güç yarışında olması durumunda aktörler birbirine karşı en iyi seçeneği değerlendirecektir. Mevcut teknolojinin getirdiği yenilik ve imkanlar da bu seçeneklerden biridir. Düşük maliyet, hızlı çözüm ve pratik kullanımlarından dolayı siber silahların söz konusu güç elde etme yarışında önemli bir kuvvet çarpanı olacağını aşikardır. Ancak burada devletlerin dışında bireyleri ve sivil toplumu da ilgilendiren önemli bir sorun ortaya çıkmaktadır.

Özel hayatın gizliliği ve hak ihlalleri konusunda siber silahların dünyada oluşturduğu kötü algı halen devam etmektedir. Siber silahların bir savunma aracı olmasından öte saldırı

aracı olarak kullanılması sonucu kimi devletler otoriter ve baskıcı rejim anlayışıyla herhangi bir terör ya da kritik suçlarla iltisaklı olmayan kişi veya grupları da hedef alabilmektedir. Nitekim Cemal Kaşıkçı'nın öldürülmesi sürecinde en yakın arkadaşının bir siber silahla hedef alınması ve Kaşıkçı'nın akıllı telefonunun da bu istismardan etkilenmesi örnek teşkil etmektedir. Buradan hareketle siber silahların tıpkı diğer silahlarda olduğu gibi yasal bir çerçeve ile denetlenmesi mümkün olmasa da bu konuda bir çalışma yürütülmesi ihtimal dâhilindedir.

KAYNAKÇA

Tek Yazarlı Kitaplar

Arı, T. (2011). *Uluslararası İlişkiler Teorileri - Çatışma, Hegemonya, İşbirliği.* Bursa: MKM Yayıncılık.

Burchill, S. (2005). *Theories of International Relations* (Third Edition b.). New York: Palgrave Macmillan.

Çifci, H. (2012). *Her Yönüyle Siber Savaş* (2. Basım b.). Ankara: TÜBİTAK.

Nye, J. S. (2011). *The Future of Power.* New York: Public Affairs.

Çok Yazarlı Kitaplar

Darıcılı, A.B. (2018). Askerileştirilen ve Silahlandırılan Siber Uzay. Acaravcı, Ali içinde, *Sosyal ve Beşeri Bilimlere Dair Araştırma Örnekleri* (s. 311-327). Ankara: NOBEL Akademik Yayıncılık

P. W. Singer, A. F. (2015). *Siber Güvenlik ve Siber Savaş.* (A. Atav, Çev.) Ankara: Buzdağı Yayınevi.

Dergi Makaleleri

Bayraktar, G. (2014). Harbin Beşinci Boyutunun Yeni Gereksinimi: Siber İstihbarat. *Güvenlik Stratejileri Dergisi, 10*(20).

Denning, D. (2000). Reflections on Cyberweapons Controls. *Computer Security Journal, 16*(4).

Smeets, M. (2018). A Matter of Time: On the Transitory Nature of Cyberweapons. *Journal of Strategic Studies, 41*(1).

Rid, T, McBurney P. (2012). Cyber-Weapons. *The RUSI Journal, 157*(1).

Konferans & Kongre Bildirileri

Arimatsu, L. (2012). A Treaty for Governing Cyber Weapons: Potential Benefits Practical Limitations. *4th International Conference on Cyber Conflict.* Tallinn: NATO CCDCOE Publications.

Brantly, A. F. (2018). The Cyber Deterrence Problem. *10th International Conference on Cyber Conflict - CyCon X.* Tallinn: NATO CCDCOE Publications.

Sandıklı, A., & Emekliler, B. (2011). Güvenlik Yaklaşımlarında Değişim ve Dönüşüm. *Uluslararası Balkan Kongresi: 21. Yüzyılda Uluslararası Örgütlerin Güvenlik Yaklaşımları ve Balkanların Güvenliği* (s. 8). Kocaeli: Kocaeli Üniversitesi.

İnternet Kaynakları

Albabwa. (2019, January 1). *Khashoggi's Phone Was Hacked by Saudi Regime - Friend*. Albabwa News: https://www.albawaba.com/news/khashoggi-phone-was-hacked-saudi-regime-friend-1237872 adresinden alınmıştır

Citizen Lab. (2019, September 24). *Missing Link: Tibetan Groups Targeted with 1-Click Mobile Exploits*. Citizen Lab - Targeted Threats: https://citizenlab.ca/2019/09/poison-carp-tibetan-groups-targeted-with-1-click-mobile-exploits/ adresinden alınmıştır

ENISA. (2015, December). *Definition of Cybersecurity.* European Union Agency for Network and Information Security: https://www.enisa.europa.eu/publications/definition-of-cybersecurity adresinden alınmıştır

Gavel, D. (2008). *Harvard Kennedy School Insight Interview*. Belfer Center: https://www.belfercenter.org/publication/joseph-nye-smart-power adresinden alınmıştır

GReAT - Kaspersky Lab. (2018, March). *Gauss: Abnormal Distribution.* Kaspersky Lab: https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/20134940/kaspersky-lab-gauss.pdf adresinden alınmıştır

GReAT. (2015, June). *The Duqu 2.0 - Technical Details.* Kaspersky Lab: https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07205202/The_Mystery_of_Duqu_2_0_a_sophisticated_cyberespionage_actor_returns.pdf adresinden alınmıştır

Marczak, B. (2014, February 28). *Hacking Team's U.S. Nexus*. Citizen Lab: https://citizenlab.ca/2014/02/hacking-teams-us-nexus adresinden alınmıştır

Marczak, B. (2019). https://medium.com/@billmarczak/how-tahnoon-bin-zayed-hid-totok-in-plain-sight-group-42-breej-4e6c06c93ba6 adresinden alınmıştır

Marczak, B. (2020, January 3). *A BREEJ TO FAR: How Abu Dhabi's Spy Sheikh hid his Chat App in Plain Sight*. Medium: https://medium.com/@billmarczak/how-tahnoon-bin-zayed-hid-totok-in-plain-sight-group-42-breej-4e6c06c93ba6 adresinden alınmıştır

McAfee. (2011, February). *Global Energy Cyberattacks: Night Dragon.* McAfee Labs White Paper: https://www.mcafee.com/wp-content/uploads/2011/02/McAfee_NightDragon_wp_draft_to_customersv1-1.pdf adresinden alınmıştır

O'Neill, P. H. (2019). *The Fall and Rise of a Spyware Empire*. MIT Technology Review: https://www.technologyreview.com/s/614767/the-fall-and-rise-of-a-spyware-empire/ adresinden alınmıştır

Security Response Attack Investigation Team, T. I. (2018, December). *Shamoon: Destructive Threat Re-Emerges with New Sting in its Tail*. Symantec - Threat Intelligence: https://www.symantec.com/blogs/threat-intelligence/shamoon-destructive-threat-re-emerges-new-sting-its-tail adresinden alınmıştır

sKyWIper Analysis Team. (2012, May). *sKyWIper (a.k.a Flame a.k.a Flamer): A Complex Malware for Targeted Attacks.* Crysys: https://www.crysys.hu/publications/files/skywiper.pdf adresinden alınmıştır

U.S. Deparment of Defense. (2013, February 5). *Cyberspace Operations.* https://fas.org/irp/doddir/dod/jp3_12r.pdf adresinden alınmıştır

UAB. (2016). *2016-2019 Ulusal Siber Güvenlik Stratejisi.* T.C. Ulaştırma ve Altyapı Bakanlığı Haberleşme Genel Müdürlüğü: https://hgm.uab.gov.tr/uploads/pages/siber-guvenlik/2016-2019guvenlik.pdf adresinden alınmıştır

Rapor

Mcclory, J. (2017). *Soft Power of 30 - A Global Ranking of Soft Power 2017.* Portland: USC Center on Public Diplomacy .

Nye, J. S. (2010). *Cyber Power.* Belfer Center: https://www.belfercenter.org/sites/default/files/legacy/files/cyber-power.pdf adresinden alınmıştır

Privacy International. (2016). *The Global Surveillance Industry.* Privacy International.

Schmitt, M. N. (2013). *Tallinn Manual on The International Law Applicable to Cyber Warfare.* NATO Cooperative Cyber Defence Center of Excellence: http://csef.ru/media/articles/3990/3990.pdf adresinden alınmıştır

Schreier, F. (2015). *On Cyberwarfare.* The Geneva Centre for the Democratic Control of Armed Forces - DCAF.

Symantec. (2011). *W32.Duqu: The Precursor to the Next Stuxnet.* V. 1.4. Symantec Security Response.

Wueest, C. (2014). *Targeted Attacks the Energy Sector.* Symantec Security Response.

Diğer

Amesys. (2009). CasperT. *System Presentation - Manual Document*.

Amesys. (2009). EagleGLINT. *Operator Manual*.

GammaGroup. (2010). FinFisher. *Governmental IT Intrusion and Remote Monitoring Solutions*.

Hacking Team. (2012 (Revision 1.1)). Remote Control System . *Da Vinci Whitepaper*.

Hacking Team. (2013). RCS Galileo. *Advanced Training Manual*.

NSO Group. (2014). Pegasus. *Product Description*.

THE POWER IN CYBERSPACE AND GLOBAL IMPACT OF CYBER WEAPON TECHNOLOGIES

From the perspective of the realist perspective, it is assumed that states are considered as the main actors in the international arena, it is necessary to say that the struggles about power are also among the states. It becomes a need for states to gain power in order to protect

their interests and ensure their national security. At this point, the importance of cyber weapons has been the topic of discussion. The point where the cyber weapons come from shows that there is an uncertainty about what the cyber weapons will be in the future. The fact that actors growing in cyber space have a software power for attack, namely cyber weapon, annoys other actors. In the international system, many state and non-state actors are re-determine their national security policies due to threats and possibilities caused by technologies developing from past to present. Especially in recent years, cyberspace with widespread uses of the internet is considered as a new warfare zone. Besides cyberspace, various concepts such as cyber power, cyber warfare, cyber security are also carefully reviewed by both states and non-state actors. Along with such concepts, security incidents caused by threat actors in cyberspace are also important issues.

It is necessary to state that in cyber weapons have a noticeable upward trend especially in the last ten years. These cyber weapons produced either directly by the state or by private companies stands out as a new threat to the world. Increasing the capacity of collecting data from any target or damaging a target by an information technology product globally reveals the severity of the situation. In this context, it is possible to examine cyber weapons in the form of types of cyber weapons targeting institutions and individuals or groups. It is possible to say that cyber attack operations targeting institutions are for both physical damage (such as Stuxnet) and intelligence (such as Duqu, Flame etc.).

As for cyber weapons targeting individuals or groups, these are mostly state-sponsored weapons and serve purposes such as surveillance, technical tracking, and data acquisition. Such weapons are usually produced by private companies under certain financial institutions, not the states. Examples are companies such as the Italian Hacking Team, the Israeli NSO Group, and the French Amesys. Apart from these cyber weapon technologies, especially in authoritarian regimes, there are also cyber weapon tools that are not manufactured by any company, but are manufactured by the state. Here, the People's Republic of China (PRC) and the United Arab Emirates (UAE) examples stands out.

As can be seen, it is possible for cyber weapons types to both physically damage and acquistion data within the framework of intelligence operations or to be used for technical tracking and spying. Both states and non-state actors have armed within the framework of national security or national interests by producing such cyber weapons or purchasing them from other actors. With the development of the possibilities of cyberspace, many states are updating their national security policies within this scope.

The states that want to ensure their national security are working on obtaining power in cyberspace by improving their investments in military power. Based on this, they also invest in cyber weapons technologies by strengthening their cyber defense and cyber attack capabilities. As cyber weapons have been on the rise since the last decade, it is likely that states will obtain to this technology in scop with their interests and thus the global cyber weapons market will grow. It is possible that not only states but also non-state actors can obtain power in this context. Although the mentioned companies state that they only sell their products to the states, it is possible to say that these weapons also can be obtained by another actor. As a matter of fact, the leaked documents clearly show this.