World Journal of Human Sciences, 2020 - 2
Dünya İnsan Bilimleri Dergisi, 2020 – 2
ISSN: 2717-6665

Bilişim Çağında Siber Saldırılar Ve Yeniden Bloklaşma

Orhan KURUDAL [12]

ÖZET

21. yüzyılın, iletişim ve bilişim çağına dönüşmesiyle birlikte internet her alanda kendini göstermekte ve her kesimden insan tarafından etkin bir şekilde kullanılmaktadır. Bu kullanım; bireylerin, kurumların ve devletlerin işlerini kolaylaştırmaktadır. Ancak internetin bu güzel yönünün ardında bir de olumsuz yönü olan siber saldırılar ve siber savaşlar bulunmaktadır. Siber saldırıları, hem bireyler hem örgütler hem de devletler yapabilmektedir. Makalede, bireylerin ve örgütlerin yaptığı saldırılardan ziyade devletlerin diğer devletlere karşı yaptığı siber saldırılar ele alınmaktadır. Bu bağlamda devletlerarası yapılan siber saldırılar, vaka incelemesine tabi tutulacak, soğuk savaş dönemindeki batı ve doğu blokunun benzeri bir bloklaşmanın yeniden oluştuğu gösterilmeye çalışılacaktır. Bu çalışmada önce kısa şekilde; soğuk savaş dönemi bloklaşması, devletlerin neden bloklaştığı sorusunun cevabına, siber saldırıların oluştuğu yer olan internet, siber saldırı, siber savaş ve siber güvenlik konularına değinilecektir. Ardından da, yeniden oluşan doğu - batı bloklaşmasını göstermek amacıyla, Rusya'nın – Estonya, Gürcistan, Hollanda, Ukrayna ve NATO'ya karşı, ABD'nin – İran' a karşı ve Çin Halk Cumhuriyeti'nin – Avrupa Birliği, Avustralya ve ABD'ye karşı yaptığı siber saldırılar analiz edilmektedir. Makalede amaç, bu saldırıların sebep sonuç ilişkisini irdelemek değil; Avrupa ve Rusya arasındaki soğuk rüzgârların estiği bu dönemde yeniden oluşan doğu – batı bloklaşmasının siber saldırılarla daha net bir şekilde ortaya çıktığını göstermektir.

Anahtar Kelimeler: Bloklaşma, Siber Saldırı, Amerika Birleşik Devletleri, Rusya, Çin Halk Cumhuriyeti.

[12] Orhan KURUDAL, Kırşehir Ahi Evran Üniversitesi Yüksek Lisans Öğrencisi, Kırşehir Ahi Evran Üniversitesi, Uluslararası İlişkiler Anabilim Dalı Merkez/Kırşehir, orhkrdl40@gmail.com

World Journal of Human Sciences, 2020 - 2
Dünya İnsan Bilimleri Dergisi, 2020 – 2
ISSN: 2717-6665

Cyber Attacks in the Information Age

And Re-block

ABSTARCT

With the transformation of the 21st century into the age of communication and information, the Internet shows itself in every area and is used effectively by people in every segment. this use facilitates the work of individuals, institutions and governments. Hovvever, behind this beautiful aspect of the internet, there are cyber attacks and cyber wars, which also have a negative aspect. Cyber attacks can be done by individuals, organizations or States. We are going to deal with cyber attacks which are done between States rather than the individuals or organizations. In this context, cyber attacks betvveen States will be subjected to case study and it will be tried to be shown that a blocking similar to the western and eastern bloc in the cold war era is reconstructed. In this study, firstly, it will be discussed that the cold war era blocking, the answer of the question of why States are blocking, the internet where cyber attacks occur, cyber attack, cyber warfare and cyber security. And then, to demonstrate the re-emerging east-west bloc, we will analyze the cyber attacks of Russia against Estonia, Georgia, the Netherlands, Ukraine and NATO, the USA against Iran and People's Republic of China against the European Union, Australia and the USA. Our aim here is not to examine the cause and affect relatinship of these attacks, but to Show that eastern and western bloc that re-emerged in this period when Europe and Russia have a tense relationship appeared more clearly with cyber attacks.

Keywords: Block, Cyber Attack, United States of America, Russia, People's Republic of China.

GİRİŞ

Bloklaşma; devletlerin var olan güçlerini korumak ya da anarşik uluslararası sistemde var olabilmek amacıyla siyasi, kültürel, ekonomik, ideolojik ve jeopolitik açıdan kendini yakın hissettiği bir başka devlet veya devletlerle kurdukları ittifaktır. Özellikle bloklaşma; Soğuk Savaş döneminde, Doğu-Batı Bloku şeklinde net biçimde görülmektedir. İki kutuplu sistemin var olduğu bu düzende, devletler kendi güvenlikleri için bu bloklardan birini seçmek durumunda kalmışlardır. Soğuk Savaş sonrası dönemde, bu bloklaşma ortadan kalkmış gibi görünmektedir. Ancak gelişen internet teknolojisi ile yeni bir âlem olan siber uzay hayatımıza girmiş ve devlet altyapıları bu âlemde dizayn edilmeye başlanmıştır. Fakat bu dizayn ile devletlerin yapısında yeni açıklar oluşmaya başlamış ve bu açıklar kullanılarak o devlete zarar verilmek istenmektedir. Bu bağlamda; reel ortamda gerçekleştirilen saldırının, siber otama aktarılması ile siber saldırılar ortaya çıkmıştır.

Siber saldırı; internet bağı kullanılarak siber ortamda, bireylerin, örgütlerin ya da devletlerin, diğer birey, örgüt ya da devletlere karşı gerçekleştirilen, bilgi çalmak, istihbarat sağlamak ya da elektronik aletlere zarar vermek için yaptıkları saldırılardır. Bu tür saldırlar internetin hayatımızın her alanına girmesiyle başlamıştır. Siber saldırılar, devletler tarafından yapıldıkça savaşa dönüşmektedir (ALKAN, 2012). Bu sebeple devletler güvenliklerini siber ortamda da sağlamaya yönelmişlerdir. Ancak siber saldırının ne zaman, kim tarafından, nasıl yapılacağı ve sonuçları kestirilememektedir (SINGER & FRIEDMAN, 2018). Bu durum da devletlerin siber saldırılar karşısında güvenlik stratejileri geliştirmelerinde zorlanmalarına neden olmaktadır.

İçinde bulunduğumuz bilişim çağında, devletler saldırıları/çatışmaları siber ortama taşımışlar ve bu şekilde birbirlerine saldırmaya başlamışlardır. Bu durumun da Soğuk Savaş Dönemi'nde olduğu gibi bir bloklaşmaya neden olduğunu; realist kuramın uluslararası sisteme bakış açısı çerçevesinde, önce Soğuk Savaş Dönemi'nde var olan Doğu-Batı Bloku'nu açıklayarak, sonra devletlerin neden bloklaştıkları sorusunun cevabını bulmaya çalışarak, ardında da sırasıyla internet, siber saldırı, siber savaş ve siber güvenlik kavramlarının ne olduğunu anlatmaya çalışarak ve son olarak da Amerika Birleşik Devletleri (ABD), Rusya Federasyonu ve Çin Halk Cumhuriyeti'nin, başka devletlere ve uluslararası

örgütlere yaptıkları siber saldırıları vaka inceleme yöntemi ile inceleyerek, ispatlamaya çalışacağız. Burada devletlerin bloklaştığını siber saldırılar çerçevesinde değerlendirerek, siber saldırıların, devletlerin yeniden bloklaşma yoluna gittiklerini açığa çıkarması bakımından önemli olduğunu anlatmaya çalışacağız. Bu çalışmada çeşitli kitap, makale ve gazete haberlerinden yararlanılmıştır. Çalışma, teknolojik gelişmelerle yeniden oluşan dünya düzenini anlamak için önemlidir.

1. SOĞUK SAVAŞ DÖNEMİ OLUŞAN BLOKLAŞMA

İkinci Dünya Savaşı sırasında, Amerika Birleşik Devletleri (ABD) ve Sovyet Sosyalist Cumhuriyetler Birliği (SSCB), Alman tehdidinden dolayı müttefik olmak durumunda kaldılar ve bu yüzden karşılıklı sorunlarını gün yüzüne çıkaramadılar. İkinci Dünya Savaşı sonrasında bu iki güç arasında Doğu Avrupa, Almanya ve Atom silahlarının kontrolü konularında anlaşmazlıklar bulunurken, Ortadoğu ve Mançurya bölgelerinde çıkar çatışmaları mevcuttu. Bu gibi sorunlar iki ülke arasında sıcak çatışmaların yerine, soğuk rüzgârların eseceği bir mücadelenin başlamasına neden oldu. Özellikle İkinci Dünya Savaşı'nda; İngiltere, Fransa ve İtalya gibi devletlerin bitkin düşmelerine ve yukarıdaki sorunlarla ilgilenme konusunda yetersiz kalmalarına neden oldu. Bu da, uluslararası sistemin iki kutuplu bir sisteme evrilmesine neden oldu.

Doğal olarak bu iki kutuplu sistemde, hegemon olan iki devlet birbirlerine üstün gelmek için diğer devletleri kendi yanına çekmeye çalıştılar. Özellikle SSCB'nin yayılmacı politikası, bu yayılmanın içine entegre olmak istemeyen devletleri ABD safına itmeye neden oldu. Böylelikle uluslararası sistemde yeni bloklaşma oluşmaya başladı. Doğu Blok' u SSCB'nin öncülüğünde; Küba, Doğu Almanya, Romanya ve Bazı Doğu Avrupa ülkeleri gibi ülkeleri kapsamaktayken; Batı Blok' u ise ABD öncülüğünde daha sonra NATO çatısı altında birleşecek olan İngiltere, Fransa, Kanada, Hollanda, İzlanda, Danimarka ve daha birçok Avrupa ülkesini kapsamaktaydı. Bu iki blok haricinde bir de bağlantısızlar hareketi vardı. Bu hareket, bazı Asya ve Afrika Devletleri'nin Batı ve Doğu bloğu arasındaki çıkar çatışmasının içerisinde kalmamak amacıyla düzenlenen üç konferans ile gerçekleşti. Bu durum da onları üçüncü bir blok olarak ortaya çıkardı. ABD ve SSCB, doğrudan bir sıcak

çatışmaya girmese de kendi bloklarında bulunan devletlere, diğer bir blokta bulunan ya da bu bloklardan bağımsız bir devletle olan sıcak çatışmasında veya aralarındaki problemler karşısında yaptıkları yardımlar ve ulusal çapta verdikleri destekler ile dolaylı olarak karşı karşıya gelmekteydiler. Buna en iyi örnek, Güney Kore ile Kuzey Kore arasında 1950 – 1953 yıllarında gerçekleşen savaştır.

Batı Blok'u, doğal olarak ABD, Güney Kore'yi desteklerken; Doğu Blok'u yani SSCB, Kuzey Kore'yi desteklemiştir. Batı Blok' u, SSCB'yi etkisiz kılmak için NATO'yu kurarken; SSCB buna misilleme olarak Varşova Paktı'nı oluşturmuştur. Bu da Soğuk Savaş Dönemi'nde kesin çizgilerle ayrılan iki bloğun oluşumunu perçinlemiştir. Ancak 1990 yılında Doğu Almanya ile Batı Almanya'nın birleşmesi ve 1991 yılında SSCB'nin dağılması ile Soğuk Savaş Dönemi biterken bloklaşma yarışı da şimdilik sona ermiş olacaktı. Soğuk Savaş Dönemi'nde oluşan bu bloklaşma bağlamında ortaya şöyle bir soru çıkmaktadır. *"Devletler neden bloklaşır?"* Günümüz Bilişim Çağı'nda oluşan bu bloklaşmaya bakmadan önce bloklaşmanın neden oluştuğuna bakılmalıdır.

2. DEVLETLER NEDEN BLOKLAŞMA GEREĞİ DUYAR?

Realizm, uluslararası sistemin anarşik olduğunu ve bu sistemde etkin aktörün devlet olduğunu öne sürmektedir. Bu bağlamda devlet, anarşik olan bu sistemde varlığını devam ettirmeye çalışmaktadır (KEYİK & EROL, 2019). Öyleyse bu anarşik yapıda güçsüz olan devletler; güçlü olan devletlerin gazabından korunmak amacıyla siyasi, kültürel, ekonomik, ideolojik ve jeopolitik çıkarları doğrultusunda kendilerine yakın hissettikleri güçlü bir devletin ya da devletlerin hegemonyası altında olmayı tercih edebilirler. Güçlü devletler de kendilerini yukarıda saydığımız alanlarda yakın hissettiği başka bir güçlü devlet veya devletlerle anlaşmalar yolu ile gruplaşma ya da ittifak kurma yolunu izleyebilir. Güçlü devletlerin kendi aralarında yaptığı ittifaklara en iyi örnek ise iki dünya savaşı arasındaki çok kutuplu sistemde oluşan bloklaşmadır.

Burada İngiltere, Fransa, SSCB ve sonradan dâhil olsa da Amerika gibi birçok devletin oluşturduğu Müttefikler Blok'u ile onların karşısında kurulan Almanya, İtalya ve Japonya

gibi devletlerin oluşturduğu Mihver Blok'u bulunmaktadır. Güçsüz devletlerin yukarıda bahsettiğimiz alanlarda kendini yakın hissettikleri güçlü devletin yanında yer aldığı duruma en iyi örnek ise bir önceki başlıkta değindiğimiz Soğuk Savaş Dönemi'dir. Görüldüğü gibi anarşik olan bir sistemde devletler, kendilerini korumak veya varlıklarını devam ettirmek amacıyla başka bir devletin hegemonyasını kabul etmek durumunda kalmakta ya da güçlülük halini korumak maksadıyla başka devlet ya da devletlerle işbirliğine gitmektedir. Ayrıca yine realistlere göre sürekli savaşın var olduğu bu sistemde; güçlü devletler, kendi çıkarlarını korumak amacıyla büyük savaşlara yol açacak olan bloklaşmadan da kaçınmadıklarını göstermektedirler.

Devletler kendilerini bu anarşik ortamda başat güç olarak göstermek ve var olan gücünü en az kayıpla korumak amacıyla diğer güçlü devletlerle ittifak veya bloklaşma yoluna gitmeye ihtiyaç duymaktadırlar. Thomas Hobbes'ın dediği gibi *"Devletin amacı, bireysel güvenliktir"* (HOBBES, 2019). İşte bu güvenliği, anarşik sistemde sağlamak için devletler başka devletler ile isteyerek ya da istemeyerek blok kurmak durumunda veya oluşan bloğa dâhil olmak zorunda kalmaktadırlar. Özellikle realistlere göre devletler, daha esnek davranabildikleri çok kutuplu sisteme nazaran iki kutuplu sistemlerde etkinlik alanlarının daraldığı sebebiyle, sert, disiplinli ve gergin bloklar kurmaktadırlar (YALÇIN, 2015). İki kutuplu sistemde kurulan disiplinli blokların, iki güçlü devlet arasındaki güç dengesi sayesinde sıcak savaşa girme olasılıkları daha düşüktür. Çünkü iki kutuplu sistemde, iki başat güçten başka bir üçüncü başat güç olmadığı için, iki güçten birinin tehditkâr davranması durumunda, soruna müdahil olacak başka bir güç olmayacaktır ve bundan dolayı diğer başat güç onu dengelemek zorundadır ve bunu yapmama lüksü yoktur (YALÇIN, 2015). Ancak çok kutuplu olan ve devletlerin esnek davranabildiği bir sistemde, kurulan blokların savaşa gitme ihtimali daha yüksektir. Buna en iyi örnek; Birinci ve İkinci Dünya Savaşları öncesinde kurulan blokların sıcak savaşa girmesidir.

Soğuk Savaş'ın sona ermesiyle iki kutuplu sistemden tek kutuplu sisteme geçiş olmuştur. Bu geçiş ile Soğuk Savaş Dönemi'nde var olan Doğu ve Batı Blok'u da ortadan kalkmış oluyordu ve bu durum NATO'nun da sonunu getiriyordu. Artık SSCB'nin olmadığı bir sistemde, ABD'nin Avrupa'da bulunması, Avrupa için olumsuz durumken, ABD için de yük durumdadır (WALTZ, 2008). Waltz, NATO için: *"NATO'nun günleri değilse bile yılları*

sayılıdır." demiştir (WALTZ, 2008). Ancak durum böyle olmadı ve NATO varlığını sürdürmeye devam etmektedir. NATO'nun varlığı devam etmekle kalmadı, ABD'de tek başat güç olarak tek kutuplu sistemi sürdürmeye devam etti. Tek kutuplu sistemin sürdürülemez olduğunu söyleyen Waltz gibi neorealistler, anarşik olan uluslararası sistemde devletler var olabilmek için tek olan başat gücü dengeleyeceklerini ve buna bağlı olarak güç dengesi teorisi ile diğer devletlerin ABD'yi dengeleyeceğini ve böylelikle tek kutuplu sistemin uzun olmayacağını söylerler (WALTZ, 2008). Lakin iki kutuplu sistemin bittiği zamandan bu yana hala ABD'yi dengeleyecek bir devlet ya da devletlerin oluşturduğu bir yapı oluşmuş değildir (YALÇIN, 2015). Fakat bu durumun böyle gideceğinin bir garantisi de yoktur. Tek kutuplu sistem, 11 Eylül 2001 saldırılarından sonra, ABD'nin Afganistan operasyonu, ardından da 2003 Irak işgali ile sekteye uğramaya başlamış ve ABD'nin hegemonyası sorgulanır olmuştur.

Bu sorgulamanın ardından başat güç olma yolunda ilerleyen Rusya Federasyonu, Çin, Hindistan, Avrupa Birliği'ni oluşturan güçlü ülkeler ve Japonya gibi devletler, ABD'yi dengeleme eğiliminde bulunarak, uluslararası sistemi, çok kutuplu sisteme evrilmesine ön ayak olacak çok aktörlü bir uluslararası yapıya dönüştürmüşlerdir (KANTARCI, 2012). Çok kutuplu sisteme evrilen bu çok aktörlü yapı içerisinde tekrar bloklaşmanın olmaması, geçmişe baktığımızda ve realist bakış açısıyla incelediğimizde pek de mümkün görünmemektedir.

Peki, Soğuk Savaş sonrası bloklaşma son mu buldu? Buna evet ya da hayır demek soruyu tam anlamıyla karşılamamaktadır. Reel olan, uluslararası sistemde son bulmuş gibi gözükse de siber uzayda yeni bir bloklaşmanın doğum sancıları başlamış gibi görünmektedir. Bu bağlamda buradan sonra yapacağımız, siber uzayda [*"Özünde siber uzay; "içerisinde bilginin çevrim içi olarak saklandığı, paylaşıldığı ve iletildiği, bilgisayar ağlarının (ve arkasındaki kullanıcıların) âlemidir"*(SINGER & FRIEDMAN, 2018).] gerçekleşen karşılıklı siber saldırılar incelenerek, çok aktörlü yapıya evrilen yeni sistem içerisinde oluşan bloklaşmanın ispatını yapmaya çalışmaktır. İlk olarak siber uzayın yaşam alanı olan interneti açıklamakla başlayacağız.

3. SİBER UZAYIN HAYAT SAHASI İNTERNET

İnternet; dünya çapında birçok kullanıcının oluşturduğu bilgisayar ağı sistemidir. İlk olarak internet, 1962 yılında Amerikan Askeri Araştırma Projesi kısa adı ARPANET olan proje ile Massachusetts Institute Of Technology arasında oluşan, *"galaktik ağ"* konusu üzerine ortaya çıkmıştır (ÇAKIR, 2005). Ardından 1969 yılı itibari ile de ARPANET sayesinde ilk bağlantı gerçekleşmiş oldu (ÇAKIR, 2005). Daha sonra ABD'de gerçekleşen bir dizi çalışmalar ile internet bugün ki kullanılan halini aldı. Bütün kullanıcılar internete, internet protokolü olan, Transmission Control Protocol/Internet Protocol kısa adıyla TCP/IP ile bağlanır. Bütün bilgisayarlar bu protokol ile bağlanmak zorundadır, bu yazılım kurulu olmayan bilgisayar internete bağlanamaz. Şuan dünya çapında kullanmış olduğumuz internette, sadece İnternet Protokolü (IP) kısmını kullanmaktayız (SINGER & FRIEDMAN, 2018). İnternet, günümüzde hayatın her noktasında yer almaktadır. Kurduğumuz ikili iletişimden, haberleşmeye, alışveriş yapmaktan, belge ve bilgi aktarımına, silah sistemlerinin kullanımından, nükleer santrallerin işletilmesine, bankacılık işlemlerinden, sosyal medyaya kadar her alanda internet kullanılmaktadır. İnternetin bu denli geniş alanda kullanımı yeni bir kavram olan siber uzayı ortaya çıkarmış ve ona hayat vermiştir. Siber uzay dijital verilerin üretildiği, saklandığı, paylaşıldığı ve paylaşılan bu verilerin kullanıldığı alandır (SINGER & FRIEDMAN, 2018). Bütün bu verileri kullanmamıza olanak sağlayan ve siber uzayın da hayat sahası internettir.

İnternet, kullanım alanının geniş olmasından ve dünya çapında bütün insanların ve devletlerin kullanımına açık bulunmasından dolayı tehlikeleri de beraberinde getirmiştir. Bireysel tehlikelerinin yanında, devletlere yönelik de tehlikeleri bulunmaktadır. Bu tehlikelerin en önemlisi siber saldırılardır. Bu makalede bireylere yönelik değil, devletlere yönelik olan siber saldırıları ele alacağız.

4. SİBER SALDIRI, SİBER SAVAŞ VE SİBER GÜVENLİK

İnternetin ortaya çıkmasıyla küçülen dünyada, insanlar birbirleriyle anlık iletişim kurabilir hale gelmiştir. Asya'nın bir ucanda bulunan Japonya'daki bir birey ile Avrupa'nın en ucundaki İrlanda'da bulunan bir birey, birbirleriyle anlık iletişim kurabilmektedirler. Bu iletişim her zaman iyi niyetli olmayabilir. Küçülen dünyada; bireylerin, örgütlerin ve devletlerin internete ulaşabilme olanağı ve kullanım kapasitesi her geçen gün arttıkça, internetin kötü amaçlı kullanımı da sürekli artmaktadır. Kötü amaçlı kullanımın en geniş ve zararlı kısmını siber saldırılar oluşturmaktadır. "*ABD Hükümeti 2009' da Ulusal Araştırma Konseyi'ni siber saldırılar üzerine çalışmak için topladığında, bunları 'bilgisayar sistemleri, ağlar veya bilgiyi ve/veya bunlarda yerleşik olan ya da bunları taşıyan programları değiştirmek, bozmak, aldatmak, küçük düşürmek veya yok etmek için yapılan kasıtlı hareketler' olarak tanımlamıştır*" (SINGER & FRIEDMAN, 2018). Sınger ve Fnedman'ın, Siber Güvenlik ve Siber Savaş isimli yazdıkları kitapta ABD hükümeti tarafından oluşturulan konseyde siber saldırının tanımı bize bu şekilde aktarmışlardır. Bir başka açıyla siber saldırı; internet altyapısı kullanılarak ya da bilgisayar donanımında, sonradan veri aktarımı yapmak amacı ile kullanılan araçlarla (Flash Bellek, CD, Hard Disk gibi) kişi, devlet, kurum ve şirketlerin bilgi ve iletişim altyapılarına; bireysel, askeri, politik ve ticari amaçla yapılan planlı ve koordineli saldırılardır (ALKAN, 2012). Peki, bu siber saldırılar nasıl oluyor? Tehditler nelerdir?

İnternet ortamında yapılacak bir saldırı, fiziksel ve coğrafi bir ortam olmadığı için çok hızlı hareket edebilir ve bir hedefi birden çok saldırı vurabilir ya da bir saldırı birden fazla hedefi vurabilmektedir (SINGER & FRIEDMAN, 2018). Gerçek ortamda gerçekleşen saldırılardan çok farklı bir yapıya sahiptir. Herhangi bir coğrafi ve fiziksel engeli aşma durumu yoktur. Bir başka deyişle sizin saklanabileceğiniz coğrafi ve fiziksel bir yapı yoktur. İlk olarak hedefi bir bilgisayar ve ondaki bilgidir (SINGER & FRIEDMAN, 2018). Ancak bu saldırılar, sanal ortamda olduğu halde gerçek ortamda da fiziksel hasarlara meydan verebilmektedir. Örneğin, en küçük çapta bilgisayarınızı işlem dışı bırakabilir. Gerçek bir ortamda, fiziki unsurlar kullanılarak yapılan saldırıda, saldırının yapıldığı yer ve çevresine verecek zarar hesaplanabilir fakat siber ortamda yapılan bir saldırıda bu mümkün değildir. Bir saldırı

yapıldığında, bu saldırının en son hangi bilgisayarda biteceğini hesaplamak çok zordur (SINGER & FRIEDMAN, 2018).

Bahsetmiş olduğumuz bu siber saldırıların devlet bazında hedeflerine baktığımızda, çok çeşitlilik gösterdiğini görmekteyiz. Bunlar; Bilgi İletişim Teknolojileri, enerji üretim tesisleri (nükleer, termik ve hidroelektrik santralleri gibi), şehir su şebekeleri, finans, gıda, tarım ve sağlık alanları, iletişim kanalları, devlet yönetim kademeleri, askeri savunma sistemleri ve savunma sanayi gibi birçok alanı oluşturmaktadır. Bunların dışında sayabileceğimiz hedefler; sosyal ağlar, akıllı şebekeler, kapalı devre sistemler ve web sayfaları bulunmaktadır (Ünal, 2015). Bütün bu sistemler bir devletin hayati önem sahibi organları olarak düşünebiliriz. Günümüz bilişim çağında bir devletin bütün bu organları, tam olarak güvenliği sağlanmamış olan internet ortamında işlevsel olduğunu görmek, devletin ne gibi bir tehlikede olduğunu açıkça göstermektedir. Bütün hayati sistemler bu ortam üzerinde yürütülmektedir. Devlet bu organlarında, kapalı sistem bile kullansa tehlikeden tam anlamıyla uzak olduğu anlamına gelmemektedir. Bunun en iyi örneği ileri ki başlıklarda değineceğimiz STUXNET saldırısıdır. STUXNET, ABD tarafından üretilerek, kapalı devre sistemi yani internetten ayrı bir sistemi olan, İran Nükleer Araştırma Merkezi'nde bulunan santrifüjlere zarar veren bir virüstür.

Değindiğimiz, devletin hayati organları olan bu hedeflere yönelik hem insan hem yazılım kaynaklı tehditler bulunmaktadır. Bu tehditlerden yazılım kaynaklı olanlar; a) Zombi /Hayalet Sistem yazılımları, b) Yemleme yazılımları, c) İstem dışı e-posta yazılımları, d) Casus/Kötü amaçlı yazılımlar (virüsler, kurtçuklar, solucan, böcekler ve Truva atları gibi) oluştururken, insan kaynaklı olan tehditleri; a) organize suç grupları, b) yabancı istihbarat örgütleri, c) hackerler, d) Bilişim sistemlerine erişebilen çalışanlar, e) teröristler oluşturmaktadır (Ünal, 2015). Bu saydığımız insan kaynaklı tehditler, devlet alt ve üst yapı sistemlerine yazılım kaynaklı tehdit unsurları ile saldırarak zarar vermektedir. Bunlar içinde sayılmayan bir başka tehdit ise bir başka devlettir. Yukarıda STUXNET örneğinde de gördüğümüz gibi, bir devlet yazılım kaynaklı tehditleri kullanarak bir başka devlete siber saldırı düzenleyebilmektedir. Devlet bu saldırıyı yaparken kendi istihbarat örgütlerini kullanabileceği gibi, kendine bağlı ya da kendinden bağımsız hackerları da kullanabilmektedir. Kullanım alanı ve kullanım şekli çok geniş olan siber saldırılar, bu

yüzden kim tarafından ne zaman ve nasıl yapıldığını tespit etmek oldukça güçtür. Yapılan bir saldırıyı, kendi iradesiyle bir birey mi yaptı yoksa o bireye bir devlet mi yaptırdı ya da herhangi bir devlet bu saldırıyı kendimi gerçekleştirdi, bunu kestirebilmek, tespit edebilmek zor iştir. Bunun tespiti için bile gelişmiş teknoloji ve siber alanda kendini geliştirmiş kalifiye insan gücüne ihtiyaç vardır. Anlaşılması zor olan bu saldırı yöntemi nedeniyle, devletlerin birbirlerine karşı yaptıkları saldırılarda, karşı tarafı suçlaması çoğu zaman ispatla mümkün olmamaktadır.

Bu bağlamda devletler siber saldırıları, siber ortamda/uzayda birbirlerine karşı düzenledikleri zaman ortaya siber savaş kavramı çıkmaktadır. Reel uluslararası sistemde savaşın aktörü devlettir ve bir silahlı çatışmanın savaş olabilmesi için, çatışan aktörlerin devlet olması gerekir (VARLIK, 2013). Savaşlar bir devlet ile başka bir devlet arasında, devletler tarafından oluşturulan bloklar/ittifaklar arasında ya da bir devletle diğer devletlerin oluşturduğu blok/ittifak arasında olabilir (VARLIK, 2013). Anarşik uluslararası sistemin temel aktörü devletler, savaşın da belirleyicisi, temel aktörü, başlatanı ve bitireni olmuştur. Teknoloji geliştikçe devletlerin savaşma tarzları, silahları, yöntemleri hatta savaş alanları bile değişmiştir. Fakat tek değişmeyen savaşın kendisi olmuş ve devletler var olabilmek adına her dönemde savaşmışlardır. Modern dünyamızın bilişim çağında, hala fiziki ortamda savaş varlığını korusa da, siber uzayın hayatımıza girişiyle savaş orada da kendini göstermiştir.

Siber uzaya kadar sıçrayan savaş kavramı, burada da aynı durumda geçerliliğini korumaktadır. Siber saldırıların, siber savaş olabilmesi için devletlere yönelik olması gerekir (ALKAN, 2012). Siber saldırının, fiziki ortamdaki gibi kesin sınırları olmasa da yine de devletler tarafından uygulandığı zaman savaşa dönüşmektedir. Fiziki ortamdaki çatışmalar gibi savaşa dönüşen siber saldırıların, devletler arasında gruplaşmaya yol açmaması mümkün mü? Dünya savaşlarında devletler nasıl karşılıklı ittifak/blok oluşturduysa, bunun siber uzayda da yaşanması muhtemeldir. Devletler bu saldırılara tek başlarına ya da blok oluşturarak savunma oluşturmaları, siber uzayda da var olmalarını hatta fiziki ortama etki edecek kadar zararlı olan siber saldırılar karşısında kendini güvence altına alması doğal bir davranıştır. Kendi istek ve çıkarlarını hatta ideolojik düşüncelerini, karşı tarafa kabul ettirmek amacıyla bu saldırıları yapmaktan çekinmeyecektir. Bu saldırılar tarih süreci

içerisinde reel ortamda yaşandığı gibi devletleri kutuplaştıracaktır. Fakat uluslararası ilişkilerde, yaşanan olayların neye sebep vereceğini kesin olarak söylemek çok zordur (WALTZ & QUESTER, 1982). Bu zorluğa rağmen oluşmakta olan olaylar bize ipuçları vermektedir. İşte bu ipuçları ve yaşanan olaylar irdelendiğinde, içinde bulunduğumuz bilişim çağında devletlerin tekrar, siyasi, kültürel, ekonomik, ideolojik, jeopolitik ve çıkar bazında bloklaştığı görülmektedir. Bu bloklaşmayı daha iyi anlamak ve ispat etmek için, devletlerarası siber saldırıları ileriki başlıklarda inceleyeceğiz.

Bütün değindiğimiz, siber saldırı ve siber savaş durumlarında devletler kendi ve kendine bağlı kurumların güvenliklerini korumak için elbette tedbirler almaktadır. Bu tedbirler reel ortamdaki gibi kendi güvenliğini güvence altına alma biçimindedir. Realistlere göre savaş olağan ve uluslararası sistemde sürekli var olan bir durumdur (KARABULUT & DEĞER, 2015). Bu yüzden devletler güvenliklerini ön planda tutarak, güvenliklerine öncelikle değerlendirilmesi gereken bir durum olarak bakarlar (KARABULUT & DEĞER, 2015). Devletler, kendi güvenliklerini sağlamak amacıyla, her şeyin mübah olduğunu düşünebilirler. Böyle bir düşünce, devletlerin kendi güvenliklerini öncelemelerinden kaynaklanmaktadır. Devletler, dış ortamdan kendilerine gelebilecek tehditlere karşı iki strateji uygulamaktadırlar (EFEGİL & KALAYCI, 2012). Birincisi; devletler *"güç imkânları"* çerçevesinde *"askeri ve ekonomik"* olanaklarının geliştirilmesi olan *"iç-dengeleme stratejisi"* geliştirmektedirler, ikincisi ise diğer devletleri kendisine dayanak olmasını sağlayacak bir anlaşma yapılmasını öngören *"dış-dengeleme"* stratejisidir. (EFEGİL & KALAYCI, 2012). Devletler, gönüllü veya gönülsüz olarak bu stratejilerle kendi güvenliğini sağlamak durumundadır. Aksi halde devletler, uluslararası sistemde var olma yarışını kaybedeceklerdir. Dış dengeleme stratejisine en iyi örnek, Soğuk Savaş dönümünde oluşan Doğu ve Batı Bloklarını, kendisini tehlikede hisseden devletlerin ya da ideolojik olarak birbirine yakın devletlerin oluşturmasıdır veya bu tarz devletlerin bu bloklara katılmasıdır. Soğuk Savaş Dönemi'nin iki kutuplu sisteminde, güvenlik kavramı ABD ve SSCB etrafında dönerken, Soğuk Savaşın bitmesi, Yugoslavya'nın dağılması ve 11 Eylül saldırısından sonra güvenlik kavramının kapasitesi genişlemiştir. Hatta güvenlik kavramına, son zamanlarda artan çevresel sorunlar nedeniyle, askeri, politik ve ekonomik sorunlara ek olarak çevresel sorunlar da eklenmiştir. Son olarak güvenlik kavramına siber

sorunlar da eklenmelidir. Giderek artan siber saldırıların gölgesinde devletler güvenlik endişesi duymaktadırlar. Bu da güvenlik kavramına yeni bir oluşum daha getirmektedir. Siber ortamdaki sorunları; reel ortamda yaşanan askeri, politik, ekonomik ve çevresel sorunlardan ayırmamız mümkün değildir. Günümüzde, askeri, ekonomik, politik hatta çevresel alanların hepsinde siber altyapıya bağımlı durumdayız. Nasıl haberleşmeden bankacılığa kadar siber altyapı kullanılıyorsa en küçük örneğiyle, bir bölgedeki hava değişimleri de bu alt yapı sayesinde takip edilmektedir. Yani siber uzayı/âlemi, güvenliğin diğer alanlarından ayıramayız.

Günümüz bilişim çağında, gelişen teknoloji ve siber alt yapı sayesinde, küreselleşme hız kazanmaya başlamış, buna bağlı olarak, oluşacak tehditler kestirilemez hal almıştır (EFEGİL & KALAYCI, 2012). Bu kestirilemez duruma gelen tehditlere karşı, devletler güvenlik stratejileri geliştirmeye çalışmaktadır. Ancak, farklı ülkelerde yaşayan insanların, daha kolay iletişime geçmeye başlamasıyla artık tehditler *"risk"* olarak tanımlanmaya ihtiyaç duymuştur ve bu risklerin, ne zaman, kimler tarafından ve ne şekilde ortaya çıkacağı belirsiz durumdadır (EFEGİL & KALAYCI, 2012). Bu belirsizlikler ışığında, tahmin edilebilir olan tehditler, giderek öngörülemeyen risklere dönüşmektedir (BECK, 1992). Bu öngörülemeyen riskler siber güvenlik için oldukça uygun kavramdır. Devlet olarak, siber altyapıya dayalı kurulan bir sistem, başka bir devletten ya da herhangi bir terör örgütünden destek alan bir bireyin, evinde bilgisayar başında oturarak bu sisteme zarar verebilecek durumda olup olmaması muğlak ya da diğer bir tabirle öngörülemeyen bir risk oluşturabilmektedir. Bütün bu güvenlik kavramı çerçevesinde, siber saldırılara ve siber savaşa karşı koymanın tek yolu da siber güvenliktir. Siber güvenlik; *"Siber ortamda, kurum, kuruluş ve kullanıcıların varlıklarını korumak amacıyla kullanılan araçlar, politikalar, güvenlik kavramları, güvenlik teminatları, kılavuzlar, risk yönetimi yaklaşımları, faaliyetler, eğitimler, en iyi uygulamalar ve teknolojiler bütünüdür."* şeklinde tanımlanmaktadır (ALKAN, 2012). Bu tanım üzerinden devletin kendi güvenliğini siber uzayda sağlamak için, en iyi şekilde donanmış kalifiyeli bireylere ve en gelişmiş teknolojilere ihtiyacı vardır. Siber uzaydaki bu yarışta bir devlet, kalifiye eleman yetiştirme ve daha gelişmiş teknolojileri üretmede yetersiz kalması durumunda, güvenlik zafiyeti doğacaktır ve devletin bu anarşik sistemde yeri olmayacaktır. Bu güvenlik gereklerini yerine getiremeyen devletler varlığı devam ettirmek için, siber

güvenlik bağlamında güvenlik gereklerini yerine getiren bir devletin ya da devlet/ulus üstü örgütlerin korumasını kabul edeceklerdir. Böylelikle kendilerine yapılan bir siber saldırıda bu devletlerin ya da örgütlerin kendisini savunmasını veya güvenliğini sağlamasını bekleyecektir. Bu kabullenme reel ortamda Soğuk Savaş döneminde en iyi şekilde örnekleri ile doludur. Bu dönemde, gerekli, askeri, ekonomik ve teknolojik donanıma sahip olmayan devletler, güvenliklerinin sağlanması amacıyla, Doğu ve ya Batı Bloklarına entegre olmak zorunda kalmışlardır. İleriki başlıklar içerisinde inceleyeceğimiz vakalarda, işte bu dönemdeki gibi blokların oluştuğunu ve bu oluşan bloklara, siber güvenliği sağlayamayan devletlerin dâhil olmasını, siber saldırılar üzerinden inceleyeceğiz.

5. RUSYA FEDERASYONU'NUN, ESTONYA, GÜRCİSTAN, HOLLANDA, UKRAYNA VE NATO'YA SİBER SALDIRILARI

Doğu Bloku'nun başını çeken SSCB'nin dağılmasından sonra, SSCB'nin yerine devamı nitelikte olan Rusya Federasyonu kuruldu. Rusya, SSCB'nin Batı Bloku ile olan sorunlarını bir kenara bırakmak istese de tam anlamıyla başarılı olabilmiş değil. Özellikle SSCB gibi Rusya da hala ABD ile bir yarış içerisindedir. SSCB'yi çevrelemek için kurulan NATO bile hala varlığını korumaktadır. Soğuk Savaş döneminde SSCB ve ABD arasında yaşanan, diğer devletleri kendi safına çekme çabası, hala Rusya ile ABD ve Batı Avrupa devletleri arasında, SSCB'nin dağılmasından sonra bağımsız olan devletlerin kendi yanlarında yer almasını sağlama yarışında varlığını devam ettirmektedir. Bu yarışın en iyi örnekleri; Rusya'nın 2008 yılında Gürcistan'a, 2013'de Ukrayna'ya müdahalesidir. 2008 yılında Gürcistan'ın, hem NATO'ya hem AB'ye katılmak için müzakerelerde bulunması üzerine, Rusya, Güney Osetya sorununu da bahane ederek Gürcistan' a müdahalede bulundu ve Güney Osetya'yı ele geçirerek Tiflis' e kadar yaklaştı ancak 2008 yılının Ağustos ayında Fransa'nın arabuluculuğu ile Rusya müdahaleyi durdurarak Gürcistan'dan birliklerini çıkardı (CİTAK & HARRİS, 2018). 2013 yılında ise Ukrayna'da Rusya yanlısı lider Viktor Yanukoviç'in, Ukrayna - AB Ortaklık Anlaşması'nı imzalamaması üzerine Ukrayna'da başlayan protestoların ardından Yanukoviç Ukrayna'yı terketmek zorunda kaldı ve yerine batı yanlısı muhaliflerin geçmesi üzerine Rusya, Kırım'ı ilhak etti (KEREM, 2018). Ardından

Rusya'nın desteklediği milisler ile Kiev yönetimine bağlı güçler arasında çatışmalar yaşandı (KEREM, 2018). Bu iki örnekte de görüldüğü gibi, iki ülke de batı yanlısı politikalar izlemeye başladığı sırada Rusya'nın hedefi olmaktadırlar, aynı şekilde Rusya yanlısı politika izlediklerinde ise Ukrayna'da olduğu gibi iç karışıklık baş göstermektedir. Yani Soğuk Savaş'tan dönemimize kalan miraslardan biri de bloklaşma faaliyetleridir. Hala devamlılığını sürdüren bloklaşma Batı ile Rusya arasında ciddi şekilde devam etmektedir. Bu örneklerdeki gibi gerçek ortamda gerçekleşen saldırılar, aynı nedenlerle siber ortamda da gerçekleşmektedir. Rusya, bu iki ülkeye askeri müdahale ettiği gibi bu iki ülke ve bazı batı ülkelerine siber saldırılarda da bulunmuştur. Sırasıyla Rusya'nın gerçekleştirdiği iddia edilen saldırılar:

5.1. Estonya'ya Siber Saldırı

2004 yılında Estonya'nın NATO üyesi olmasıyla, Rusya ile arasındaki ilişkiler bozulmuştur. İlişkilerin bozulmasının ve Estonya'nın Batı yanlısı politikalarının ardından bir de Estonya, SSCB döneminde kalma başkent Tallinn'de bulunan *"Bronz Askeri Heykeli"* kaldırması üzerine, 2007 yılında Estonyalı Ruslar, Estonya'nın bilişim sistemini çökertmişlerdir (DARICILI, 2015). Estonya, bu saldırıya kadar dünyanın en çok internete *"bağlı"* devleti durumundaydı (SINGER & FRIEDMAN, 2018). Rusya, başkentten kaldırılan heykelin bedelini bu bağlılık aracılığıyla ödetmişti. Estonyalı Ruslar; sadece kendileri değil, Rusya'nın da dâhil olduğu yüz noktadan aldıkları destekle Estonya'ya saldırı düzenlediler (DARICILI, 2015). Estonya'ya düzenlenen bu siber saldırılar; Estonya Cumhurbaşkanlığı, parlamento, bankalar ve siyasi partilerin dâhil olduğu birçok internet sitesini hedef aldı ve ülkenin uluslararası sistemle bağlantısını kesti ("Estonya'ya siber saldırı,"2007). Bu saldırının hemen ardından Estonya, Rusya'yı hedef göstererek saldırıdan sorumlu tuttu. Daha sonra Estonya NATO'dan yardım isteyerek, bu saldırının tüm ittifakı tehlikeye soktuğunu belirtti (SINGER & FRIEDMAN, 2018).

BBC'nin haberine göre, kendilerine açıklama yapan Kremlin Sözcüsü Dimitri Peskov; *"İddiaları yalanlayarak 'gerçek dışı' olarak nitelendirdi ve Estonya' ya yönelik siber saldırıda Rusya'nın sorumluluğu olmadığını söyledi"* ("Estonya'ya siber saldırı," 2007).

Rusya, saldırıyı her ne kadar kabul etmese de, Estonya'daki Ruslar'a ek olarak çok sayıda Rusya'ya bağlı sunuculardan saldırıların yapılması Rusya'yı hedef haline getirdi. Ancak siber saldırıların nereden, ne zaman geleceğinin belirsiz olması ve saldırı yapanın tam olarak tespitinin zor olmasından dolayı bir devleti suçlamak elde somut delillerin olmamasından bir amaca ulaşamamaktadır. Estonya'ya yapılan bu saldırı, birçok ülkedeki bilgisayarların ele geçirilmesiyle oluşturulan botnetlerden yapılmasından dolayı, saldırının net yeri ve kimden geldiği tespit edilememiştir (SINGER & FRIEDMAN, 2018). Estonya'nın, NATO'dan yardım istemesi üzerine, hazırlıksız olan NATO, saldırı anında destek sağlayamadı ama sonradan gönderdiği geçici teknik personel siber saldırıyı sonlandırmıştır (DARICILI, 2015).

5.2. Gürcistan'a Siber Saldırı

2008 yılında Gürcistan'ın Batı yanlısı hareketleri ve Güney Osetya sorunu nedeniyle Rusya, Gürcistan'a askeri müdahalede bulunmuştu. Bu müdahaleden önce, Rusya'dan geldiği düşünülen siber saldırılar Gürcistan'ı vurdu. Bu siber saldırının hemen ardından da Rus askerleri Gürcistan'a girdi. Bu saldırılar, Estonya saldırısıyla benzerlik göstermekte ve aynı şekilde siber altyapıya yöneliktir (DARICILI, 2014). Bu saldırı, *"hibrit savaş"* konumunda ilk sıcak çatışma olması bakımından da çok önemlidir (DARICILI, 2014). Gürcistan, bu siber saldırıdan dolayı NATO üyesi olamamasına rağmen, NATO'dan uzman desteği almıştır. Bu saldırı Gürcistan'ın, siber altyapısı ve internete bağlılığı Estonya kadar gelişmiş ve halk bazında çok yaygın kullanımı olmadığı için etkisi Estonya saldırısına göre daha az olmuştur (DARICILI, 2014). Gürcistan'a saldırı, önce siber ortamdan sonra reel ortamdan gelmesi bakımından da çok ürkütücü olmaktadır ve devletlerin bu tür saldırıların önemini kavraması bakımından Gürcistan saldırısı örnek teşkil etmektedir.

5.3. Hollanda'ya Siber Saldırı

Hollanda Savunma Bakanı Ank Bijleveld, Rus İstihbarat servisinin Kimyasal Silahların Yasaklanması Örgütü'ne (KSYÖ) yapılması planlanan siber saldırının engellediğini

söylemiştir (AA, 2018). Haber Türk'ün haberine göre, Hollanda Askeri İstihbarat ve Güvenlik Servisi Genel Direktörü Onno Eichelsheim yaptığı açıklamada; diplomatik belgelerle Hollanda'ya giren dört Rus ajanının saldırıyı gerçekleştirmeye çalıştığını, ancak yakalandıklarını ve üzerlerindeki eşyalara el konulduğunda KSYÖ'ye ait wifi şifresinin kırılmaya çalışıldığının görüldüğünü aktarmıştır (AA, 2018). Bu ajanlardan birinin, "*Enformasyon Teknolojileri Uzmanı"* olduğu ve bu dört ajanın Hollanda tarafından sınır dışı edildiği açıklanmıştır (REUTERS & HABER, 2018). Ancak Rusya yine böyle bir saldırının planlanmadığını söyleyerek, Hollanda'ya Nota vermiştir.

5.4. Ukrayna'ya Siber Saldırı

2013 yılında Ukrayna'da, Rus yanlısı olan Viktor Yanukoviç, AB ile yapılacak olan Ortaklık Anlaşması'nı imzalamaması üzerine başlayan protestolar nedeniyle ülkeden kaçmak zorunda kalması ve Batı yanlısı muhaliflerin iktidara gelmesiyle Rusya, Kırım'ı ilhak etmişti. İşte bu ilhak sırasında Rusya, Ukrayna'nın siber altyapısını hedef almış ve ülkedeki iletişimi keserek Kiev'in, Kırım ile iletişim kurmasını engellemiştir (DARICILI, 2014). Ardından Kırım'da bulunan ayrılıkçı grupları, siber saldırıların hemen sonrasında provoke eden Rusya, Sivastopol'da şiddet içermeyen eylemlerle kendisinin desteklenmesini sağladı (DARICILI, 2014). Rusya, Gürcistan örneğinde olduğu gibi burada da Batı eğilimi artan bir devlete, askeri müdahale bulunmadan önce ve bulunduktan sonra siber saldırılarla yıpratmaya çalışmıştır. Ancak Ukrayna'nın, siber ağı hem karasal hem uydular üzerinden olduğundan bu saldırılar dış dünya ile bağlantısını kesmede başarılı olamadı (DARICILI, 2014).

5.5. NATO'ya Siber Saldırı

Haber Türk gazetesinin internet sitesindeki haberin başlığında, NATO'nun her ay 500 siber saldırıya uğradığını yazmaktadır (AA, 2017). Bu haberi NATO Muhabere ve Bilgi Ajansı Genel Direktörü olan Scheid'e dayandıran gazete, *"NATO, siber alanı da hava, kara ve denizin yanı sıra bir askeri alan olarak değerlendiriyor"* şeklinde haberine devam

etmektedir (AA, 2017). Aynı gazetenin bir başka günkü haberinde, NATO Genel Sekreteri Jens Stoltenberg *"Rusya demokratik kurumlarımıza duyulan güveni baltalamak üzere sosyal ağları ve sanal ortamı kullanıyor. Bu sürekli olarak gelişen bir tehdit ve buna adapte olmak zorundayız."* dediğini aktarmaktadır (DHA, 2017). Haberde görüldüğü üzere Rusya, SSCB'ye karşı kurulan bir örgütü siber saldırı bağlamında hedef almakta ve NATO da SSCB'yi tehdit olarak algıladığı gibi Rusya'yı da tehdit olarak algılamaktadır. Jens Stoltenberg başka bir açıklamasında, kendisine Rusya'dan gelecek siber saldırı karşısında NATO'nun 5. Maddesini uygulamaya koyup koymayacakları sorulduğunda, net bir cevap vermemekle birlikte, gelecek siber saldırının çeşidine göre 5. Maddenin uygulanıp uygulanmayacağına karar verilebileceğini belirtmiştir (SPUTNIK, 2018). Ayrıca, bu siber saldırıların tam tersi olarak Rusya kendisine *" 2018 yılında dört buçuk milyar"* siber saldırının yapıldığını ve bu saldırıların çoğunun NATO üyesi devletlerden geldiğini belirtmiştir ("Rusya'ya yapılan 4 buçuk milyar siber saldırıdan NATO ülkeleri sorumlu," 2019).

6. ÇİN HALK CUMHURİYETİ'NİN, AVRUPA BİRLİĞİ, AVUSTRALYA VE ABD'YE SİBER SALDIRILARI

Çin Halk Cumhuriyeti; giderek güçlenen ekonomisi ve teknolojisi sayesinde, çok kutuplu sisteme evrilen yenidünya düzeninde, ekonomik gelişim açısından ilk sıralardadır. Her geçen sene güçlenen ekonomisi sayesinde ABD'yi geride bırakacağı yönünde tahminler mevcuttur. Ancak Çin sadece ekonomisiyle değil, gelişmiş teknoloji ve kalifiye uzmanları sayesinde üst sıralardadır. Çin, bu teknolojik gelişmeler ve yetişen kalifiye elemanlar sayesinde siber uzayda da adını duyurmaktadır. Gelişen ekonomisini korumak için Çin'in, her geçen gün artan oranda siber saldırlar gerçekleştirdiği vurgulanmaktadır (SINGER & FRIEDMAN, 2018). Özellikle son zamanlarda Çin kaynaklı siber saldırıların sayısında artış gözlemlenmiştir. Çin Hükümeti'nin, halkı üzerinde sıkı ve etkin tedbirlerinden dolayı, Çin'den batı ülkelerine yapılan siber saldırılarda ABD, Çin Hükümeti'ni sorumlu tutmaktadır (SINGER & FRIEDMAN, 2018). Bu siber saldırılar New York Times'ta, *"Çin'in yükselişiyle ortaya çıkan, ABD'nin bir numaralı problemi"* olarak aktarılmıştır

(NEW YORK TİMES & akt.P.W.SINGER). Hatta ABD ve Tayvan, Çin'den gelebilecek siber tehditlere karşı, Tayvan'ın siber açıklarını tespit ederek gerekli önlemleri almak için siber savaş tatbikatı bile yaptı (BIKTIM, 2019). ABD ve Tayvan'dan, bu tatbikatın Kuzey Kore baz alınarak yapıldığı bildirilse de, Tayvan'a tehdit oluşturan yegane devletin Çin Halk Cumhuriyeti olması, bu tatbikatın ibresini Çin'e çevirmektedir (BIKTIM, 2019).

Çin'in bu hızlı gelişmesi ve ABD'nin Çin'in düşmanı ile siber ortamda gerçekleştirdiği siber savaş tatbikatı da, bize ABD'nin sadece Rusya'yı değil, Çin'i de siber tehdit olarak algıladığını göstermektedir. Bu algıdan dolayı olacak ki Çin kendisine yönelik olan siber saldırı suçlamalarına karşı, *"ABD'nin halen Soğuk Savaş zihniyetine saplandığını"* söylemektedir (SINGER & FRIEDMAN, 2018). Bütün bunların yanında Avrupa Birliği, Avustralya ve ABD'den Çin kaynaklı olduğu iddia edilen siber saldırıların da mevcut olması Batı'nın, Çin'i hedef göstermesine neden olmaktadır.

Anadolu Ajansı'nın haberine göre, *"AB'de görev yapan diplomatların gizli görüşmeleri"* Çin kaynaklı siber saldırı sonrası ele geçirildiği ve bu saldırının *"siber güvenlik firması 'Alan 1'"* in tespit ettiği öğrenilmiştir (AA, 2018). Ele geçirilen bu görüşmelerin birçok ülke hakkında olduğu ve ele geçirilenler tarafından sızdırıldığı anlaşılmaktadır (AA, 2018).

Çin hakkında bir başka siber saldırı iddiası ise Avustralya'dan gelmiştir. Avustralya, kendisine ait *"parlamento ve üç siyasi partiye"* siber saldırının Çin tarafından düzenlendiğini belirtmiştir (REUTERS & akt. BAG, 2019). Avustralya, Çin ile olan ticaretinden dolayı olayı gizli tutmaya çalıştıklarını sonradan açıklamıştır (REUTERS & akt. BAG, 2019). Bu iddiayı Çin yalanlarken kendilerine de siber saldırlar düzenlendiğini belirtmiştir (REUTERS & akt. BAG, 2019).

Son olarak Çin'i siber saldırı konusunda suçlayan diğer bir ülke ABD'dir. 2001 yılında ABD ve Çin uçaklarının çarpışması sebebiyle Çin, ABD'ye ait içinde *"Beyaz Saray'ın web sitesinin de"* bulunduğu birçok siteye siber saldırı düzenlemiş ve bu saldırılar ABD'nin uçak kazası için özür mektubu göndermesi ile son bulmuştur (SINGER & FRIEDMAN, 2018). Bu sefer 2015 yılında, ABD tarafından yapılan açıklamada, Çin tarafından ABD şirketlerine defalarca siber saldırı yapıldığı açıklandı ("Çin'den ABD'ye siber saldırı iddiası," 2015). Ayrıca, ABD siber güvenlik şirketi olan *"CrowdStrike"* aynı şekilde Çin'den, ABD

şirketlerine siber saldırı geldiğini doğruladı ve saldırının amacının *"istihbarat toplama amaçlı değil, fikri mülkiyet ve ticari sırları çalmaya yönelik olduğu"* aktarıldı ("Çin'den ABD'ye siber saldırı iddiası," 2015). Bu saldırının amacının askeri ya da istihbarata yönelik olmadığı açıklansa da yine başka bir siber saldırıda ABD, Çin'in bir siber saldırıda askeri bilgileri ele geçirdiğini bildirmiştir. 2018 yılında gerçekleşen bu saldırıda, ABD, *"Çin Hükümeti'ne bağlı bilgisayar korsanlarının, ABD donanmasına ait çok hassas bilgileri ele geçirdiğini"* belirtmiştir (WASHİNGTON POST & YENİÇAĞ, 2018). Yeniçağ gazetesinin, Washington Post gazetesinden aldığı habere göre; *"bilgisayar korsanları ABD donanması ile işbirliği yapan şirketlerin bilgisayarlarını ele geçirerek ABD denizaltılarında kullanılmak üzere süpersonik bir anti-gemi füzesi planları da dâhil olmak üzere, denizaltı savaşlarında kullanılmak üzere çok sayıda önemli bilgiyi çaldı."* (WASHİNGTON POST & YENİÇAĞ, 2018). Çin ise yine saldırıları kabullenmediğini açıklamıştır (WASHİNGTON POST & YENİÇAĞ, 2018).

7. AMERİKA BİRLEŞİK DEVLETLERİ'NİN İRAN'A SİBER SALDIRISI: "STUXNET"

ABD ve İran, 1979 Devrimi'nden önce sıkı birer müttefikken ABD, İran'a nükleer araştırmalar konusunda destek sağlamaktaydı. Ancak 1979 Devrimi'nden sonra müttefik ilişkisi katı birer düşman ilişkisine dönüşmüş hatta ABD, İran'ı *"şer üçgeni"* içerisinde saymıştı. Devrimden sonra İran, nükleer araştırmalar konusunda önce SSCB'den, SSCB'nin dağılmasından sonra Rusya'dan destek almıştır. İran'ın nükleer çalışmaları batılı ülkelerce ve ABD tarafından, İran'a ambargo uygulanacak kadar eleştirilmiştir. İran ve ABD arasında, dönem dönem sıcak savaş söylentileri ve söylemleri olsa da bu zamana kadar doğrudan bir çatışma yaşanmamıştır. Tabi bu reel ortam için geçerlidir. Siber ortamda işler böyle olmamış ve muhteşem denebilecek kötücül yazılım olan STUXNET İran'ı vurmuştur. STUXNET saldırısı yaşanana kadar, bu kadar bilgi birikiminin kullanıldığı, düzenli çalışmaların ürünü olan ve tüm dünyada endişeye sebep veren, özellikle İran'ı şaşkına çeviren böyle bir saldırı gerçekleşmemiştir.

Bilgisayar uzmanları tarafından 2010 yılında yapılan bir araştırmada *"Supervisory Control And Data Acquisition (SCADA)"* isimli, *"Alman Siemens"* firması tarafından üretilerek, endüstriyel alanda siber sistemlerde kontrol amacıyla kullanılan sistemi hedef alan bir virüs tespit edildi (ÇELİK, 2013). Daha kapsamlı yapılan araştırmalar sonucu, özellikle Ralph Langner isimli güvenlik uzmanının yaptığı çalışmada, bu virüsün İran'da çok sayıda bilgisayara bulaştığını tespit etti (SINGER & FRIEDMAN, 2018). Ardından Ralph *"Stuxnet"* ismi verilen bu virüsü inceledikçe çok kapsamlı bir çalışmanın ürünü olduğunu anladı (SINGER & FRIEDMAN, 2018). İncelemeler daha ileri gittikçe bu virüsün, *"Siemens'in WinCC7PCS7 SCADA kontrol yazılımını"* doğrudan hedef aldığı ve *"kendisini 2012'de silmesine sebep olan bir kendi kendini imha mekanizması"* olduğu görüldü (SINGER & FRIEDMAN, 2018).

Daha sonra yapılan araştırmalarda bu virüsün, İran'ın *"Natanz nükleer tesisini"* hedef aldığı tespit edildi. Ancak, İran'ın bu tesisindeki *"SCADA"* sistemi internet üzerinden bağlı değildi ve bu yüzden virüsün tesiste çalışan birinin dışarıdan getirdiği bir bilgisayar ya da flash bellek yüzünden sisteme bulaştığı tespit edildi (ÇELİK, 2013). STUXNET virüsü, nükleer tesiste bulunan santrifüjleri, *"kapatmayarak, basınç sistemlerinde ayarlamalar yaparak, santrifüjdeki pervanelerin yavaşlamalarına sonra aniden hızlanmalarına sebep olarak ve santrifüj hızlarını üst seviyede zorlayarak"* bozulmalarına sebep oluyordu (SINGER & FRIEDMAN, 2018). Bu arızalar yüzünden tesisten yeterli verim alınamıyordu ve tesiste çalışanlar siber saldırı olduğunun farkında değillerdi (SINGER & FRIEDMAN, 2018). Tesiste çalışan uzmanlar, internete bağlı olmadıkları için siber saldırı konusunda hiçbir endişeleri yoktu, bu yüzden sorunun santrifüjler de olduğunu düşünerek sürekli bozulan parçaları değiştirdiler ve bunun siber saldırı olduğunu, Ralph açıklayana kadar kimse anlayamadı (SINGER & FRIEDMAN, 2018). Bu tarz bir siber saldırı dünyada ilk kez uygulanmıştı ve gayette başarılı olmuştu. Gerçek ortamda sıcak çatışmaya girerek büyük riskler ve can kaybına neden olana kadar, böyle bir saldırı hem daha düşük bütçeli hem de herhangi bir can kaybına sebep olmamıştı. Belki de bu saldırı, savaş yöntemlerini siber âleme taşıyarak köklü değişiklere yol açacaktır.

SONUÇ

Realist kuram çerçevesinde uluslararası sisteme baktığımızda, anarşik bir yapıda olduğu görülmektedir. Bu yapının aktörü olan devletler varlıklarını devam ettirmek ve güvenliklerini sağlamak için bir takım ittifak ve bloklaşma yollarına gitmektedirler. Bu güvenliği sağlamak için devletler, iki dünya savaşı öncesi olduğu gibi savaşa neden olacak bloklar kurmuşlardır. İki dünya savaşı öncesi var olan çok kutuplu sistemde devletler daha esnek davranmaları sebebiyle savaş ortamı oluşmuştur. Ancak Soğuk Savaş Dönemi'nin iki kutuplu olmasını sağlayan iki süper gücün, etrafında toplanan devletlerin oluşturduğu Doğu ve Batı bloklaşması savaşa neden olmamıştır. İki süper gücün baskın iki kutuplu sisteminde devletlerin kuruduğu bloklar serbest alan bulamadıklarından, bu bloklaşmanın sonu savaşa dönüşmemiştir.

Soğuk Savaş sonrası tek kutuplu sistemde, devletlerin birleşerek, tek kutbu oluşturan ABD'ye karşı dengeleyici politika izlenmesi gerekse de, bu yapı daha oluşamamıştır. Ancak ekonomik ve askeri alanda hızlı şekilde ivme kazanan bazı Asya ve Avrupa ülkeleri bu tek kutuplu sistemin çok kutuplu sisteme evrilmesine yol açmaktadır. Çok kutuplu sistem oluşum süreci devam ederken, bunu oluşturan güçlü devletler karşılıklı sıcak çatışmaya girmese de, hayatımızın her alanına girmiş olan internet ortamında savaşlar başlamış durumdadır. İnternette hayat bulan siber uzayda/âlemde karşılıklı siber saldırılar yapılmaktadır. Bu siber saldırılar Soğuk Savaş Dönemi'nin, Doğu ve Batı Bloku devletleri arasında yaşanması da, aslında bu bloklaşmanın tam anlamıyla ortadan kalmadığını göstermektedir.

Belli başlı farklılıklar dışında her şey aynı düzlemde sürmektedir. Bu farklılıklar SSCB'nin yıkılması sebebiyle yerini alan Rusya'nın ve devrimle batıdan kopan İran'ın bu bloklaşma içinde olmasıdır. Rusya'nın, SSCB'nin parçası olan ve sonradan bağımsızlıklarını sağlayarak batıya yönelim gösteren Estonya, Ukrayna ve Gürcistan gibi devletlerle NATO ve Hollanda gibi eski Batı Bloku devletlerine gerçekleştirdiği siber saldırılarla, hala kendisinde Doğu Bloku güdülerinin varlığını göstermektedir. Buna ek olarak gerçek ortamda Rusya ile bağlarının güçlü olduğunu bildiğimiz ve hala Komünist sistem ile yönetilen Çin, yine Rusya gibi batı devletlerini siber saldırılar ile hedef almaktadır. Buna

karşılık NATO ve Avrupa Birliği gibi örgütlerle, batı devletleri, sürekli Rusya ve Çin'i siber saldırı yapmakla suçlamakta ve iki devleti tehdit olarak algılamaktadır.

Yeni oluşan bu bloklaşma içine dâhil olan ve Soğuk Savaş Dönemi Bloklaşmasının farkı olarak değerlendirdiğimiz İran, Soğuk Savaş Dönemi'nin ilk yıllarında sıkı bir ABD müttefiki iken, 1979 İslam devrim ile İran yönünü SSCB' ye dönmüştür. İlk dönemlerde nükleer araştırmalarda İran'a destek veren ABD, devrim sonrası bu desteği keserek İran'ın nükleer araştırmalarını eleştirmiş ve bu araştırmalar nedeni ile İran'a ambargo uygulanmasını sağlamıştır. Bu açıdan İran, devrim sonrası yalnızlığa itilmiş olsa da daha soran SSCB ile ilişkilerini geliştirmiştir. Soğuk Savaş sonrası dönemde ise Rusya ile iyi ilişkilere devam etmiş ve nükleer faaliyetlerine devam etmiştir. İran ile sıcak çatışmaya girmek istemeyen ABD bunu siber âleme taşıyarak STUXNET isimli bilgisayar virüsü ile İran'ın Nükleer Araştırma Merkezi'ni vurarak, bu merkezdeki santrifüjlerin düzgün çalışmamasına ve arızalanmasına neden olmuştur.

Bütün bu vakalar incelendiğinde, Soğuk Savaş dönemindeki bloklaşmanın aslında tam olarak ortadan kalkmadığı görülmekte ve doğu-batı devletleri arasında gerçekleşen siber saldırılarla bu bloklaşma, net olarak görünür olmaya başlamıştır. Rusya'nın, batıya yönünü dönen devletlere olan siber saldırıları, Çin'in batı devletlerinin kurumlarına yönelik siber saldırıları, NATO'nun, bir zamanlar SSCB'yi tehdit olarak gördüğü gibi şimdide Rusya ve Çin'i birer siber tehdit olarak görmesi ve ABD'nin İran'a yönelik, siber uzaya damga vuran siber saldırısı, doğu ile batı arasında siber ortamda da ayrışmanın olduğunu göstermektedir. Saldırıya uğrayan Estonya, Gürcistan gibi devletlerin NATO'dan yardım istemesi de buna eklendiğinde, Bilişim Çağı'nda da, Devletleri'n bloklaştığı açıkça görülmektedir.

KAYNAKÇA

AA. (05.10.2018). Rus istihbaratı Hollanda' da siber saldırı düzenledi iddiası! *HABER TURK*. Retrieved from https://www.haberturk.com/rus-istihbarati-hollanda-da-siber-saldiri-duzenledi-iddiasi-2167882

AA. (19.12.2018). Diplomatik yazışmalar ele geçirildi, AB soruşturma başlattı! *HABER TURK*. Retrieved from https://www.haberturk.com/diplomatik-yazismalar-ele-gecirildi-ab-sorusturma-baslatti-2266495

AA. (23.11.2017). NATO MUHABERE VE BİLGİ AJANSI GENEL DİREKTÖRÜ: NATO her ay 500 siber saldırıya uğruyor. *HABER TURK*. Retrieved from https://www.haberturk.com/nato-her-ay-500-siber-saldiriya-ugruyor-1726436

ALKAN, M. (Producer). (2012, Mayıs). Siber güvenlik ve Siber Savaşlar. *www.tbmm.gov.tr*. Retrieved from https://www.tbmm.gov.tr/develop/owa/tbmm_internet.arama?q=sunumlar

Beck, U. (1992). *Risk Society: Towards a New Modernity*: SAGE Publications.

Bıktım, E. (07.11.2019). Tayvan ve ABD Çin'e karşı sanal savaş tatbikatı yaptı. *CNN TÜRK.com*. Retrieved from https://www.cnnturk.com/teknoloji/tayvan-ve-abd-cine-karsi-sanal-savas-tatbikati-yapti

Citak, I., & Harris, C. (09.08.2018). 'Avrupa, Güney Osetya Savaşı'na gerekli tepkiyi verseydi Rusya Kırım'ı ilhak edemezdi'. *euronews*. Retrieved from https://tr.euronews.com/2018/08/09/-avrupa-gurcistan-ve-osetya-savasina-gerekli-tepkiyi-verseydi-rusya-kirimi-ilhak-edemezdi

ÇAKIR, H. (2005). Bir İletişim Dili Olarak İnternet. *Erciyes Üniversitesi Sosyal Bilimler Enstitüsü Dergisi, 1*(19), 71-96.

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

Çin'den ABD'ye siber saldırı iddiası. (20.10.2015). *SPUTNIK TÜRKİYE*. Retrieved from https://tr.sputniknews.com/abd/201510201018462617-cin-abd-siber-saldiri/

DARICILI, A. B. (2014). RUSYA FEDERASYONU KAYNAKLI OLDUĞU İDDİA EDİLEN SİBER SALDIRILARIN ANALİZİ. *International Journal of Social Inquiry, 7*(2), 1-16.

DARICILI, A. B. (2015). *NATO'nun Siber Güvenlik Stratejisinin Analizi.* Paper presented at the ULUSLARARASI SİSTEMDE YENİ DÜZEN ARAYIŞLARI, Bursa.

DHA. (20.11.2017). NATO'dan Rusya açıklaması: Saldırıları artırdılar. *HABER TURK*. Retrieved from https://www.haberturk.com/nato-rusya-dan-gelen-tehditlere-adapte-olmak-zorundayiz-1720896

Efegil, E., & Kalaycı, R. (2012). *Dış politika teorileri bağlamında Türk dış politikasının analizi*: Nobel.

Estonya'ya siber saldırı. (17.05.2007). *BBC TURKISH.com*. Retrieved from http://www.bbc.co.uk/turkish/news/story/2007/05/070517_estonia_cyber.shtml#top

Hobbes, T. (2019). *Leviathan: veya bir din ve dünya devletinin içeriği, biçimi ve kudreti*: Yapi Kredi Yayinlari YKY.

KANTARCI, Ş. (2012). Soğuk Savaş Sonrası Uluslararası Sistem: Yeni Sürecin Adı "Koalisyonlar Dönemi mi?". *Güvenlik Stratejileri Dergisi, 8*(16), 0-84.

KARABULUT, A., & DEĞER, F. (2015). Uluslararası İlişkilerde Güvenlik Kavramı ve Realist Yaklaşım'a Genel Bakış. *İstanbul Gelişim Üniversitesi Sosyal Bilimler Dergisi, 2*(2), 69-79.

Kerem, S. (30.11.2018). Rusya-Ukrayna: İki dost nasıl düşman oldu? *BBC NEWS TÜRKÇE*. Retrieved from https://www.bbc.com/turkce/haberler-dunya-46391387

KEYİK, M., & EROL, M. S. (2019). REALİZME GÖRE GÜÇ VE GÜÇ DENGESİ KAVRAMLARI. *Uluslararsı Kriz ve Siyaset Araştırmaları Dergisi*, 20.

NewYorkTimes, & akt.P.W.SINGER. (A. ATAV, Trans.). In (pp. 133).

Reuters, & akt. BAG, M. (16.09.2019). 'Çin, Avustralya Parlamentosu'na siber saldırı düzenledi' iddiası. In: Euronews.

Reuters, & HABER, a. T. (17.10.2018). NATO siber operasyon merkezi harekete geçiyor. In *TRT HABER*.

'Rusya'ya yapılan 4 buçuk milyar siber saldırıdan NATO ülkeleri sorumlu'. (08.01.2019). *AKŞAM*. Retrieved from https://www.aksam.com.tr/dunya/rusyaya-yapilan-4-bucuk-milyar-siber-saldiridan-nato-ulkeleri-sorumlu/haber-811370

SINGER, P. W., & FRIEDMAN, A. (2018). *Siber. Güvenlik [ve] Siber. Savaş*: Buzdağı yayınevi.

SPUTNIK. (17.09.2018). Stoltenberg: Rusya'nın siber saldırılarına karşılık vermeye hazırız. *SPUTNIK TÜRKİYE*. Retrieved from https://tr.sputniknews.com/karikatur/201809171035237480-nato-stoltenberg-rusya-siber-saldiri-karsilik-5madde-kolektif-savunma/

Ünal, A. N. (2015). *Siber güvenlik ve elektronik bileşenleri*: Nobel Akademik Yayıncılık.

VARLIK, A. B. (2013). SAVAŞI TANIMLAMAK: TERMİNOLOJİK BİR YAKLAŞIM. *Avrasya Terim Dergisi, 1*(2), 114-129.

WALTZ, K. (2008). Uluslararası Politikanın Değişen Yapısı. *Uluslararası İlişkiler Dergisi, 5*(17), 2-44.

Waltz, K., & Quester, G. H. (1982). *Uluslararası İlişkiler Kuramı ve Dünya Siyasal Sistemi*. A.Ü. S.B.F. YAYINLARI.

WashingtonPost, & YENİÇAĞ, a. (2018). Çin'den ABD'ye siber saldırı. In.

YALÇIN, H. (2015). Uluslararası Sistem ve İstikrar: Kavramsal Bir Değerlendirme. *Akademik İncelemeler Dergisi, 10*(1), 212.