KÜRESELLEŞME SÜRECİNDE DÖNÜŞEN GÜVENLİK ALGISI VE SİBER GÜVENLİK

Onur YILMAZ[*]

Özet

Küreselleşmeyle beraber güvenlik konusunda da çeşitli dönüşümler yaşanmıştır. Özellikle teknolojik gelişmelerle beraber dünya adeta küçük bir köye dönüşmüş, mesafelerin bir anlamı kalmamıştır. Teknolojideki bu değişim, bilgi kaynaklarının bağlantılı hale gelmesi, dünyadaki birçok devletin siber ortamda bütün hizmetleri sunması gibi nedenler güvenlik anlayışının da değişmesi gerektiğini ortaya koymaktadır. Artık güvenlik tehditlerine sadece devletler tarafından ve silahlı olarak değil; şirketler, terör örgütleri ve hatta bireyler tarafından da hem de siber uzay dediğimiz sanal alandan maruz kalınabilmektedir. Devletlerin siber güvenlik alanına karşı ilgileri gecikmiştir. Fakat özellikle Estonya, Gürcistan, NATO gibi devlet ve örgütlere yapılan saldırılar sonrası bu konu daha iyi anlaşılmıştır. Bu makalede siber güvenliğin ne olduğu ve güvenlik alanındaki değişimler, siber saldırı örnekleri üzerinden anlatılmaya çalışılmıştır.

Anahtar Kelimeler: Siber, Siber Güvenlik, Güvenliğin Dönüşümü, Siber Saldırılar, Küreselleşme.

Abstract

Along with globalization, there have been diverse transformations in security. The technology advancement in the world has transformed the globe into a miniature pie and this has lead to an absence of borders. The diverse change in technology reveals that the security accepts the change as the sources of facts become linked and almost every state in the world endeavors all services in cyber space. Regarding cybersecurity the states have been late in dealing with it. However, on the other hand it has shown to be better understood exclusively after the attacks on states and organizations such as Estonia, Georgia and NATO.

Within this context this work tries to explain what the cybersecurity is and the changes in the security patch through the examples of the cyber attacks.

Key Words: Cyber, Cybersecurity, Transition of Security Perception, Cyber Attacks, Globalization.

[*] Master Öğrencisi, Kocaeli Üniversitesi, İİBF-Uluslar arası İlişkiler Bölümü, E-mail: onrylmz1993@gmail.com

GİRİŞ

Küreselleşme ortaya çıktığı ilk andan itibaren hem olumlu hem olumsuz anlamda birçok gelişmeyi de beraberinde getirmiştir. Küreselleşmenin ne olduğu üzerine birçok tartışma bulunmasına rağmen; üzerinde mutabakat sağlanan nadir özelliklerinden biri yönü onun değiştirici ve dönüştürücü özellikleridir. Küreselleşme hayatın her yönünde ve her aktöründe bir değişim işlevi görmüştür ki bireyler, ekonomi, toplum, kültür, devletler ve sistemler de buna dâhildir. Diğer taraftan ekonomi, siyaset, toplum, kültür ve hatta bireylerin bu sürece uyum göstermesi ulus devletlere nispeten daha az sancılı olmuştur. Ulus devletler, küreselleşmenin kendilerine etkilerinin fazla olmayacağını, uluslararası alanda egemenliklerine bir tehdit doğurmayacağını düşünmüş olsalar da sonrasında ekonomik anlamda egemenlikleri çokuluslu şirketlerce; dış egemenlikleri uluslararası ve ulus ötesi örgütlerce; iç egemenlikleri sivil toplum örgütlerince müdahalelere konu olunca bu sefer de küreselleşme kavramına endişe ile yaklaşmışlardır.

Günümüzde ise küreselleşme sürecinin değiştirici ve dönüştürücü özelliklerinin yadsınamaz gerçekliği devletler tarafından da kabul edilmekte ve bu anlamda tespitler yapılmakta, olumsuz olabilecek etkileri anlamında ise önlemler alınmaktadır. Ulus devletlerin egemenlik, sınırsal belirlilik ve güvenlik üzerinde temellendiği düşünüldüğünde bu üç olgunun da küreselleşme ile değişime ve dönüşüme uğradığı bir gerçektir. Makalede ise bu üç olgudan küreselleşmenin güvenlik üzerinde oluşturduğu değişim ve bu değişimin bir parametresi olarak ortaya çıkan siber güvenlik üzerinde durulacaktır.

Bilindiği üzere Westphalia barışı sonrası ortaya çıkan yenidünya düzeninde sistemin yeni oyuncuları ulus devletler olmuş; dolayısıyla uluslararası sistem de bu aktörler üzerinden tanımlanıştır. Westphalian sistemin özünde ise realist bir okumanın olduğu aşikârdır. Nitekim güvenlik algılaması da bu anlamda realist bir algılamayla tanımlanmıştır. Buna göre güvenlik, devletlerin uluslararası alanda var olabilmeleri için olmazsa olmazdır. Öyleyse devletler somut güç araçlarını etkinleştirmeli, savunma ve saldırı kabiliyetlerini arttırmalıydılar. Güçlü bir askeri ordu aynı zamanda devletlerin uluslararası sistemde başat aktör olabilmeleri adına önemli bir unsur sayılmaktaydı. Sistemin temel aktörleri olarak ulus devletlerin görülmesi tehdit yaratabilecek unsurların da genel anlamda devlet odaklı olacağı düşüncesini

doğurmuştur. Fakat küreselleşmeyle birlikte bu güvenlik yaklaşımının pek de geçerli olmadığı görülmüştür. Realist paradigmanın yön verdiği, merkezi orduların güç potansiyelleriyle ve belirli sınırlar üzerinden algılandığı güvenlik olgusu da değişime uğramıştır. Çünkü artık sistemde sadece devletler değil, çokuluslu şirketler, ulus ötesi örgütler, küresel terör örgütleri, sivil toplum örgütleri gibi yeni yapılar ve yapılanmalar da var olmuştur.

Küreselleşmenin getirmiş olduğu birbirine bağlılık, bağlantılılık ve bağımlılık ilişkileri içerisinde dünya üzerinde var olan her şey birbiriyle ilişkili hale gelmektedir. Özellikle teknolojinin de gelişmesi ve yaygınlaşmasıyla birlikte bu bağlantılar mesafeleri engel tanımaksızın gelişmekte ve iç içe geçmektedir. Bilgisayar sistemleri, kodlama programları ve diğer dijital gelişmelerle saniyelerle ölçülebilecek kadar kısa süreler içerisinde bu bağlantıları kurma ve kurulan bağlantıları harekete geçirme imkânı da kolaylaşmıştır. Küreselleşmenin bütün bu olanakları sunmuş ve sunuyor olması da diğer taraftan devletleri güvenlik yönünden yeni bir tehlikeyle yüz yüze getirmektedir: Siber güvenlik.

Küreselleşme sonrası değişen güvenlik algılamaları paralelinde, küreselleşmenin ulus devletleri en çok zorladığı alanlardan biri de şüphesiz siber güvenlik alanı olmuştur. Çünkü hemen hemen bütün ulus devletlerde teknolojiyle birlikte bir dijitalleşme meydana gelmiştir ve bu dijitalleşmeden devletlerin bürokratik, ekonomik, politik ve hatta savunma sistemleri de payını almıştır. Yani artık devletler de hemen hemen birçok alanda ve kurumlarında dijitalleşmeyi gerçekleştirmişler, hizmetlerini çevrimiçi olarak sunmaya başlamışlardır. Bu durum yeni güvenlik tehditleri ortaya çıkarmıştır ki bu tehditlerin hepsi sadece devletler tarafından değil bireyler, şirketler, suç örgütleri, dolandırıcılar ve hatta küresel terör örgütleri tarafından yaratılmaktadır. Bu oluşumlarla mücadele etmenin yolu ise askeri anlamda ordular değil, siber alanda oluşturulacak olan siber ordular olarak düşünülmektedir. Siber güvenlik alanı devletlerin uzun bir süre kavrayamadıkları ve yeteri önemi vermedikleri bir alandır. Ancak siber saldırıların devletleri kilitleyebilecek duruma getirebileceğinin örnekleri görüldüğü zaman bu alanın ciddiyeti kavranabilmiştir.

ABD, Rusya, Çin ve NATO gibi güçlü yapıların dahi siber saldırılara maruz kaldığı düşünüldüğünde siber alandaki güvenlik okumalarının yeniden düşünülmesi gerektiği devletler tarafından da anlaşılmıştır. Yeni rekabet alanlarından biri olan siber uzay, hem devletlerin birbirleriyle yarışacağı hem de birbirlerinden, küresel terör örgütlerinden, suç

organizasyonlarından ve hatta bireylerden gelebilecek tehditleri bertaraf etmeleri gereken yeni bir durum yaratmaktadır.

Makalede öncelikle küreselleşme ile değişen güvenlik algısından bahsedilmiş ve bu anlamda yeni olan siber güvenlik alanı ve bu alana dâhil kavramsal çerçeveye yer verilmiştir. Daha sonra kavramların ve değişen güvenlik algısının devletlere ne gibi tehditler getirdiğinin anlaşılabilmesi adına siber alanda gerçekleşen önemli saldırılara örnekler verilmiştir. Devletlerin bu siber saldırılar sonrası güvenlik algılamalarında ne gibi değişikler olduğu üzerinde durulmuş, yeni güvenlik mekanizmaları ise bu başlıklar altında incelenmiştir.

Küreselleşmenin Güvenlik Üzerine Etkileri

Küreselleşme her ne kadar üzerinde mutabakata varılamamış bir kavram olarak belirse de, kabul edilen en önemli özelliği onun değiştirici ve dönüştürücü etkileridir. Bu etkisiyle de özellikle 1990 ve sonrası dönemde hızlı bir şekilde yoluna devam eden bu süreç klasik kabullerle şekillenmiş siyaset, ekonomi ve güvenlik tanımlamalarını, algılarını ve kavramsallaştırmalarını da değiştirmiş ve dönüştürmüştür. (Erdoğan, 2013: s. 266).

Küreselleşme süreciyle beraber güvenlik algılamasının nasıl değiştiği üzerinde durabilmek adına; klasik anlamda realizmin sınırlarını çizdiği güvenlik algısından bahsetmek gerekecektir. Realizmin klasik güvenlik kavramının özünü ve sınırlarını çizdiği açıktır. Klasik realist teoride güvenlik; devletlerin tekelinde ve anarşik olan uluslararası sistemde bir güvensizlik ortamında şekillenmektedir. Bu anlamda güvenlik kavramı bizatihi devletlerin sahip olduğu askeri güç ile orantılı ve büyük ölçüde bağlantılı olduğu düşünülmektedir. (Sandıklı ve Emeklier, 2014: s. 5). Bu anlamda kurulan Westphalian düzen de bu realist paradigma ekseninde, hem başat aktörlerin devlet olması hem de genel anlamda güç ilişkileri üzerinde temellenen bir sistem öngörmüştür. Fakat küreselleşmenin ortaya çıktığı dönemde ne devletler artık uluslararası arenada tek aktördürler ne de etkileme kapasiteleri askeri güçleriyle sınırlıdır.

Tüm alanlarda devleti egemen güç olarak gören realist paradigma özellikle uluslararası örgütler paralelinde ekonomik anlamda bu hakimiyetini sorgulatır hale gelmiş, daha sonra ulus ötesi (Aksoy, 2016: s. 3). Yapılanmalar baş gösterince siyaset yapmada, dış politika yapmada, iç politikada sınırsız bir egemenlikten taviz verir hale gelmiştir. Ekonomik, politik alanlardaki bu

değişimlerden güvenlik algısı da payını almıştır. Özellikle bir tehditle karşılaşıldığında, klasik realist çerçeveden bunun bir askeri çözümle halledilmesi gerektiği anlayışı yavaş yavaş terk edilmiştir. Çünkü tehdit kaynağının sadece bir diğer devlet olması durumu söz konusu değildir. Güvenlik artık sadece devletlerarası bir ilişki değil, daha çoğul ve çoklu bir görünüme evirilmiştir. Güvenlik alanındaki bu çeşitlenmenin kaynağında küreselleşmenin olduğu açıktır. Fakirlik, çevre sorunları, salgın hastalıklar, iç çatışmalar, soykırım, nükleer, radyolojik, biyolojik silahlar, küresel terörizm, uluslararası suçlar (Demiray ve İşcan, 2008: s. 155) gibi birçok yeni güvenlik sorunu devletlerin başa çıması ve vatandaşlarını koruması gereken diğer taraftan onun egemenliğini sorgulayan ve hatta sorgulatan bir sürece götürmüştür.

Küreselleşmenin en önemli özelliği; onun sınırları yumuşatma, belirginsizleştirme ve hatta birçok manada da birleştirmesidir. Özellikle teknolojik gelişmeler sonrası artık dünyanın her bölgesi, birbiriyle ilişkili ve etkileşimli hale gelmiştir. Bu manada devletlerin artık iç egemenlik-dış egemenlik alanları da belirginsizleşmiş, paralelinde iç güvenlik-dış güvenlik ayrımı da anlamını eskisine oranla yitirmiştir. Teknolojik gelişmelerle beraber her ne kadar devletler daha teknolojik ve yıpratıcı silahlar elde etmişlerse de bunları kullanma kabiliyetleri de eskisine oranla azalmıştır. Çünkü küreselleşmenin getirdiği bilgi yayılımı, bir devletin kazandığı askeri anlamda üstünlüğü diğerinin de takip etme ve aynısını kısa bir sürede kazanma-elde etme olasılığını arttırmıştır. Diğer taraftan bu teknolojik silahların kullanılmasının sınırlandırılmasına yönelik uluslararası toplum nezdinde antlaşmalar da imzalanmıştır. Böylece mesela; nükleer bir silaha sahip olmak devletler için her ne kadar daha güvenlikli hissedilmesini (Adaoğlu, 2008: s. 9) sağlasa da hem bunun birçok devlet tarafından kısa bir sürede edinilmesinden hem de 1925 Cenevre Protokolü uyarınca bu silahların kontrol altına alınmış olması bu manada kullanılmasının önünde engelleyici bir durum yaratmaktadır. Şüphesiz bunun altında yatan ana etmenlerden birisi de devletlerin özellikle bu alanda tek başına karar verme ya da gücü oranında bu silahları kullanabilme yetisini elinden alan; küreselleşme süreciyle etki alanı bulmuş olan sivil toplum örgütleri, insan hakları platformları gibi yeni aktörler olmuştur.

Yeni aktörlerden biri olan ve bu anlamda güvenlik dönüşümünün nasıl keskin olabileceğinin anlaşılması yönünden en iyi örneklerden biri de küresel terörizm ve küresel terörist örgütlerdir. Çünkü bu örgütler de artık hem nükleer silahlara sahip olabilmekte hem de bunları kullanarak küresel anlamda terör faaliyetleri uygulayabilmektedir. (Sancak, 2013: s. 130). 11 Eylül 2001 terör saldırıları küresel terör örgütlerinin, küresel faaliyetlerinin ulus devletlerin, Westphalian

güvenlik anlayışının yani realist güvenlik anlayışının eksik yönlerini daha doğrusu miladını doldurduğunu göstermesi açısından önemlidir. 11 Eylül saldırılarının Küreselleşmeyle bağlantılı bir noktada durmasının en önemli nedeni; saldırıyı gerçekleştiren örgütlerin oluşum süreçlerinde de küreselleşmenin getirdiği şartların yatmasıdır. Öyle ki küreselleşme; El-Kaide gibi terör örgütlerinin, terör faaliyetlerini yapmalarını kolaylaştırmıştır. Çünkü bu örgütler bilgi ve teknolojinin yaygınlaşmasıyla, uluslararası örgütleri taklit ederek kendi örgütsel şemalarını oluşturabilmekte, kuruldukları bölgenin çok çok uzağındaki yerlerle iletişim imkânlarını bulabilmekte, para aklama yöntemleriyle de kendilerine finansman sağlayabilmektedir. Özellikle küreselleşmeyle beraber çok küçük maliyetlerle, telekomünikasyon teknolojisi (Türköz, 2016: s. 154) yardımıyla da büyük tahribatlar yaratabilmektedirler. Sınırların eskisi kadar sert ve denetimli olmaması da bu durumu kolaylaştırmaktadır.

Küreselleşmenin bütün kolaylıklarından faydalanarak 11 Eylül gibi bir terör hareketi gerçekleştirebilen bir örgüt; devletlerin uluslararası alanda etkileme kabiliyeti olan tek aktör olmadığını, realist paradigmanın bu anlamda yanıldığını, dahası klasik anlamda güvenlik tanımlamalarının da artık geçerli olmadığını göstermiştir. Küreselleşmeyle beraber artık ülkeselliğin, tehditleri dışarıda tutma özelliğini yitirdiği gerçeğiyle karşı karşıya kalınması, güvenlik kavramının genişletilmesi ve yeniden düşünülmesi gerektiğini de gün yüzüne çıkarmıştır. (Ağır, 2011: s. 159).

Devletler, bu değişen güvenlik durumuna yeni önlemler getirmek gerektiği inancına varmış olsalar da küreselleşmenin getirdiği bir diğer olguyla da karşı karşıya kalmaktadırlar ki bu yeni güvenlik perspektifine de hazırlıklı olmadıkları bir gerçektir: Siber Güvenlik.

Siber İle İlgili Kavramlar

Siber politika ve siber güvenlik konuları, sosyal bilimlerde henüz hak ettiği değeri bulamadığından, bu alanda - giderek artsa bile - yapılan çalışma sayısı arzu edilenin çok gerisindedir. Bu nedenle, siber politika ile ilgili çalışmalarda hala kavramsal tartışma önem arz etmektedir. Bu makalede de başta siner olmak üzere, siber uzay, siber tehditler ve siber güvenlik gibi kavramların tartışılmasında yarar görülmüştür.

Siber Nedir?

Siber terimi; sibernetik kelime kökünden türetilmiş olup ilk olarak 1958 yılında canlılar ve makinalar arasındaki iletişim disiplinini inceleyen Sibernetik biliminin babası sayılan Louis Couffignal tarafından kullanılmıştır. (Sesli Sözlük, 2017). Yalnız güncel anlamda bu kavram kullanıldığında sanal alan ve bu alana ilişkin olarak anlaşılmaktadır.

Siber Uzay Nedir?

Siber Uzay, siber olana yönelik en geniş kavram olarak karşımıza çıkmaktadır. Çünkü siber uzay; bilgisayar ağları ve bu ağlar vasıtasıyla ulaşılabilen her türlü veri kaynağını kapsayan alan olarak tanımlanmaktadır. (Karaçay, ty: s. 1). Yani telefon, radyo, televizyon gibi elektronik olarak kumanda edilebilen her türlü cihaz, kayıt edilebilen ses ve görüntüler, grafikler, projeler, banka işlemleri, e-ticaret, e-devlet üzerinden yapılan her türlü işlem de ayrıca siber uzay tanımlamasına tabidir.

Siber uzaya yönelik bir diğer tanım ise ABD Savunma Bakanlığı tarafından yapılmıştır. Buna göre siber uzay; ‘‘İnternet iletişim ağları, gömülü işlemci ve kontrol birimlerini içeren, bilgi teknolojileri altyapılarından meydana gelen, bir birine bağlı ağların oluşturduğu bilgi ortamındaki bir küresel alandır.’’ (Ceylan, 2014: s. 1).

Her ne kadar siber uzay ya da siber ortam internetle birlikte ve bağlantılı bir kavram olarak düşünülse de, siber uzay internetten çok daha fazlasını ifade etmektedir. Çünkü gerçek dünyada meydana gelmeyen bir işlem dahi, siber uzayda meydana gelebilir kabiliyettedir. Örneğin basit bir çipteki hesaplama dahi bir siber uzay olayıdır ki bunun yapılması sırasında herhangi bir internet bağlantısı da gerekmemektedir. (Fentz, 2005: s. 1).

Bazı tanımlamalarda ise siber uzayda birer kullanıcı olarak cihazlardan cihazlara da bir iletişim ve etkileşim olabileceği anlaşılmaktadır. Fakat çalışmada bu tanımlamaları dikkate almamak durumunda kalınmaktadır çünkü çalışmada asıl olan insan amaçlarının siber uzaydaki etkileri ve sonuçlarıdır. (Ottis and Lornes, ty: s.1).

Siber Tehdit Nedir?

Kişisel ve kurumsal verilerin gizliliğini yasal olmayan şekillerde aşarak bunlara ulaşmak veya tahrip etmek amacıyla yapılan her türlü siber saldırı ve saldırı girişimine siber tehdit denir. Sunucu web servis hizmetlerini durdurma, virüsler veya trojenler bu tehditlere örnek olarak verilebilir. (Şahinaslan, 2003: s. 2-8).

Siber tehditler gelişen bilişim sistemleriyle beraber hem devlet hem de devlet dışı aktörler için; yeni tehditler ortaya çıkarmaktadır ki bu tehditlerin soyut alandan geliyor olması, tespit edilebilme özelliğinin az olması gibi etkenler, tehditlerin sonuçları açısından bir öngörülmezlik durumu doğurmaktadır. Bir diğer taraftan bu tehditlerin merkezi bir yapıya sahip olmaması da belirsizliğini arttırmaktadır. Bu anlamda tehdidin kaynağı tek bir birey (hacker); birey toplulukları (hacker grupları), terör örgütleri veya bizatihi devletler de olabilmektedir. (Kurnaz, 2016: s. 65).

Siber Tehdit Türleri

Teknolojik gelişmenin hızla artması ve küreselleşmeyle beraber, dünyada iletişim ve bağlantılılık yönünden çok sıkı bir ilişki söz konusu olmuştur. Bu durumun iyi yönleri olduğu gibi güvenlik alanında olduğu gibi tehlikeli bir durum da oluşabilmektedir. Siber saldırılar - fiziksel altyapıya yönelik saldırılar ve sosyal mühendislik dışında - genellikle internet üzerinden yapılan saldırılar olarak gerçekleşmektedir ki bunları şöyle sıralayabiliriz;

1) Bilgi ve istihbarat sağlama amacıyla kullanılan casus yazılımlar aracılığıyla yapılan saldırılar,
2) Portal ve internet hizmetinin aksatılması veya engellenmesine yönelik yapılan saldırılar,
3) Yemleme(phishing) olarak adlandırılan ve illegal yollardan yanıltma amacıyla yapılan saldırılar,
4) İstem dışı elektronik posta olarak adlandırılan Spam yöntemiyle zararlı dosyalar göndererek yapılan saldırılar,
5) Ağ trafiğini dinleyerek yapılan saldırılar, (Şahinaslan, 2003: s. 8).
6) Sosyal medya kullanarak yapılan saldırılar,
7) Sosyal Mühendislik,
8) Arama Motorları,
9) Ücretsiz Web Hizmeti Sunma.

Bu siber saldırı araçlarıyla etki yaratmak isteyen grupların temelde farklı hedefleri olmasına rağmen bu amaçlar aşağıdaki şekilde özetlenebilir;

1) Devletler genellikle düşman ya da hedef devleti, örgütü zayıflatmak, çökertmek, istihbarat sağlamak adına,
2) Siyasi örgütler kendi amaçları doğrultusunda toplumu manipüle etmek, propaganda amacıyla,
3) Kurum içi veya kurum dışı rakip ya da düşmanlar haksız rekabet araçlığıyla sektörde üstünlük sağlamak adına,
4) Suç örgütleri propaganda yapmak, ekonomik olarak finanse edilmek ve militan devşirmek amacıyla bu saldırıları gerçekleştirebilirler. (Çetinkaya, 2011: s. 1).

Peki, bu saldırılarla ne amaçlanmaktadır ya da neler yaşanabilir?

Telekomünikasyon şirketlerine sızılarak istihbarat sağlanabilir, özel bilgiler elde edilebilir, özel hayat ifşa edilebilir.

1) Nükleer tesislerde yangın çıkarılıp patlama yapılabilir.
2) Uçaklar havada çarpışabilir
3) Bankacılık sektörü tamamen işlemez hale getirilebilir.
4) Elektrikler kesintilerine sebebiyet verilebilir.
5) Sağlık bilgi sistemleri ele geçirilerek hasta kayıt bilgileri çalınabilir.
6) Hava yolları, hava ve deniz kontrolleri, demiryolları, otoyollar ve sinyalizasyon sistemleri gibi ulaşım sistemleri ele geçirilerek sistemin işleyişine müdahaleler gerçekleştirilebilir.
7) Medya kurumlarına yapılan müdahalelerle karşı propaganda içerikleri paylaşılabilir hatta ülkenin tamamen uluslararası toplumla iletişimi kesilebilir.

Bütün bu tehditlerin gerçekleştirilmesi ise son derece basit ve az maliyetli şekilde olabilmektedir. Dünyanın herhangi bir yerinde internete bağlı olunması koşuluyla bu saldırılardan birini gerçekleştirmek bugünkü teknolojiyle mümkün olmuştur. Bu nedenle devletlerin siber tehlikelerden kendilerini koruyabilmeleri için; kendi siber güvenlik alanlarını oluşturmaları bir zorunluluk halini almaktadır.

Siber Güvenlik Nedir?

Siber ortamda var olan bilişim sistemlerini saldırı ve tehditlerden korumak, bu ortamda korunmak istenen bilginin gizliliğini sağlamak, bu tehdit ve saldırıların mahiyetini ve kaynaklarını tespit etmek, bu müdahalelere karşı müdahaleler ve hamleler geliştirmek amacıyla oluşturulmuş olan ulusal hukuk, uluslararası hukuk ve insan haklarına uygun her türlü önlem ve sistemleri siber güvenlik olarak tanımlayabiliriz. (Kara, 2013: s. 5-6)
Bir diğer tanımlama yine paralellik göstermektedir. Buna göre siber güvenlik; siber uzayda kullanıcıların ve kurum-kuruluşların güvenliklerini sağlamak amacıyla kullanılan; araçlar, güvenlik politikaları, kılavuzlar, eğitimler, uygulamalar, güvenlik teminatları ve her türlü teknolojik altyapılanmadır. (Bilgi Teknolojileri ve İletişim Kurumu[BTK], 2008: s. 1-13).

Bu güvenlik önlemleri sayesinde, siber tehditler yok edilebilmekte yahut etkileri azaltılabilmektedir. Bu önleyici adımları atmak yakın zamanda hayati öneme haiz olmuştur. Çünkü siber saldırılar bir ülkedeki bütün hayatı durdurabilecek, felaketlere yol açabilecek mahiyette gerçekleşmektedir ki yakın zamanda Estonya'ya yapılan siber saldırı bu anlamda iyi bir örnek teşkil etmektedir. Tehditlerin hızlıca artarak güvenliği tehlikeye düşürmesi sonucu birçok devlet, güvenlik politikalarında siber güvenlik konusuna da yer vermek durumunda kalmışlardır. Bu anlamda devletler özellikle bu politikaları hayata geçirmek adına kalifiye kadroları oluşturma, altyapı hizmetlerini sağlamak gibi büyük yatırımlar yapmaktadırlar. (Yıldız, 2014: s. 58).

Görüldüğü üzere yeni güvenlik paradigmasına paralel olarak, siber güvenlik tanımlamalarının hiçbirinde somut anlamda ordulardan, silahlardan ve hatta diplomasiden bahsedilmemektedir. Buradan yola çıkarak yeni güvenlik algılamasının da devletler nezdinde anlaşılabilmesi adına bu perspektifi edinebilmeleri gerekmektedir. Güç olgularını sadece iyi, disiplinli, modern silahlarla donatılmış ordular üzerinden algılayan devletlerin, siber alandaki tehditlere göğüs geremeyecekleri de aşikârdır.

Devletlerin temel olarak siber alanında öncelikli olarak güvenliklerini sağlamaları gereken alanlar; bilişim, enerji, mali işler, gıda, sağlık, su, ulaşım, kamu güvenliği, savunma, nükleer-biyolojik ve kimyasal tesislerdir. (T.C Ulaştırma Denizcilik ve Haberleşme Bakanlığı, 2012: s. 12). Özellikle savunma tesisleri ve araçlarında dışa bağımlı ülkeler adına, siber alanda tehlikeler de büyümektedir. Çünkü yeni savunma araçlarının hemen hemen hepsi siber alanda kontrol edilebilmekte ve bu anlamda kodlamalar üretici diğer ülke veya şirketlerin müdahalesiyle

yönlendirilebilmektedir. Bu anlamda özellikle kritik düzeydeki bu alanlarda milli teknolojilerin üretilip kullanılması temel öncelik olmalıdır.

Ulus devletler siber alanda birincil nitelikteki hedeflerden ilkini teşkil etmektedirler. Çünkü organize suç örgütlerinin siber alanda hareket kabiliyetleri artarken ulus devletlerin bu alanda görece yavaş kaldıkları görülmüştür. Her ne kadar bu terör organizasyonları bu alanda hareket kabiliyeti bulabiliyor olsalar da devlet kurumsallığı, istikrarı ve finansmanı gibi özelliklerden yoksun olmaları devletler tarafından avantaja çevrilebilir.

Her ne kadar siber alanda asıl hedeflerin ulus devletler, tehdit kaynaklarının da terör organizasyonları, suç örgütleri, bireysel dolandırıcılar olduklarını düşünsek de bu alanda devletlerin de birbirlerine rakip oldukları, üstünlük arayışı içinde oldukları da açık ve kesindir. Yakın zamanda siber saldırıların artması ve bu saldırıların devletleri işleyemez, yönetilemez duruma düşürebileceği gerçeğini ortaya koyması sonucu Birleşmiş Milletler, AB ve NATO gibi uluslararası örgütler de siber güvenlik alanında önlem almak durumunda kalmışlardır.

Eurastat tarafından yapılan araştırmaya göre AB üyesi ülkelerde internet kullanıcılarının siber alanda tehditle karşılaşma oranları %25 olarak gerçekleşmektedir. Bunun anlamı AB üyesi ülkelerdeki her dört kullanıcıdan biri güvenlik sorunlarıyla karşı karşıya gelmektedirler. Birlik içerisinde en fazla tehditle karşılaşan ülkeler %42, %39 ve %36 ile sırasıyla Hırvatistan, Macaristan ve Portekiz iken; en az tehditle karşılaşan ülkeler ise %10, %11 ve %13 ile sırasıyla Çek Cumhuriyeti, Hollanda ve Slovakya'dır. (Eren, 2017: s. 36). Bu araştırmadan da yola çıkarak AB'nin bu alanda politikalar geliştiriyor olması, güvenlik önlemleri alıyor olması da gayet doğal karşılanmaktadır.

2005 yılı Eylül ayı itibariyle de Avrupa Ağ ve bilgi Güvenliği Ajansı (ENISA) faaliyetlere başlamıştır. 2007 yılında ise Avrupa Polis Ofisi (EUROPOL) öncülüğünde ''Web'i Kontrol Et'' adında bir program başlatılmıştır. Yine 2010 yılında Avrupa Birliği Bakanları, kurulan siber güç ajansına gerekli teşviklerin sağlanması adına Komisyona çağrıda bulunmuştur. Avrupa Polis Ofisi e-dolandırıcılık, spam, botnet, internet üzerinden kimlik hırsızlığı, menkul kıymetler borsasında faaliyet gösteren hackerlar, yazılım yoluyla yöneltilen tehditler ve bazı cihazlardan kaynaklanan güvenlik eksiklikleri konusunda güvenlik önlemleri almakta, çeşitli sistemler oluşturmaya çalışmaktadırlar. AB idari birimleri tarafından bildirildiği üzere bu sistem ve çalışmaların maliyeti 750 milyar Euro'ya mal olmaktadır. (Yıldız, 2014: s. 93).

NATO ise özellikle 2000 yılından sonra siber tehditlere maruz kalınca bu alandan bir politika geliştirmek durumunda kalmıştır. Özellikle 1999 yılında NATO'nun Sırbistan müdahalesi sonrası Çin ve Rusya orijinli olduğu düşünülen siber saldırılar NATO'nun da bu tarz saldırılara karşı zayıf olduğu gerçeğini ortaya koymuştur. Bu münasebetle 2002 Prag Zirvesi'nde Siber Savunma Programı kabul edilmiş ve üye devletlerin ve NATO'nun bu tarz siber saldırılara karşı korunması gerektiği vurgulanmıştır. Mukabilinde Bilgisayar Olaylarına Müdahale Gücü Teknik Merkezi, Prag Yetenekler Taahhüdü, Kapsamlı Siyasi Yönerge gibi araçlarla bu alanda savunma teknikleri gerçekleştirilmeye çalışılmıştır. Estonya'ya yönelik yapılan siber saldırılar sonucu, ülkenin haftalarca yönetilemez hale gelmesi sonucu, NATO da siber güvenlik meselesini öncelikli risk alanı olarak kabul etmiştir. (Seren, 2006: s. 16-17).

Tüm bu adımlarla beraber NATO'nun amacı üye ülkelerde olası siber tehditlere karşı anında ve hızlı bir şekilde müdahale ederek, tehditleri bertaraf etmektir. Nitekim NATO gibi büyük bir askeri gücün, karar alma mekanizmaları açısından etkinliği uluslararası sistemde birçok devletten daha üstün nitelikteki yapısıyla üyelerine bu alanda da güvenlik sağlaması beklenen bir durumdur.

Güvenlik kavramının bu derecede değiştiği, dönüştüğü bir ortamda ulus devletlerin de bu alanda varlıklarını sürdürebilmeleri adına, adapte olabilme kabiliyetleri son derecede önem arz etmektedir. Realist paradigmanın önceledığı manada bir güvenlik algılamasının tek başına yeterli olmadığı bu gelişmeler karşısında devletlerin egemenliklerini kanıtlamaları gereken yeni bir alan olmuştur siber uzay…

DÜNYA'DA SİBER SALDIRI ÖRNEKLERİ

Siber güvenlik saldırılarına gerçekleşmiş örnekler üzerinden yaklaşmak hem konunun anlaşılması adına, hem de güvenlik sorunsalının ne denli tehlikeli olabileceğini kavramak açısından son derece önemlidir. Bu anlamda bir siber savaş durumunun yaşandığı olaylar da mevcuttur ki bu savaşların hiçbiri realist paradigmada öngörüldüğü üzere askeri ordularla yapılmamaktadır.

Bu da bizlere göstermektedir ki yeni güvenlik anlayışı, yeni güvenlik önlemleri yaratılması gereken bir mahiyettedir. Aksi takdirde, aşağıda örneklerini göreceğimiz şekilde vahim sonuçlarla karşılaşılabilir, normal hayatın seyri beklenilmedik müdahalelere maruz kalabilir ve devletlerin yönetme kabiliyetleri dahi elinden alınabilir.

Siber saldırılar elbette sadece devletlerarasında gerçekleşmemektedir. Çok taraflı saldırıların gerçekleştiği bir alan olarak siber alanın aktörleri bireyler, terör örgütleri, aktivist örgütlenmeler ve devletler olabilmektedir. Diğer taraftan bu grupların da birbirleriyle sürekli etkileşim içerisinde oldukları gözlemlenebilmektedir. Yani devlet gibi bürokratik ve merkezi yapılanmalar, tek bir birey tarafından siber alanda tehlike altında kalabilmektedir.

Çalışmada ise esas güvenlik tartışması ve aktör olarak devlet temellendirildiği için devletlerarasında cereyan eden ve siber savaş olarak niteleyebileceğimiz siber saldırı ve savaşlardan bahsedilecektir.

Sibirya Doğalgaz Patlaması (Logic Bomb)

1982 yılında Sibirya'da doğalgaz boru hatlarına yönelik yapılan siber saldırılar sonucu meydana gelen büyük patlama, siber anlamda da ilk saldırı olma niteliği göstermektedir. Çünkü ilk defa siber teknolojiler kullanılarak bir saldırı düzenlenmiştir.

Bu siber saldırının aktörleri ABD ve Sovyet Rusya olmuştur. ABD öncülüğünde Sovyetler Birliği'ne ambargo uygulanan bu yıllarda, Sovyetler bu ambargoyu bir şekilde aşmak niyetiyle Kanada'da bir şirketin doğalgaz boru hatlarını kontrol etmekte kullandıkları sistemi ele geçirmişlerdir. Aslında tam olarak ele geçirdiklerini düşünmüşlerdir oysa ABD bu girişimin farkına varmış ve CIA (Amerikan Haberalma Örgütü) bu yazılımların içerisine ''*Logic bomb''* (www.gizmocrazed.com, ty: s. 1). adında bir nevi saatli bomba yerleştirmiştir. İşte 1982 yılında gerçekleşen bu büyük patlamanın arkasında yatan basit bir aldatmacayla yapılan siber saldırıdır. (Tandoğan, 2010: s. 1).

Bu olaya mukabil yeni güvenlik anlayışının ve savaş alanının siber alana kaydığı ve artık bu alanda egemenlik sağlanılması gerektiğinin anlaşılması adına önemli bir örnek olmuştur.

Ay Işığı Labirenti (Moonlight Moze)

Siber saldırı tarihine ‘’Moonlight Moze’’ olarak geçen bu saldırı ABD’nin NASA, ABD Enerji Bakanlığı, Pentagon ve üniversitelerine yönelik olarak gerçekleşmiş; askeri haritalar, askeri tesislere ait bilgiler üniversite araştırma-geliştirme projeleri gibi son derece gizli bilgiler çalınmıştır. (Işık, 2017: s. 1).

Saldırıların arkasında her ne kadar kabul etmeseler de Rusya’nın olduğu ABD tarafından yapılan teknik takiplerle tespit edilmiştir. CIA bu saldırıyı daha önce benzeri görülmemiş şekilde koordineli bir saldırı olduğunu açıklamıştır. (Doman, 2016:cs. 1). Yani CIA daha baştan bunun arkasında bir devletin olduğunu belirtmiş ve bu tarz bir siber saldırının bir grup hacker tarafından yapılamayacağını belirtmiştir.

ABD’nin de bu saldırıyı tespit etmesi aslında 2 yıl gibi uzun bir süre almıştır. Çünkü saldırı aslında 1996 yılından itibaren şekillenmeye başlamış, 1998 yılında ise ABD bu sızmayı tespit edebilmiştir. (Hürriyet Gazetesi, 2017)

Bu saldırı ABD gibi bir süper gücün dahi, siber alanda tehditlere maruz kalabileceğini ve bu tehditlerin boyutlarının ne denli ağır olabileceğini göstermesi açısından çok önemlidir.

Kosova Krizi-NATO

NATO 1990’lı yıllarda Yugoslavya’nın da sonunu getiren çatışmalarda zaman zaman müdahalelerde bulunmuştur. Özellikle NATO’nun 1999 yılında yapmış olduğu hava saldırıları sonrası Sırp lider Miloseviç’in sonunu getirmiş olması, beraberinde birçok eleştiri de getirmiştir. Bu eleştirilerin harekete geçirdiği grupların bazıları ise hackerlardı ki özellikle NATO’nun bilgi sistemlerine yaptıkları basit sızmalarla ses getirmeyi başarmışlardır. NATO’nun siber uzaydaki gücünün sorgulanmasına sebep olan bu saldırılar neticesinde gerekli adımları atmak gerektiğini düşünen NATO, 2002 Prag Zirvesi’yle siber olaylara anında ve etkili bir şekilde müdahalede bulanabilecek bir merkez oluşturmasını kararlaştırmıştır. (Yener, 2014: s.1).

Saldırılar süresince NATO kendi içerisindeki koordinasyonu sağlayamamış, üye ülkelerle online iletişime geçememiştir. Bu saldırıların önemli bir özelliği ise NATO'ya karşı yapılan ilk siber saldırı olmasıdır. Soğuk Savaş süresince karşısında somut düşmanları olan NATO doğal olarak savunma stratejilerini de bu yönde oluşturmuştur. Fakat Soğuk Savaş sonrası dönemde artık bu güvenlik algısının değiştiği ve yeni savunma teknikleri oluşturma ihtiyacının doğduğu da bu saldırılar neticesinde NATO nezdinde de anlaşılmıştır.

Estonya'ya Yönelik Siber Saldırılar

Estonya 1991 yılında bağımsızlığını ilan ettikten sonra yıllar içerisinde teknoloji ve iletişim alanında büyük reformlar gerçekleştirerek, Avrupa içerisinde en kablolu ülke olma yoluna girmiştir. Ülkede yaşayan vatandaşlarının %65'ten fazlasının internete erişim sağlayabildiği ülkede, hükümet fonksiyonlarının birçoğu da çevrimiçi ortamda yapılabilmektedir. Bu işlemlerin içerisinde bankacılık işlemleri, vergi ödeme işlemleri ve hatta oy verme işlemleri de dâhildir. Estonya adına söylenmesi gereken bir diğer önemli husus ise meclislerince internet ulaşımının bir temel insan hakkı olarak nitelendirilmesidir. (W. Beidleman, 2009: s. 2-5). Bütün bu teknolojiyle iç içe geçmişlik Estonya'yı siber uzayda bir hedef haline getirdiğinde ise bu olumlu hava tersine dönmüştür.

2007 yılına gelindiğinde Estonya hükümeti, İkinci Dünya Savaşı'ndan (SSCB dönemi) kalma Tallinn şehrindeki Bronz Asker Heykelini şehrin dışına taşımak isteyince özellikle ülkede yaşayan Ruslar bu duruma büyük tepki göstermişlerdir. (Boyraz, 2015: s. 32-40). Bu tepkiler 27 Nisan 2007 tarihine gelindiğinde ise Rusya'nın da müdahil olduğu bir şekle bürünerek siber saldırı niteliğine dönüşmüştür. Estonya gibi iletişim ve teknolojik ilerlemenin her türlü faydasından yararlanabilen ve Avrupa'da bu anlamda önemli bir yere sahip olan ülkede üç hafta boyunca hayat durma noktasına gelmiştir. Estonya devlet sistemlerine, bankacılık sektörüne, kolluk kuvvetlerine, medya şirketlerine ve internet altyapılarına yapılan bu saldırılarla adeta, ülkede işlem yapmak imkânsız hale gelmiştir. (Geers, 2008: s. 1).

Estonya örneği diğer devletler açısından da önemli olmuştur çünkü belki de ilk defa teknolojik olarak güçlü bir devlette 3 hafta gibi bir sürece, hemen hemen hayatın durduğu görülmüş ve hükümet ise bu krizden etkilenmiştir. Ülkeyi yönetilemez hale getiren bu siber saldırılarda

NATO da müttefik ülkeyi koruma sorumluluğu dolayısıyla her ne kadar saldırıları durdurmada yardımcı olmuşsa da itibarı sarsılan bir diğer yapı da yine NATO'nun kendisi olmuştur.

Gürcistan'a Siber Saldırılar

2008 yılında Gürcistan'a karşı gerçekleştirile siber saldırıların arkasında Rusya Federasyonu'nun olduğu iddia edilmektedir. Bu siber saldırıların arkasında ise tarihi sorunlar yatmaktadır. Güney Osetya ve Abhazya bölgeleri Sovyetler Birliği dağıldıktan sonra de facto bir şekilde özerk bölge gibi hareket etmekteydiler. Fakat 2008 yılında buradaki milliyetçi söylemler ve girişimler artınca Gürcistan ordusu ülkenin toprak bütünlüğünü savunmak amacıyla Güney Osetya'ya müdahalede bulunmuştur. Bunun üzerine Rusya Federasyonu da Osetya'ya girince iki ülke arasındaki gerginlik tırmanmıştır. Olayların perde arkasında ise Gürcistan'ın Batı'ya daha sıcak bakması ve ayrıca NATO üyesi olmak istemesi yatmaktadır. (Darıcılı, 2014: s. 7.)

Gürcistan'a karşı gerçekleştirilen siber saldırılar ise 2007 Estonya siber saldırısına benzerlik göstermektedir. 2008 yılında gerçekleşen bu saldırıların Gürcistan hükümeti bilgi altyapı sistemlerine yönelen ağır bir siber saldırı olduğu görülmüştür. Saldırıların ise sadece Rusya tarafından değil birkaç farklı bölgeden yapıldığı kaydedilmiştir. NATO ise Gürcistan'a yapılan bu saldırılarda ülkeye yardım edememiştir çünkü Gürcistan bu tarihte henüz NATO üyesi bir ülke değildir. Yine de saldırılar arttığında Gürcistan hükümetinin talepleriyle, birkaç kişiden oluşan uzman bir ekip gönderilmiştir. Saldırılardan uzun bir süre sonra bu uzman ekibin de yardımıyla ülkedeki bilgi sistemi normale döndürülebilmiştir. (Boyraz, 2015: s. 5).

Ancak saldırıların bitmesine kadar geçen süre Gürcistan adına bir somut savaştan daha fazla olumsuz anlamda etkiler doğurmuştur. Ülkenin dış dünyayla olan bağlantıları koparılmış, dışarıya bir e-posta bile göndermesi imkânsız hale gelmiştir. Gürcistan'daki banka sistemleri de tehlike altında kalmış, kredi kartları ve mobil telefonlar kullanılamamıştır. Her ne kadar Gürcistan tehlikeleri atlatmak adına Rusya ile olan iletişimini siber alanda bloke etmeye çalışsa da bu sefer siber saldırılar başka ülkeler üzerinden ülkeye yöneltilmiştir. Elbette Rusya ne Estonya ne de Gürcistan saldırılarını yaptığını kabul etmese de; saldırıların Rusya ile olan anlaşmazlık olaylarından hemen sonra gerçekleşmesi bu iddiaları güçlendirmektedir. (Kara, 2013: s. 49).

Wikileaks Belgeleri

Irak'ta da görev almış ve ABD ordusuna mensup kıdemli er Bradley Manning tarafından, ABD Dış İşleri Bakanlığı'nın 1996-2010 yılları arasındaki gizli yazışmaları, ordu veri tabanındaki gizli bilgiler 2010 yılında Wikileaks sitesi üzerinden dünyaya yayılmış, sızdırılmıştır. (Kara, 2013: s. 17).

Wikileaks sitesini 2006 yılında kuran Julian Assange bu site üzerinden Kenya'daki yargısız infazlar, Fildişi sahillerine bırakılan zehirli atıklar, Guantanamo kampındaki insanlık dışı uygulamalar hakkında pek çok gizli bilgiyi kamuoyuna sızdırmaya başlamıştır. 2010 yılında gelindiğinde ise ABD'nin Irak ve Afganistan gibi ülkelere yaptığı hukuk dışı uygulamaları da sızdırınca büyük paniğe neden olmuştur. (Adaklı, 2011: s. 1).
Wikileaks sitesi üzerinden yapılan açıklamaya göre bu girişimin amacı kamuoyunu bilgilendirmek, politik etik yaratmak ve hükümetlerin etik olmayan politikalarını ifşa etmektir.

Wikileaks belgelerinin sadece ABD'ye yönelik olarak düşünülmemesi gerekmektedir. Çünkü buradaki diplomatik kayıtlarda her ülkeyle yapılan gizli temaslar aşama aşama basına sızdırılmış, diplomatik anlamda kısa vadede olmasa da uzun vadede birçok şeyi değiştirebilecek bilgiler, belgeler ortaya çıkmıştır. Zaten belgelerin ortaya çıkmasından hemen sonra Wikileaks belgelerini bu site üzerinden yayımlayan Julian Assange birçok tehditle karşılamıştır. (Arsoy, 2011: s. 1).
ABD'nin küresel anlamda en güçlülerden biri olduğu aşikârdır fakat bu gücü siber alanda, hem de hiç beklemediği bir aktör -kendisi adına çalışan ABD'li yetkililer- tarafından böyle bir saldırıya maruz kalmasına engel olamamıştır.

Wikileaks belgelerinin bu makale açısından önemli olmasının altında yatan ana sebep; onun bir devletten bir devlete karşı değil; bireyden devlete karşı olarak gerçekleşmesidir. Bu anlamda makalenin başından beri vurgulanan güvenliğin dönüşümünü en iyi yansıtan örneklerden biridir. Küreselleşmeyle beraber artık tehditlerin çok yönlü olduğunun, bireyden şirkete, kurumsal yapılardan tekil yapılanmalara kadar bu alanda her aktörün etkin olabileceğinin en somut örneklerinden biridir. Bu da devletlerin artık bu alanda güvenlik sağlamayı bir öncelikli alan haline getirmeleri gerektiğini ortaya çıkarmaktadır.

SONUÇ

Küreselleşmeyle beraber dünyanın her bölgesinin birbiriyle bağlantılı hale geldiği açıktır. Bu anlamda hiçbir birimin ve sistemin uluslararası alandan izole bir şekilde varlığını sürdürmesi yahut bir etkileşim içerisinde olmaması pek gerçekçi değildir. Ekonomi, toplum, kültür, siyaset ve hatta bireyler bu küreselleşme sürecinin birer parçalarıdır ve bu değişim-dönüşüm sürecine de dâhildirler. Elbette uluslararası sistemde halen başat aktör olma vasfını koruyan ulus devletler de küreselleşme sürecinde değişim ve dönüşüm içerisinde olmuşlar, olumlu ve olumsuz etkilerden kendilerini azade tutamamışlardır.
Küreselleşme sonrasında değişen-dönüşen bir diğer kavram da güvenlik olmuştur. Realist paradigmanın klasik öğretilerinden olan güçlü askeri ordu ve ülkesel anlamda sınırların kontrolüyle tam anlamıyla bir ülkenin güvenliğini sağlamak gerçekçi durmamaktadır. Çünkü artık tehditler somut değil, soyut alanda belirmekte fakat sonuçları itibariyle somut dünyayı ağır bir şekilde etkileyebilmektedir. Estonya ve Gürcistan siber saldırılarında da görüldüğü üzere bir ülke bütün kurumlarıyla beraber saldırı altında kalabilir, ülkede hükümet etme imkânsız bir hale bürünebilmektedir. Bütün bunlar olurken de bu düşman saldırının aktörleri savaş meydanlarında değil; aksine dünyanın herhangi bir bölgesinde internete bağlantısı olan sıradan bir yerde bulunabilmektedir.

Ulus devletler, son yıllarda siber uzayda hâkimiyet kurmanın gerekliliğini ve önemini idrak edebilmişler, kendi savunma ve güvenlik algılamalarını da buna göre düzenlemeye başlamışlardır. Birçok ülke bu anlamda siber güvenlik yasaları oluşturmuş, bu alanda uzman kadrolar elde etmek adına yatırımlar yapmaya başlamıştır. Uluslararası alanda da siber güvenlik alanında bir takım işbirlikleri oluşturulmaya çalışılmaktadır. NATO, üyesi olan ülkelere bu anlamda da bir güvenlik şemsiyesi sunma çabasındadır. Yine Avrupa Birliği ve Birleşmiş Milletlerin de bu yönde çalışmaları bulunmaktadır.

Devletler siber alanda her ne kadar gecikmeli olsa da hâkimiyet sağlama anlamanda eli en güçlü yapılardır. Çünkü diğer hiçbir yapılanma bu konuda süreklilik, yatırım ve merkezileşmeyi görece devletlerden daha iyi gerçekleştirememektedir. Ayrıca siber güvenlik alanı her ne kadar bir risk alanı olarak görülse de burada elde edilebilecek bir üstünlük, uluslararası sistemde belirleyicilik anlamında da bir hareket kabiliyeti yaratabilecektir. Diğer taraftan siber

teknolojilere sahip ülkelerin, bu teknolojileri pazarlama imkânları da yüksek ve ekonomik olarak karlı görülmektedir. Son zamanlarda devletlerin siber alana ilgilerinin artmasının bir diğer önemli sebebi de bu ekonomik dürtüler olmuştur.

Sonuç olarak her ne kadar küreselleşmenin olumlu birçok sonucu olsa da bu süreçte değişim yönünde doğru, zamanında ve uygun adımlar atılmazsa çeşitli sorunlarla karşılanması yüksek ihtimaldir. Küreselleşmeyle değişen güvenlik algılaması paralelinde siber güvenlik de bunlardan biridir. Eğer devletler bu alanda hâkimiyetlerini sağlayabilirlerse uluslararası sitemde varlıklarını sürdürebilmeleri daha kolay olacaktır aksi takdirde güvenlik tehlikeleriyle yüz yüze gelmeleri ve beka sorunu yaşamaları kaçınılmazdır.

KAYNAKÇA

ADAKLI Gülseren. (2011). "Wikileaks Versus Kapitalizm", Bianet Online Haber Portalı, http://www.bianet.org/bianet/bianet/127079-wikileaks-versus-kapitalizm erişim tarihi: (07.12.2017).

ADAOĞLU Hacer Soykan. (2008). ''Küreselleşme ve Egemenlik Kavramının Değişmesine Yol Açan Etmenler.'' İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, Cilt 166, Sayı 1, sayfa 9.

AĞIR Bülent Sarper .(2011). ''Güvenlik Kavramını Yeniden Düşünmek: Küreselleşme, Kimlik ve Değişen Güvenlik Anlayışı.'' Güvenlik Stratejileri, Sayı 22, sayfa 109.

AKSOY Merve .(2016). , "Küreselleşme ile Değişen Güvenlik Algısı Bağlamında Bush Doktrini.", İHH İnsani ve Sosyal Araştırmalar Merkezi. Sayfa 3, http://insamer.com/wp-content/uploads/2016/04/K%C3%BCreselle%C5%9Fme-ile-De%C4%9Fi%C5%9Fen-G%C3%BCvenlik-Alg%C4%B1s%C4%B1-Ba%C4%9Flam%C4%B1nda-Bush-Doktrini.pdf (28.11.201).

ARSOY Helin .(2011). Ankarabarosu.org, http://www.ankarabarosu.org.tr/siteler/ankarabarosu/hgdmakale/2011-1/12.pdf erişim tarihi: (07.12.2017).

BOYRAZ H.M. .(Aralık, 2015), "NATO'nun Siber Güvenlik Politikası: Tarihsel Süreç ve Kırılma Noktaları" Cilt IV, Sayı 12, s.32-40, *Türkiye Politika ve Araştırma Merkezi (Research Turkey), Londra:* Research Turkey. http://researchturkey.org/?p=10236&lang=tr erişim tarihi: (03.12.2017).

Btk.gov.tr https://www.btk.gov.tr/File/?path=ROOT%2F1%2FDocuments%2FSayfalar%2FSiberGuvenlik%2FUlusalVeUluslararasiBoyutlariileSG.pdf erişim tarihi: (01.12.2017).

CEYLAN Haluk. .(2014). Halukceylan.wordpress.com. https://halukceylan.wordpress.com/2014/11/13/siber-alan-siber-uzay-nedir/ erişim tarihi:(30.11.2017).

DARICILI A.Burak .(2014). ‘’Rusya Federasyonu Kaynaklı Olduğu İddia Edilen Siber Saldırıların Analizi.’’ Uludağ Üniversitesi Sosyal Bilimler Enstitüsü Dergisi, Cilt 7, Sayı 2, Sayfa 7.

DEMİRAY Muhittin ve İşcan İsmail Hakkı. (2008). ‘’Uluslararası Sistemde Güvenlik Kavramının Değişimi Ekonomik ve Jeopolitik Arka Planı.’’ Dumlupınar Üniversitesi Sosyal Bilimler Dergisi, Sayı 21, sayfa 155.

DOMAN Chris .(2016). ‘’ The First Cyber Espionage Attacks: How Operation Moonlight Maze Made History.’’ https://medium.com/@chris_doman/the-first-sophistiated-cyber-attacks-how-operation-moonlight-maze-made-history-2adb12cc43f7 erişim tarihi: (03.12.2017).

ERDOĞAN İbrahim. (2013), ‘’Küreselleşme Olgusu Bağlamında Yeni Güvenlik Algısı.’’ Akademik Bakış, Cilt 6, Sayı 12, sayfa 266.

EREN Mehmet. (2017). ‘’Avrupa Birliği’nin Siber Güvenlik Stratejisi İçin Kuramsal Çerçeve ve Strateji Belgesi Öncesi AB’nin Eylemleri’’. Cyberpolitikjournal, Cilt 2, Sayı 3, sayfa 36. http://cyberpolitikjournal.org/wp-content/uploads/2017/07/Journal-Vol_2_No_3_17.pdf erişim tarihi: (02.12.2017).

FENTZ Stefan. .(2005). Univie.ac.at. http://www.univie.ac.at/frisch/isegov/aushaengUniWien/CyberpaceSecurity_Fenz.pdf erişim tarihi: (30.11.2017).

GEERS Kenneth .(2008). ‘’Cyberspace And The Changing Nature of Warfare.’’ SC Media, https://www.scmagazine.com/cyberspace-and-the-changing-nature-of-warfare/article/554872/ erişim tarihi: (03.12.2017).

Hürriyet Gazetesi .(2017). http://www.hurriyet.com.tr/bugunku-siber-saldirilar-20-yil-oncesiyle-baglantili-40417840 erişim tarihi: (03.12.2017).

IŞIK Ezgi. ‘’Dünden Bugüne Siber Savaşlar.’’ http://www.bookmark.com.tr/dunden-bugune-siber-savaslar/ erişim tarihi: (03.12.2017).

KARA Mahruze. (2013). Siber Saldırılar-Siber Savaşlar ve Etkileri. Yüksek Lisans Tezi. İstanbul Bilgi üniversitesi Sosyal Bilimler Enstitüsü, İstanbul.

KARAÇAY Timur. Başkent.edu.tr http://www.baskent.edu.tr/~tkaracay/etudio/agora/bt/siber.html erişim tarihi: (30.11.2017).

KURNAZ İbrahim. (2016). ‘’Siber Güvenlik ve İlintili Kavramsal Çerçeve’’. Siber Politikalar Dergisi, Cilt 1, Sayı 1, sayfa 65. http://cyberpolitikjournal.org/wp-content/uploads/2017/02/Journal_Dergi_pdf.pdf erişim tarihi: 01.12.2017.

OTTIS Rain. Lornes, Peeter. Erişim: 01.12.2017, https://www.researchgate.net/publication/287868009_Cyberspace_Definition_and_implications

SANCAK Kadir .(2013). ‘’Güvenlik Kavramı Etrafındaki Tartışmalar ve Uluslararası Güvenliğin Dönüşümü.’’ Karadeniz Teknik Üniversitesi Sosyal Bilimler Enstitüsü Dergisi, Sayı 6, sayfa 130.

SANDIKLI Atilla ve Emeklier Bilgehan .(2014). ‘’Güvenlik Yaklaşımlarında Değişim ve Dönüşüm’’, sayfa 5, http://www.bilgesam.org/Images/Dokumanlar/0-81-2014040746sandikli_emeklier.pdf (28.11.2017).

SEREN Merve .(2006). ‘’Siber Tehditlerle Mücadelede Farkındalık ve Hazırlık.’’ Siyaset, Ekonomi ve Toplum Araştırmaları Vakfı(SETA), Sayı 183, Sayfa 16-17.

Sesli Sözlük, https://www.seslisozluk.net/cyber-nedir-ne-demek/ (30.11.2017).

ŞAHİNASLAN Önder .(2003). Siber Saldırılara Karşı Kurumsal Ağlarda Oluşan Güvenlik Sorunu ve Çözümü Üzerine Bir Çalışma. Doktora, Trakya Üniversitesi Fen Bilimleri Enstitüsü, Edirne.

T.C Ulaştırma Denizcilik ve Haberleşme Bakanlığı. (2012). http://www.bilgiguvenligi.org.tr/wp-content/uploads/2016/03/Ulusal_Siber_Guvenlik_Stratejisi.pdf erişim tarihi: (02.12.2017).

TANDOĞAN Uğur .(2010). Dünya Gazetesi. https://www.dunya.com/kose-yazisi/savasa-hazir-miyiz/7527 erişim tarihi: (03.12.2017).

TÜRKÖZ Şükrü .(2016). ‘’Küresel Terörizm Sorununa Güvenlik Perspektifli Bir Yaklaşım.’’ Niğde Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi.’’ Cilt 9, sayı 2, sayfa 154.

W. BEIDLEMA ve Lieutenant Colonel Scott .(01.2009). Defining and Deterring Cyber War. http://indianstrategicknowledgeonline.com/web/DEFINING%20AND%20DETERRING%20cyber%20war.pdf erişim tarihi: (03.12.2017).

YENER Yavuz .(2014). ‘’NATO Ve Siber Güvenlik 2-Strateji.’’ Siber Bülten https://siberbulten.com/makale-analiz/nato-ve-siber-guvenlik-2-strateji/ erişim tarihi: (03.12.2017).

YILDIZ Mithat. (2014). Siber Suçlar ve Kurum Güvenliği. Uzmanlık Tezi. Ulaştırma Denizcilik ve Haberleşme Bakanlığı.