ISSN: 2587-1218

SİBER UZAYIN GÜVENLİKLEŞTİRİLMESİ: ABD ÖRNEĞİ

Upagül Rakhmanova[♣]

Özet

Bu çalışmada, ABD'nin siber uzayın güvenlikleştirilmesini nasıl hayata geçirdikleri araştırılacaktır. Bunun için öncelikle, Kopenhag Okulu tarafından geliştirilmiş güvenlikleştirme teorisi ve siber uzay kavramı irdelenecektir. Aynı zamanda, 1995'ten bu yana Amerikan hükümetinin siber alanı güvenlikleştirmek amacıyla kullandığı söz-edimlerinin etkili olup olmadığı da sorgulanacaktır. Ayrıca, siber uzayın güvenlikleştirilmesinde önemli rol oynayan kurumsal yapılanmaları analiz ederek, örgütlenmelerin yetki, sorumluluk, etkinlik ve faaliyetleri irdelenecektir. Son olarak, ABD'nin uluslararası düzeyde ülkenin siber uzay alanındaki amaç ve hedeflerini ortaya koyan 2003'ten bu yana yayınladıkları siber güvenlik strateji belgeleri üzerinde durulacaktır.

Anahtar kelimeler: Siber Uzay, Güvenlikleştirme, ABD, Kopenhag Okulu, Söz-edim

THE SECURITIZATION OF THE CYBER SPACE: THE CASE OF THE USA

Abstract

This paper explores how the American Government understands and characterizes cyberspace and its securitization. Adopting the framework of securitization theory, which was developed by Copenhagen School, paper seeks to understand and describe the role of speech-acts, that the American Government since 1995 engage in in order to securitize the cyber space. In this context, organizational structures, their responsibilities, activities that play an important role in securitization of the cyber space will be analized. Finally, it will focus on the cyber security strategy documents that the United States has published since 2003, which set out the goals and objectives of the cyber space.

Key words: Cyberspace, Securitizasion, USA, Copenhagen School, Speech-act

Giriş

♣ MA Student, Dept. of International relations, Selçuk University, upagul@gmail.com

Siber uzaya ve ayrıca siber güvenliğe olan ilgi her geçen gün artmaktadır. Ayrıca, her ülke kendi siber alanın korumaya ve güvenlikleştirmeye çabalamaktadır. Siber uzay kavramının herkes tarafından kabul edilen tanımı bulunmamasıyla beraber, siber uzay konusu günümüzde en çok güvenlik bağlamında ele alınmaktadır, zira hayatımızın hemen hemen her alanını etkilemektedir. Günümüzde artık, siber güvenlik sadece bireyler için değil, devletleri de ortadan kaldırabilecek kadar tehditleri oluşturabileceğinden, siber güvenlikle ilgili söylemler, "güvenlikleştirme teorisi" çerçevesinde incelenebilmektedir. Fakat, 1990'larda Kopenhag Okulu temsilcileri, siber güvenliği devletlerin varlığına bir tehdit olarak algılamıyordu, zira onlara göre siber güvenliğin o denemde diğer güvenlik sorunları üzerinde basamaklı (*cascading*) etkileri yoktu (Buzan, Waever, & De Wilde, 1998, s. 25). Ancak, 21.yüzyıla geldiğimizde, dünyada yaşayan insanların yarısından fazlasının internet kullanıcıları haline gelmesi, günümüzde bu durumu değiştirmiş bulunmaktadır.

"Güvenlikleştirme" kavramını akademik camiyaya Waever, 1995'te yazdığı *Securitization and Desecuritization* makalesi ile kazandırmıştır. "Güvenliği" bir *speach act* (söz-edim) olarak gören Waever'e göre, iktidar sahipleri bir konuya "güvenlik" olarak işaret etmekle, onu güvenlik sorunu haline getirmiş olurlar (Waever, 1995, s. 55). Güvenlikleştirme teorisi ise, daha sonra 1998'de Buzan, Waever ve Wilde tarafından kaleme alınarak, Uluslararası İlişkiler'de akademiyanın kullandığı terminolojisine kazandırılmıştır (McDonald, 2008, s. 566). Kopenhag Okulu, güvenlikleştirme teorisi ile, güvenlik çalışmaları'ndaki genişleyen tartışmanın orta noktasını yakalamada başarılı olmuştur (Hansen & Nessenbaum, 2009, s. 1158). Michael Williams, Kopenhag okulunun da defalarca dile getirdikleri gibi, güvenlik söyleminde, bir konu dramatize edilir ve yüksek öncelikli bir konu olarak sunulur demiştir (Williams, 2003, s. 514) Buna örnek olarak, Temmuz 2012'de ABD eski Başkanı Barack Obama, The Wall Street Journal'da yayınlanan bir fikir (*opinion*) yazısını verebiliriz. Bu yazıda, ülkeye karşı yapılan siber saldırıları, karşılaştıkları en ciddi ekonomik ve ulusal güvenlik sorunlarından biri olarak tanımlamıştır.

Bu çalışma ABD'nin siber uzayı nasıl güvenlikleştirdiğini ve ülke liderlerinin siber tehditlere karşı, dinleyicileri inandırmak amacıyla kullandıkları ifadelerin başarılı olup olmadığını irdelemeyi amaçlamaktadır. ABD'nin siber uzayı güvenlikleştirmesini inceleyen bu çalışmanın giriş bölümünün ardından gelen bölümde güvenlikleştirme teorisinden söz

edilecektir. Çalışmanın bir sonraki bölümünde ise Siber uzayın ne olduğu ve faklı tanımları ele alınacaktır. Makalenin son bölümünde ise ABD'nin siber uzayı güvenlikleştirmeyi nasıl yerine getirmeye çalıştığından bahsedilecektir.

Çalışmamız "güvenlikleştirme" ve "siber uzay" konularına odaklanmış olup, ABD'nin siber uzayı nasıl güvenlikleştirmeye çalıştıklarını ele almaktadır. Temel olarak siber uzay ve güvenlikleştirme teorisi üzerine yazılmış önemli eserleri ele aldığımız bu çalışmada, konunun toplumsal, siyasal ve bilimsel boyutlarıyla incelemeye ve konuya bir bütün olarak bakılmaya çalışılmıştır. Gerekli veriler ise, tarama tekniği ile toplanmıştır. Başvurulan referans kaynaklar, temel olarak siber güvenlik, siber tehdit, güvenlikleştirme, Kopenhag Okulu hakkında yazılan kitaplar ve makalelerden oluşmakla birlikte, özellikle güncel veriler ve ABD başkanlarının söylemleri için genel ağ ortamından yararlanılmıştır.

2. Güvenlikleştirme Teorisi

Güvenlikleştirme kavramı ilk olarak 1995 yılında Ole Waever tarafından *Securitization and Desecuritization* (Waever, 1995) makalesinde kullanılmıştır. Waever makalesinde "güvenliği" bir *speach act* (söz-edim) olarak görmüştür. Ayrıca söz-edimleri sadece iktidar sahipleri ürettiklerini öne sürmüştür. Ona göre, iktidar sahipleri belirli bir konuyu "güvenlik" problemi olarak isimlendirirken, devlet veya iktidarı elinde bulunduran elitler, bu "güvenlik" problemine karşı başvuracakları eylemleri otomatik olarak meşrulaştırmış olur. Bir konuya "güvenlik" olarak işaret etmekle, onu güvenlik sorunu haline getirmiş olurlar. Keza iktidar sahiplerinin "güvenlikleştirme" aracını, kontrolü elinde tutabilmek için kullanabileceklerini de yazmıştır. (Waever, 1995, s. 54). Kopenhag okulu temsilciler ise güvenlikleştirme kavramını daha ileri düzeye taşıyarak, daha doğrusu 1998'de yayımlanan *Security: a new framework for analysis* adlı kitabında onu bir teori haline getirmekle birlikte akademik yazıma kazandırmış bulunmaktalar. Güvenlikleştirme teorisi inşacı bir temele sahip olmaktadır, zira bu teoriye göre, güvenlik konuları güvenlik tehdidi olarak inşa edilmektedirler. Bu inşa edilmiş güvenlik konusu ise, söz-edimler ile tekrarlanarak, insanların diğer bir deyiş ile "hedef kitlenin" aklına enjekte edilir ki, bunun sayesinde tehdit olarak kabul ettikleri konulara karşı olağan üstü tedbirleri alabilmek meşru hale gelmiş olur. Bu, kimilerinin elinde bir araç haline gelebilmekteyken, kimileri için gerçekten bir tehdidin olduğuna insanları inandırmanın yararlı bir yolu olmaktadır. "Güvenlikleştire" – bu

öznelerarası ve sosyal olarak inşa edilir. Yani herhangi bir tehdit olarak gördüğü veya tehdit olarak sunmak istediği konuyu söz-edimler yoluyla güvenlik sorunu olarak hedef kitleye sunar. Bunun sonucunda kendi meşru olmayan eylemlerini hedef kitlenin kabul etmesini veya en azından alınacak tedbirlere tolere etmelerini sağlamış olurlar (Buzan, Waever, & Wilde, 1998, s. 31).

Waever'in 1995 makalesinde, "güvenlikleştirmek" sadece belli bir sorunu dile getirmekten ibaretti. Yani Waever 1995'te "güvenliği" dil teorisinin yardımıyla söz-edim olarak tanımlamıştır (Waever, 1995, s. 55). Daha doğrusu devlet temsilcisi, "güvenlik" kavramını dile getirerek belli bir gelişmeyi özel bir alana sokar ve bu gelişmeyi engellemek, bloke etmek için gerekli tüm araçları kullanma hakkını talep etmiş olur. (Waever, 1995, s. 55) Ancak, Kopenhag okulu ise, güvenlikleştirmenin sadece bir sorunu dile getirmekten ibaret olmadığını, söz-edimin güvenlikleştirme eyleminin sadece bir parçası olduğunu yazmışlardır. Onlara göre, "güvenlik", politikayı oyunun yerleşik kurallarının ötesine götüren ve meseleyi ya özel bir politika türü ya da siyaset olarak ele alan bir "hamledir". Güvenlikleştirme, bu yüzden siyasallaşmanın daha aşırı bir versiyonu olarak açıklanmıştır. (Buzan, Waever, & Wilde, 1998, s. 23).

1995 yılında vurgu *söz-edimde* ya da güvenlikleştiricide iken, 1998'de artık vurgu "güvenlikleştirici hamleye" taşınmıştır. Bu cümleyi açıklarsak, olağanüstü tedbirler ya da araçlar gerektiren bir tehdidin belirlenmesi ve bu durumun hedef kitle tarafından kabul edilmesi, güvenlik söyleminin dile getirilmesinden daha da önemlidir. (Williams, 2003, s. 526) Ayrıca, güvenlikleştirme eylemi üç temel öğeden oluşmaktadır. Bunlar - güvenlikleştirilmesi gereken konu, yani referans nesnesi; ikincisi, güvenlikleştiren aktör, başka deyiş ile hedef kitleye sürekli tekrarlayarak güvenlik konusunu enjekte eden kişi/grup; üçüncü öğe de işlevsel aktörlerdir, yani güvenlik alanındaki kararları önemli derecede etkileyen aktörler. (Balzacq, 2005, s. 178) Güvenlikleştirme eyleminin analizini yapmak mümkündür, bu ise korunması gereken konunun büyüklüğü ve seviyesi ile belirlenebilmektedir. Güvenlikleştirme teorisine göre, güvenlikleştirme analizinde üç ayrı düzey öngörülmüştür. Bunlar mikro, makro ve orta düzeylerdir. Kopenhag Okulu yazarları, söz-edimin örgütsel mantığına odaklanmanın kimin güvenlikleştirici aktör olduğunu belirlemede en iyi yol olduğuna inanmışlardır (Buzan, Waever, & Wilde, 1998, s. 40).

Kopenhag Okulu için, sorunlar dil aracılığıyla güvenlik sorunları (veya daha doğru bir şekilde tehditler) haline gelir. Dil, belirli aktörleri veya meseleleri belirli bir politik topluluğa tehdit eden konuma koyar ve dolayısıyla güvenlikleştirmeyi meşru yapar (McDonald, 2008, s. 568). Güvenlikleştirmenin ayırt edici özelliği, onun bir retorik yapıya sahip olasıdır. Yani, 'hayatta kalma' (*survival*) eyleminin önceliği, 'konuya anında, şimdi müdahale edilmezse, başarısızlığı düzeltmek için çok geç olacak' (Buzan, 1997, s. 14).

Yukarıda da bahsettiğiimiz gibi, güvenlikleştirme kendisi bir eylemdir, bir süreçtir (O'Reilly, 2008, s. 67). Bir konuyu alıp güvenlik tehdidi olarak gösterdikten sonra, geri kalan bütün diğer konular ikincil plana gitmiş olur. Güvenlikleştirilmesi gereken konu, öncelik kazanır ve tehdidin ortadan kalkmasına kadar diğer konuların önemi olmayacak gibi bir algı oluşur. Bu da, karar alan aktörlere her türlü tedbiri alarak, sorunu çözüme ulaştırma özgürlüğü verir. (Buzan, Waever, & Wilde, 1998, p. 24) Güvenlikleştirme eylemini gerçekleştiren aktör ise, bu durumun farkında ve olağanüstü tedbirler kullanmak istediği konuları güvenlik sorunu olarak etiketler. (O'Reilly, 2008, s. 66). Kopenhag okulu güvenlikleştirmeyi bir spektrum yardımıyla açıklamaktadır. Buna göre, her konu, "politize edilmemiş", "politize edilmiş" ve "güvenlikleştirilmiş" şeklinde sınıflandırılabilir. Mevcut şartlar altında her konu bu spektrumdaki yerini almaktadır. (Buzan, Waever, & Wilde, 1998, s. 24).

Bu teoriye göre, bir konuyu güvenlikleştirmek bu, söylemler üreterek hedef kitle üzerinde çalışmaktır. Bu manada güvenlikleştirme çalışmak, bir argümanın nasıl ve ne zaman hedef kitle üzerinde yeterli etkiyi yaparak onların normal şartlar altında kabul etmeyecekleri olağanüstü tedbirlerin alınmasını kabul etmelerini sağladığını araştırmak olmaktadır. Buna göre "güvenlikleştirme çalışmaları", kimin, hangi konuları, kimin için, neden, hangi sonuçlarla ve hangi şartlar altında güvenlikleştirdiğinin net olarak anlaşılmasını hedefler. Kısacası, güvenlikleştirme çalışırken araştırmacının görevi, bir konunun gerçek bir güvenlik sorunu olup olmadığının ortaya çıkarılması değil, güvenlikleştime eyleminin nasıl ve ne zaman gerçekleştiğinin, bunun öğelerinin (güvenlikleştirici, referans nesnesi, hedef kitle) neler ya da kimler olduğunun ve bunun sonuçlarının neler olduğunun ortaya konulmasıdır. (Buzan, Waever, & Wilde, 1998, s. 32) Fakat, başarılı bir güvenlikleştirme 3 aşamadan, veya daha doğrusu üç bileşenden oluşmaktadır. Bunlar, tehditin kendisi, acil tedbir ve olağan kuralların yıkılmasının ilişkilere tesir etmesidir. Bir de, bir konunun tehdit oluşturduğunu

ortaya koyan bir söz-edim kendi başına güvenlikleştirme oluşturmaz. Bu sadece bir hamledir, yani güvenlikleştirici hamledir.

Başarılı bir güvenlikleştirme, neyin dikkate alınması gerektiği ve kolektif olarak, yani bütün hedef kitlenin bir tehdit olarak karşılık verileceği konusunda ortak bir anlayışa varmalarıdır. (Buzan, Waever, & Wilde, 1998, s. 26).

Kopenhag Okulu, daha önceden geliştirmiş oldukları bölgesel güvenlik gibi diğer güvenlik yaklaşımlarını da güvenlikleştirme teorisinden sonra güncellemişlerdir. Güvenlikleştirme teorisini eleştirenler de vardır, onlara göre bu teori çok dar ve sınırlıdır. Zira güvenliği oluşturma eyleminin kendisi sınırlı tanımlanmıştır. Sadece baskın, iktidar sahibi aktörlerin konuşmalarına dayanmaktadır. Başka insanları devre dışı bırkamaktadır (McDonald, 2008, s. 564) ki, günümüzde sadece iktidar sahipleri değil, internet aracılığıyla sıradan bir insan da toplum içinde, hatta ülkeleri ve bölgelere kadar yankı yaratacak konuşmaları yaparak, etki yaratabilmektedir.

Sonuç olarak söylenmesi gereken nokta, bir konunun güvenlikleştirilip güvenlikleştirilmeyeceğini güvenlikleştirici aktör belirler. Onun verdiği bu karar her zaman politik karardır. (Buzan, Waever, & Wilde, 1998, s. 29) Bir konuyu güvenlikleştirmek, en kısa şekilde aşağıdaki gibi açıklanabilir. Ortada bir sorun var, onu güvenlik sorunu olarak etiketlemek, tekrar tekrar aynı konulardan bahsetmek, hedef kitleyi ikna etmek, onları inandırmak ve ortak düşünceyi inşa etmektir. Bunun sonucunda da yapılacak eylemleri otomatik olarak meşrulaştırmaktır.

3. Siber Uzay

Siber teriminin tarihsel ve felsefi kökleri genellikle Platon'un "Devlet" adlı yapıtındaki mağara alegorisine kadar uzanır. Ancak modern çağı ele alırsak, sibernetik teriminden türetilmiştir. Norbert Weiner tarafından 1948'deki ünlü *Cybernetics: Or Control and Communication in the Animal and the Machine* adlı yapıtında kullanmıştır (Choucri, 2012, s. 7). "Siber uzay" kavramını ise ilk kez bilim-kurgu yazarı William Gibson tarafından, 1984'te bir bilgisayar korsanının Matrix adı verilen bir bilgisayar sistemine sızarken yaşadıklarını anlatan *Neuromancer* adlı romanında kullanılmıştır (Singer W. & Friedman, 2014, s. 12). Enformasyon çağında herhang bir kelimenin önüne siber, bilgisayar veya

enformasyon gibi sözcükleri yerleştirmekle, yeni kavramları üretmek yaygınlaşmıştır (Cavelty, 2008, s. 21). Günümüzde siber uzay kavramının herkes tarafından kabul edilmiş tek bir tanımı yoktur. Ayrıca Gibson'un kullandığı maanadan farklı bir zemine kaymış bulunmaktadır. Bu yüzden çalışmamızda bir kaç tanımı verilecektir. Kimilerine göre siber uzay, ekranımızın ardındaki dünyayı işaret eden bir kavramdır. (Klimburg & Mirtl, 2012, p. 4) Ulusal sınırların geçerli olmadığı, devletler tarafından kontrol altına alınamamış ve askerler aracılığıyla koruma altına almanın imkansız olduğu alan ve bazen de İnternet'e karşılık olarak da kullanılan kavramdır. Bazıları siber uzayı harika ve "olmayan yer" (*no place*) olarak tanımlamaktalar. Bu ise dijital alemin fiziksel alanı aştığı anlamına gelir. Bilgi ve onu manipüle eden varlıklar elektronlar gibi - her yerde ve hiçbir yerdedir (L.Herrera, 2016, s. 67).

ABD Savunma Bakanlığı, siber uzayın vaftiz babası olarak kabul edilebilir zira bu, ARPANET gibi ağların ve eski bilgisayarların finansmanına dayanır. Yine de Pentagon bile bebeği büyüdükçe ayak uydurmak için çabaladı. Yıllar içinde siber uzayın ondan fazla farklı farklı tanımını yayınlamıştır. Bunların arasında "Soyut bilginin bilgisayar ağları üzerinden iletildiği kavramsal ortam" tanımı vardı, ama daha sonra bu tanım reddedildi, çünkü siber uzayın sadece iletişim ve büyük ölçüde hayali olduğu iddia edtmekteydi. Bir diğer tanım ise "elektronik ve elektromanyetik spektrumun kullanılmasıyla karakterize edilen bir alan" olarak tanımlanmıştır, fakat bu da bilgisayar ve füzelerin güneşten gelen ışığa kadar her şeyi kapsadığı için reddedilmiştir (Singer W. & Friedman, 2014, s. 13).

Günümüzde hayatımızı etkileyen faliyetlerin büyük kısmı siber uzayda/ortamda gerçekleşmektedir. Siber uzay, insan tarafından ve insanın hayatını kolaylaştırabilmek için yapılmış olsa da, kimileri bu alanı kötü niyet için kullanabilmektedir. Siber uzay, bireyleri daha önce mümkün olmayan şekillerde güçlendirmekte ve etkinleştirmektedir ve insan faliyetleri için oluşturulmuş yeni bir alandır. Siber uzaya ilişkin tanımların biri de 2003 tarihinde yayınlanan Amerika'nın Ulusal Siber Savunma Strateji belgesidir. Belgede siber uzay, ülkenin kritik altyapılarını etkileyen sinir sistemi olarak tanımlanmış olmakla birlikte, ülkenin ekonomisi ve ulusal güvenliği için sağlıklı çalışan bir siber uzaya dikkat çekilmiştir (The White House, 2003, p. 1).

Bir diğer tanıma göre, siber uzay herşeyden önce bir bilgi ortamıdır. Dijital ortamda oluşturulan, depolananan ve paylaşılan verilerden oluşmaktadır. Ama siber uzay tamamen sanal ortamdan ibaret değildir, zira veri depolayan bilgisayarları ve bilgi akışını sağlayan sistemleri ve altyapıyı içerir. Bu, ağa bağlı bilgisayarların internetini, kapalı intranetleri, hücresel teknolojileri, fiber optik kabloları da kapsar (Singer W. & Friedman, 2014, s. 14). Başka bir tanımda ise, siber uzay, devlet aktörleri tarafından sadece kısmen kontrol edilen veya kontrol edilebilen alandır. Bu alandaki güç, özel sektör aktörlerinin, özellikle de iş sektörünün elindedir. Daha iyi koruma önlemleri almak için gereken uzmanlık ve kaynakların çoğu hükümetlerin dışında yer almaktadır. Askeri ya da bu konuyla ilgili herhangi bir devlet kurumu, kritik (bilgi) altyapılara sahip değildir ve bunlara doğrudan erişimi yoktur. Onları askeri bir görev olarak korumak imkansızdır ve siber uzayı bir işgal bölgesi olarak görmek bir yanılsamadır. Militanlar ülkelerinin siber uzayını savunamazlar - ulusal sınırların mantığı uygulanmadığı için askerlerin ve tankların konumlandırılabileceği yer yoktur. (Cavelty, 2012, s. 151).

ABD'li siyaset bilimci Joseph Samuel Nye, "Nuclear Lessons for Cyber Security?" başlıklı makalesinde nükleer alan ve siber uzay arasında tüm benzerlikleri ve farklılıkları saymıştır. Nye, nükleer çağın başında bu güce sahip devletlerin kabul etmediği işbirliğini daha sonra kabul etmesine benzer bir sürecin siber uzayda da gerçekleşeceğini savunmaktadır. Siber uzayın sanal katmanında sınırların olmayışı ve bu durumdan kaynaklı egemenlik alanlarının belirsizliği, devlet dışı aktörlerin güç kazanmasına neden olmuştur (Nye, 2011, s. 37). Bu durumu güç yayılımı (diffusion of power) olarak kavramsallaştıran Nye, devletlerin kara, deniz ve hava boyutlarında olduğu gibi siber uzayda da bir güç olarak var olmalarına karşın, siber uzayın doğasının devletlerin tek aktör olarak bu alanda hâkim olmalarına izin vermeyeceğini belirtmiştir (Nye, 2011, s. 20). Bu bağlamda siber uzayda güç, büyük devletlerden diğer devletlere ve daha da önemlisi devlet dışı aktörlere yayılmaktadır (Nye, 2011). Bir bilgi ortamındaki güvenliğin kanonik hedefleri, bu tehdit kavramından kaynaklanmaktadır. Geleneksel olarak, üç hedef vardır: Gizlilik, Bütünlük, Erişebilirlik, bazen "CIA üçlüsü" olarak adlandırılmaktadır. Gizlilik, verileri gizli tutmak anlamına gelir. Gizlilik sadece bazı sosyal ya da politik amaç değildir. Dijital dünyada, bilginin değeri vardır. Bu bilgiyi korumak bu nedenle çok önemlidir (Singer W. & Friedman, 2014, s. 35).

Siber uzay konusu günümüzde en çok güvenlik bağlamında ele alınmaktadır, zira hayatımızın hemen hemen her alanını etkilemektedir. Hayatımızı her yönden kapsayan bu alanının güvensizliği ise herkesi, ister devletler olsun, ister Uluslararası Ögrüt veya şirket olsun, tedirgin etmektedir. Siber uzayı tanımlamanın zor olması, onun her an büyümekte olması veya küresel bir nitelik taşımasıyla sınırlı değildir. Bunun nedeni, günümüzdeki siber uzayın, ilk başta mütevazi bir şekilde ortaya çıkmasından çok farklı olarak tanınmaz hale gelmesindendir.

4. ABD'nin Siber Uzayı Güvenlikleştirmesi

Siber uzay alanında devlet tarafından güvenlikleştirme çabaları 1995 Clinton yönetimi sırasında başlamıştır. İlk etapta ABD siber uzayı ekonomik ve kültürel üstünlüğünü kabul ettirebileceği bir alan olarak değerlendirmiştir (Darıcılı, 2017, s. 350). Ciddi güvenlik mekanizmaları ise 11 Eylül 2001'den sonra başlamıştır. 2001'in sonlarında, FBI Başkanının ofisinde bir bilgisayar yoktu, hatta ABD Savunma Bakanı ona gelen maillerin çıktısını almak için asistanın yardımından yararlandığı, gelen maile cevabı da kalemle kağıda yazıp asistana verdikten sonra, asistanı ardından onları bilgisayarda tekrardan yazdığı bilinmektedir. Bundan on yıl sonra ülkeyi siber tehditten korumakla görevli olan İç Güvenlik Bakanı Sekreteri'nin 2012'de düzenlediği bir konferansta, "Gülmeyin, ama ben e-posta hiç kullanmıyorum" demesi, onun için güvenlik korkusu değildi. Onun için bu, sadece e-postaların faydalı olduğuna inanmamasıydı. 2013 yılında, Yargıç Elena Kagan, ABD Yüksek Mahkemesi yargıçlarının dokuzunun sekizini de aynı şekilde e-posta kullanmadıklarını açıklamıştı. Ama nihateninde bu insanlar, siber alanda neyin yasal olduğuna karar verecek olan insanlardır. (Singer W. & Friedman, 2014, s. 5).

Ocak 2009'da göreve başlanan Başkan Barak Obama, ABD siber güvenlik politikasının gözden geçirilmesini emretmişti. Obama'nın başkanlık döneminde konuşmalarında ABD'nin siber saldırılardan dolayı ciddi önlemler almaları gerektiğini sıkça dile getirerek yeni politikalar üretmiştir. Mayıs 2009'da Başkan Obama, politika incelemesini kabul etti ve ABD hükümet departmanlarının ve kurumlarının Beyaz Saray Siber Güvenlik Koordinatörü (WHCC- *The White House Cyber security Coordinator*) aracılığıyla siber güvenlik çabalarını koordine etmeye başladığını söylemiştir. WHCC, tüm ABD hükümet departmanlarının ve

ajanslarının, siber güvenlik stratejileri ve ABD siber güvenlik stratejisi ile uyumlu protokolleri uygulamaya koymalarını sağlamakla görevli olmuştur (Kiggins, 2014, s. 164).

Thierry Balzacq, bir konuşma eyleminin istenen etkiyi elde etmesi için, güvenlikleştirici aktörün "kendi dilini izleyicinin deneyimine göre ayarlaması" gerektiğini belirtmiştir (Balzacq, 2010, s. 9). 2009'da Obama'nın göreve başlamasından hemen sonra siber uzay alanında güvenlikleştirme işlemlerinin çok büyük tempolarla ilerlediğini görmek, hedef kitleyi inandırmış veya en azından susturmuş, kabullendirmiş anlamına gelmektedir. ABD Ordusuna bağlı Siber Komutanlığın (*Cyber Command*) generali, 2010'da Kongre'ye verdiği konuşmasında, Amerika silahlı kuvvetleri milyonlarca siber saldırıyla karşı karşıya olduğunu söylemiştir (Singer W. & Friedman, 2014, s. 68). Siber güvenlik konusunun Kongre'ye taşınması, artık önemli adımların alınacağı anlamına gelmekteydi. Obama'nın talimatıyla 2009 yılında hazırlanmış önemli bir belge Siber Uzay Politika Revizyonu *(Cyber Space policy review)* belgesidir. Bu belgede temel olarak, ABD siber savunma sisteminde görev alan resmi kurum ve kuruluşların, federal ve yerel düzeyde çok başlı yapısına eleştiride bulunularak, bu durumun giderilmesi için bazı tedbirlerin alınması gerektiği ve ulusal siber güvenlik sistematiğinin ancak bu kuruluşların birlikte ve eşgüdüm halinde hareket etmesi ile etkili olabileceği belirtilmektedir (The White House, 2009). Bundan sonraki önemli adım, yine Obama'nın talimatıyla hazırlanan Ağlanmış Bir Dünya'da Refah, Güvenlik ve Açıklık (*International Strategy for Cyberspace. Prosperity, Security, and Openness in a Networked World Siber Uzay İçin Uluslararası Strateji)* isimli dökümanın olmuştur (The White House, 2011).

Michael Williams, Kopenhag okulunun da defalarca dile getirdikleri gibi, güvenlik söyleminde, bir konu dramatize edilir ve yüksek öncelikli bir konu olarak sunulur demiştir (Williams, 2003, s. 514) Buna örnek olarak, Temmuz 2012'de ABD eski Başkanı Barack Obama, The Wall Street Journal'da yayınlanan bir fikir (*opinion*) yazısını verebiliriz. Bu yazıda, ülkeye karşı yapılan siber saldırıları, karşılaştıkları en ciddi ekonomik ve ulusal güvenlik sorunlarından biri olarak tanımlamıştır. Modern Amerikan halkının çoğunun yaşamının bağımlı olduğu ağlara siber tehditlerin olduğunu, hemen harekete geçme ve düşmanlarından bir adım önünde olma fırsatı ve sorumluluğu olduğunu vurgulayan Obama, ulusal ve ekonomik güvenliklerinin uğruna, Senato'nun 2012'deki Siber Güvenlik Yasasını

geçirmesini rica ederek, büyüyen tehlikeye karşı savunmalarını güçlendirmelerinin zamanı geldiğini söylemiştir (Obama, 2012).

Günümüzde ise en son 23 Nisan 2015 tarihinde kabul edilmiş Siber Strateji belgesi (*"The Department of Defence Cyber Strategy*) yürürlüktedir. Bu belge siber ataklara karşı ABD çıkarlarını koruma, askeri ve gizli siber operasyonları planlama gibi operasyonlara rehberlik etme, görevleri verilmiştir. ABD'nin stratejik belgelerinde Çin, Rusya, Kuzey Kore ve İran saldırgan düşman olarak *(Key Cyber Threats)* tanımlamaları, bu ülkelere karşı alınacak olağan üstü karar ve eylemleri, sadece kendi ülkesi için değil bütün dünyaya aklamış veya en azından alışmalarını sağlamış olur.

Space News adlı haber sitesinin aktardığına göre, ABD'li General David Goldfein, 23 Şubat 2018, Orlando Hava Kuvvetleri Birliği Hava Harp Sempozyumu'ndaki konuşmasında ABD'nin 'uzay savaşlarında' üstünlüğü eline alması gerektiğini vurgulayarak, "Birkaç sene içinde uzaydan savaşabiliriz" ifadelerini kullanmıştır (Erwin, 2018). "Uzayda savaş" söylemini kullanarak, hedef kitlede bir nevi korku tohumlarını attıktan sonra konuşmasının devamında da, ABD Hava Kuvvetleri'nin bu çekişmeli alanda öncülük yapmaları gerektiğini, Amerikan ulusunun bunu talep ettiğini öne sürmüştür. Goldfein ABD ordusunun askeri ateş gücünü güçlendirmesi için Hava Kuvvetleri'nin hava, kara, deniz, uzay ve siber alem dahil tüm alanalardan gelen savaş alanı istihbaratını kullanması gerektiğini vurgulamıştır (Erwin, 2018). Diğer bir deyişle, önce dinleyicilere ülkenin tehlike içinde oldukları fikri enjekte ettikten sonra alınması gereken eylemleri öne sürmüştür. Aynı toplantıda konuşan ABD Başkan Yardımcısı Mike Pence de ABD'nin 'Dünya'da olduğu gibi uzayda da egemen güç olması gerektiğini' savunmuştur. (www.tr.sputniknews.com, 2018).

Şubat 2003'te kabul ettiği ilk Siber Uzay'ın Korunmasına Yönelik Ulusal Strateji belgesi ile birlikte, başta Rusya ve Çin olmak üzere diğer devletlerin ve devlet dışı aktörlerin artan siber imkan ve kabiliyetlerini kendisine yönelik olarak askeri ve espiyonaj merkezli yeni tehdit odakları olarak kabul etmiştir. Belgenin asıl amacı, *ABD kritik altyapısını siber ataklara karşı korumak, ABD siber savunma sistemindeki açıkları tespit etmek ve gidermek, olası saldırılar karşısında uğranılabilecek zararı minimize etmek* şeklinde ifade edilmiştir (The White House, 2003). Belge yayınlandıktan sonra, kurumsal yapılanmalarını yeni şartlar dahilinde organize etmeye başlamıştır. Bu belge, ABD'nin siber uzay alanını tanımlayan, bu

alandaki hedef ve planlamalarını ortaya koyan, ulusal siber uzayın nasıl korunacağına dair planlanan sistemi belirleyen, siber uzay kaynaklı tehditleri tarif eden ilk geniş kapsamlı dokümandır.

Stratejik ve Uluslararası Çalışmalar Merkezi'nin (CSIS) başkan yardımcı olan James Andrew Lewis'in yazdığı rapora göre, askeri ve istihbarat açısından, gelişmiş asker kuvvetlerine sahip ve biri birine düşman olan ülkeler, gerçek anlamda siber saldırılar ile biri birine zarar verebilme riskine sahiptir. Birçok ülke askeri siber gücü edinmekteler, fakat Amerika'nın en tehlikeli rakipleri, siber alanında gelişmiş yeteneklerini ABD'ye göre "düşmanca" niyetle birleştiren Çin ve Rusya'dır. ABD'nin siber alandaki açıklarını kullanarak, ülkenin ekonomik, teknolojik ve askeri 'hegemonyasını' azaltmak için kullanmaktalar, ayrıca siber saldırıları askeri amaçta kullanabilecek kapasiteye sahip en iyi hazırlanmış muhaliflerdendir. Onların başarılarının örnekleri listelenemeyecek kadar çoktur. Yine bu raporda belirttiklerine göre, ABD'ye karşı yapılan saldırıların büyük çoğunluğu Rusya ve Çin'den gelmektedir. Amerika savaş içinde olmasa da, siber uzay tartışılır bir alandır. Lewis'e göre Rusya ve Çin ile siber çatışmanın risklerini yönetmek, Amerika'nın ulusal güvenliği için çok önemlidir, bu konudaki ilerlemeler, gelecekte istikrarsız devletler ve devlet dışı aktörlerle başa çıkmayı kolaylaştıracak daha istikrarlı bir ortam yaratılmasına yardımcı olacaktır. Ayrıca Rusya ve Çin için, şu anda sahip oldukları orantısız avantajları ve nispi cezasızlığı azaltarak istikrar elde edilebilir (Lewis, 2013, s. 4).

Kısacası, siber güvenlik kadar hiç bir sorun önemi bakımında bu kadar kısa zamanda ortaya çıkmamıştı (Singer W. & Friedman, 2014, s. 4), ayrıca siber uzay toplumun her kısmını etki ettiği için, iktidar sahipleri kolayca hedef kitleye kendi düşüncelerini enjekte ederek, olağan zamanda yapamayacakları veya yapmaları çok zor olacak eylemlerini hedef kitleye kabul ettirmiştir. Günümüzde ABD'nin resmi siber organizasyonu ABD Savunma Bakanlığı (*United States Department of Defense*), ABD İç Güvenlik Bakanlığı (*United States Department of Homeland Security* / DHS) ve ABD Gizli Servisleri (FBI / CIA) Şeklinde üçlü bir yapıdan oluşmaktadır. ABD'nin resmi siber organizasyonu oldukça karmaşık ve geniş bir yapıya sahiptir. ABD'nin ulusal siber savunma sisteminin sağlanması amacıyla birbirleriyle koordineli bir şekilde faaliyet yürütmek zorundadırlar. Karmaşık yapısı, ABD'nin federatif yönetim anlayışından kaynaklanmaktadır (Darıcılı, 2017, s. 339).

Siber tehditler konusunun son yıllarda bu kadar dikkat çekmesinin en önemli nedenlerinden biri, siber tehdit kavramlarının tehdit siyaseti sürecinde, ABD'li yetkililer ikna edici bir şekilde modern toplumların hayatının her alanını ettiklerini iddia etmeleridir. Tartışma giderek artan şekilde, her şeyin, örneğin, evlerin ve işyerlerinin enerjisinin ve sağlık bakım sistemlerinin etkinliğinin sağlanması dahil olmak üzere, bilgi sistemlerinin ve ağların güvenilirliğine bağlıdır. Bu kritik bilgi altyapıları, sürekli olarak veri alışverişi, devlet operasyonları, acil servisler ve ticaret için çok önemli olduğu için, kritik altyapıların omurgası olarak kabul edilir. Bilgiye/enformasyona olan bu bağımlılık - teknik güvenlik boşluklarından, teknolojinin karmaşıklığından, devam eden piyasa liberalizasyonundan ve kötü niyetli aktörlerin fiziksel ve siber saldırılarda bulunma konusundaki artan istek ve istekliliğinden kaynaklanan artan güvenlik açıkları ile birleştiğinde – en azından teoride de olsa, telekomünikasyon ve bilgi sistemlerini son derece savunmasız hedefler haline getirmektedir (Cavelty, 2007).

Devletler ve medya, tekrar tekrar siber tehditler hakkında bilgi dağıtırken, ölüm ve yaralanmalarla sonuçlanan gerçek siber saldırılar ve büyük ölçüde siber alandaki kötü niyetli aktörler tarafından tetiklenen büyük yıkıcı olayların tehditkar senaryoları sadece Hollywood filmlerinde veya komplo teorilerinin bir parçası olarak kalmıştır (Cavelty, 2008, s. 20).

5.Sonuç

"Siber uzay" kavramı, ilk başta kullanıldığı anlamdan çok farklı ve artık tanınmaz hale gelmişken, "güvenlikleştirme" kavramı da 1995'te ilk kullanılış biçiminden farklı zemine kayarak, uluslararası akademik ortama girmiştir. Siber uzay konusu günümüzde en çok güvenlik bağlamında ele alınmaktadır, zira hayatımızın hemen hemen her alanını etkilemektedir. Hayatımızı her yönden kapsayan bu alanının güvensizliği tedirgin etmektedir ki, bazı aktörler bunu güvenlikleştirmeye çalışmaktadır.

Devlet temsilcilerinin, bazen drurumu dramatize ederek, "güvenlik" kavramını dile getirip belli bir gelişmeyi, (bizim durumda siber güvenlik konusunu) özel bir alana sokarak, bu gelişmeyi engellemek, bloke etmek için gerekli tüm araçları kullanma hakkını hedef kitleden talep etmiş oldular, ve sonucunda da stratejik belgelerinde yazılan amaçlar doğrultusunda çalışmalarını yürütmek için olağan durumda almayacakları karar ve yapmayacakları eylemleri, bu "özel durumda" yapabilecekleri için, kendilerini önceden aklamış oldular.

ABD'de Clinton döneminde başlayan siber uzayın güvenlikleştirilmesine yönelik çalışmalar, Obama döneminde en yoğun şekilde geliştirilmiştir.

Güvenlikleştirme teorisine göre, bir konunun güvenlikleştirilip güvenlikleştirilmeyeceğini güvenlikleştirici iktidar sahibi aktör belirler. Onun verdiği bu karar ise her zaman politik karardır. (Buzan, Waever, & Wilde, 1998, s. 29) 2009 ile 2018 arasında Siber Güvenlik konusunda yapılan konuşmalar, kabul edilen stratejik belgeler, yeni kurumların oluşturulması, ister 2015 Ocak, Ulusal Siber Güvenlik İletişimi ve Entegrasyon Merkezinde Obama'nın yaptığı konuşma (Obama, 2015) olsun hepsi, 2012'deki ABD'ye karşı yapılan siber saldırıları, karşılaştıkları en ciddi ekonomik ve ulusal güvenlik sorunlarından biri olarak tanımlaması gibi siber uzayı güvenlikleştirmek amacıyla yapılmıştır.

Hedef kitleyi inandırmak amacıyla kullandıkları ifadelerin ve eylemlerin başarılı olup olmadığını irdelerken, kısmen da olsa başarılı olduklarını görmekteyiz. Çünkü yeni kurumların oluşturulması, siber uzayı güvenlikleştirmek amacıyla yapılan her hamle, bütçeden yüklü miktarda para gerektirir, ve sorunları zamanında Kongre'ye taşıyarak, Kongre'nin onayını almıştır. Bugün sorunlarla başedemezlerse, başka böyle şansının olmayacağını, veya geç kalacaklarını öne sürmüştür. Diğer örnek, ABD'li General David Goldfein, 2018 Şubat konuşmasında, bir kaç yıl sonra uzayda savaşabilecekleri fikrini ortaya atarak, dinleyici hedef kitle içine bir korku temelini attıktan sonra, ABD Hava Kuvvetleri'nin bu çekişmeli alanda öncülük yapmaları gerektiğini, ve bunu da Amerikan ulusunun talep ettiğini öne sürmüştür ki, olağanüstü tedbirler ya da araçlar gerektiren bir tehdidi belirlemiş oldu. Başka deyiş ile, uzayda savaş kavramını kullanmakla, "tehdidi" etiketlemiş oldu. Bunun devamında da ilgili kurumlardan, ve hedef kitleden "uzayda galibiyet" uğruna, gereken tedbirleri talep etme hakkını almış bulunmaktadır.

Kaynakça

Balzacq, T. (2005). The three faces of securitization: Political agency, audience and context . *European journal of international relations, 11*(2), 171-201.

Balzacq, T. (2010). A theory of securitization: origins, core assumptions, and variants. T. Balzacq içinde, *Securitization Theory: How Security Problems Emerge and Dissolve.* Routledge.

Buzan, B. (1997). Rethinking security after the Cold War. *Cooperation and conflict, 32*(1), 5-28.

Buzan, B., Waever, O., & De Wilde, J. (1998). *Security: a new framework for analysis.* Lynne Rienner Publishers.

Buzan, B., Waever, O., & Wilde, J. D. (1998). *Security: a new framework for analysis.* Lynne Rienner Publishers.

C.Williams, M. (2003). Words, images, enemies: Securitization and international politics. *International studies quarterly, 47*(4), 511-531.

Cavelty, M. D. (2007). *Cyber-security and threat politics: US efforts to secure the information age.* Routledge.

Cavelty, M. D. (2008). Cyber-terror—looming threat or phantom menace? The framing of the US cyber-threat debate. *Journal of Information Technology & Politics, 4*(1), 19-36.

Cavelty, M. D. (2012). The Militarisation of Cyberspace: Why less may be better. *Cyber Conflict (CYCON)* (s. 141-153). 2012 4th International Conference on. IEEE.

Choucri, N. (2012). *Cyberpolitics in international relations.* . MIT press.

Darıcılı, A. B. (2017). ULUSLARARASI IX ULUDAĞ ULUSLARARASI İLİŞKİLER KONGRESİ - Dünya Politikasında Kriz ve Değişim. *AMERİKA BİRLEŞİK DEVLETLERİ'NİN SİBER KAPASİTESİNDE ROL OYNAYAN KURUMSAL YAPILANMALARIN ANALİZİ*, (s. 337-352). Bursa.

Erwin, S. (2018, Şubat 24). www.spacenews.com: http://spacenews.com/air-force-chief-goldfein-well-be-fighting-from-space-in-a-matter-of-years/ adresinden alınmıştır

Hansen, L., & Nessenbaum, H. (2009). Digital disaster, cyber security, and the Copenhagen School. *International studies quarterly, 53*(4), 1155-1175.

Hjalmarsson, O. (2013). The Securitization of Cyberspace.

Kiggins, R. D. (2014). US Leadership in Cyberspace: Transnational Cyber Security and Global Governance. J.-F. Kremer, & B. Müller içinde, *Cyberspace and International Relations.* (s. 161-180). Berlin: Springer.

Klimburg , A., & Mirtl, P. (2012). Cyberspace and governance-a primer.

L.Herrera, G. (2016). Cyberspace and sovereignty: thoughts on physical space and digital space. V. Mauer, M. Cavelty, & S. Krishna-Hensel içinde, *Power and Security in the Information Age* (s. 81-108). Routledge.

Lewis, J. A. (2013). *Conflict and Negotiation in Cyberspace, A Report Of The Technology And Public Policy Program.* Washington, DC: Center for Strategic and International Studies.

McDonald, M. (2008, December). Securitization and the Construction of Security. *European Journal of International Relations, 14*(4), 563–587.

Nye, J. S. (2011). Nuclear lessons for cyber security? *Strategic Studies Quarterly, 5*(4), 18-38.

O'Reilly, C. (2008, September). Primetime Patriotism: News Media and the Securitization of. *Journal of Politics and Law, 1*(3), 66-72.

Obama, B. (2012, 07 19). *Wall Street Journal*. www.wsj.com: https://www.wsj.com/articles/SB10000872396390444330904577535492693044650 adresinden alınmıştır

Obama, B. (2012, 07 19). *Wall Street Journal, Opinion*. www.wsj.com: https://www.wsj.com/articles/SB10000872396390444330904577535492693044650 adresinden alınmıştır

Obama, B. (2015, 01 13). www.obamawhitehouse.archives.gov: https://obamawhitehouse.archives.gov/the-press-office/2015/01/13/remarks-president-national-cybersecurity-communications-integration-cent adresinden alınmıştır

Singer W., P., & Friedman, A. (2014). *Cybersecurity and cyberwar: What everyone needs to know.* Oxford University Press.

The White House. (2003). The National Strategy to Secure Cyberspace. Washington.

The White House. (2009, September 3). Cyberspace policy review: Assuring a trusted and resilient information and communications infrastructure. Washington, DC.

The White House. (2011, May). International Strategy for Cyberspace. Prosperity, Security, and Openness in a Networked World .

Waever, O. (1995). Securitization and Desecuritization. R. D. Lipschutz içinde, *On security.* Columbia University Press.

Williams, M. C. (2003). Words, images, enemies: Securitization and international politics. *International studies quarterly, 47*(4), 511-531.

www.tr.sputniknews.com. (2018, Şubat 28). Haziran 1, 2018 tarihinde www.tr.sputniknews.com: https://tr.sputniknews.com/abd/201802281032443091-abdli-general-birkac-yil-icinde-uzaydan-savasabiliriz/ adresinden alındı