DÖNÜŞTÜRÜCÜ ÖĞRENME KURAMIYLA SİBER UZAYDA RUSYA VE NATO REKABETİ: SOĞUK SAVAŞ'TAN SİBER SAVAŞ'A GEÇİŞ Mİ?

Ahmet Emre KÖKER[1]

Özet: Çalışmada, dönüştürücü öğrenmenin ne olduğundan yola çıkılarak, siber uzay sürecinde Rusya'nın NATO'ya ve üye ülkelerine karşı tutumu eleştirel bir bakış açısıyla analiz edilmiştir. Gerçekleştirilen analizlerin sonucunda ortaya çıkan perspektif, bizi, yapıda dönüşüm olduğu, NATO'nun kurumsal kimliğini ve üyelerinin değerlerini korumaya çalıştığı, Rusya'nın siber uzayda çıkarlarını maksimize etmeye çalıştığı ve karşıt iki grup arasında artan oranda siber çatışmalar yaşandığı sonucuna götürmüştür. Makale, 21. yüzyıl siber ortamında Rusya-NATO rekabetini siber güvenlik stratejileri çerçevesinde inceleme esasına dayanmakta olup, gelecekte gerçekleştirilecek çalışmalar için bir dayanak noktası sağlamayı amaçlamaktadır. Bu hedef doğrultusunda, çalışma, Rusya-NATO arasındaki yaşanan siber rekabeti "Siber Savaş Dönemi" şeklinde açıklayarak, askeri, siyasi, ekonomik, teknolojik ve kültürel bir ayrım yapmadan bütünsellik içinde iki karşıt gücün gayretlerine odaklanmaktadır. Bu gayretler çerçevesinde, söz konusu makale, siber uzayda güvenliği ve savunmayı sağlamaya yönelik politika üreten tüm kurum ve kişilerin birincil ve ikincil kaynaklarına odaklanmıştır.

Anahtar Kelimeler: *Rusya, NATO, Siber güvenlik, Dönüştürücü öğrenme.*

Article Category: International Relations

Date of Submission: 15.01.2023

Date of Acceptance: 28.01.2023

[1] Dr, Siyaset Bilimi ve Uluslararası İlişkiler, PTT A.Ş. Genel Müdürlüğü, Ankara, Turkey.
Email: a.emrekoker@hotmail.com / ahmetemrekoker@gmail.com.
ORCID: 0000-0002-8032-4237.

RUSSIA AND NATO COMPETITION WITH TRANSFORMATIVE LEARNING THEORY: TRANSITION FROM COLD WAR TO CYBERWAR?

Abstract: In the study, starting from what transformative learning is, Russia's attitude towards NATO and its member countries in the cyberspace process has been analyzed from a critical point of view. The perspective that emerged as a result of the analyzes carried out led us to the conclusion that there has been a transformation in the structure, that NATO is trying to protect its corporate identity and the values of its members, that Russia is trying to maximize its interests in cyberspace, and that there are increasing cyber conflicts between the two opposing groups. The article is based on examining Russia-NATO competition in the 21st century cyber environment within the framework of cyber security strategies and aims to provide a basis for future studies. In line with this goal, the study explains the cyber rivalry between Russia and NATO as the "Cyber War Period" and focuses on the efforts of two opposing powers in a holistic manner without making any military, political, economic, technological, and cultural distinctions. Within the framework of these efforts, this article focuses on the primary and secondary resources of all institutions and individuals who produce policies to ensure security and defense in cyberspace.

Keywords: *Russia, NATO, Cyber security, Transformative learning.*

Giriş

Siber uzayda Rusya ve NATO (Kuzey Atlantik Antlaşması Örgütü) arasında yaşanan gerilim, Birinci Dünya Savaşı ve İkinci Dünya Savaşı'ndan farklı olarak, nispeten Soğuk Savaş dinamiklerine benzemektedir. Günümüzde yaşanan siber savaş dönemi, özü itibarıyla psikolojik bir yapıyı temsil etmekte, karşılıklı gerilim yaşatmakta ve her an saldırıya maruz kalma korkusunu içermektedir. Bu sebeple, içinde bulunulan dönem, konvansiyonel ve nükleer savaş araçlarından ziyade siber silahların kullanıldığı bir savaş türünü simgelemektedir.

Her savaş türü, bir sonraki savaş türünün nedeni ve sonucudur. Bu anlamda, aslında Soğuk Savaş da siber savaşın doğmasının bir nedenidir. SSCB'nin ekonomik ve teknolojik yapıdaki değişime ayak uyduramaması, bu savaşın bitmesine yol açmıştır. Bu sebep ise, aynı zamanda siber savaşın başlangıcı olan internetin doğuşu, gelişimi ve yükselişini ortaya çıkarmıştır. Bu bağlamda, nasıl Birinci ve İkinci Dünya Savaşı tamamen birbirinden farklı bir savaş modeli ise, Soğuk Savaş ve siber savaş da birbirinden farklı iki savaş modelidir. Ama birbirlerini tetiklemiştir. Yani Soğuk Savaş'ın bitmesiyle birlikte, savaşın önlenmesine yönelik çabalar siber savaşın tetiklenmesine yol açmıştır.[2]

Her iki savaş da, küresel anlamda tüm dünyayı içeren bir savaştır. Şu an yumuşak bir şekilde yükselme dönemini yaşayan siber çatışmalar, uluslararası ilişkilerde dış politika stratejilerinin belirlenmesi süreçlerinde aktif olarak kullanılmaktadır. Siber uzay hakkında uluslararası hukuk kurallarında misilleme yasağının bulunmaması, karşılıklılık ilkesinin olmaması, bilinmezliği içinde barındırması, kanunlara aykırı olmaması gibi sebeplerden dolayı, ülkeler arası çatışmalarda, siber silahlar sıklıkla kullanılmaktadır. Bu bağlamda, siber uzayda gerçekleşen tüm çatışmalar savaş hukukunda veri iletişimi ve veri koruması süreçlerine yönelik gerçekleşen siber savaş dönemi olarak gösterilmektedir.[3]

Aynı zamanda, Soğuk Savaş döneminde Sovyetler tarafından saldırıya uğrama korkusuna sahip ülkeler, günümüz siber dünyasında da bu hissi farklı boyutlarda yaşamaktadırlar. Bu doğrultuda, Rusya'nın izlemiş olduğu siber stratejilerin NATO üyesi ülkelerini korkutması bu durumun en güzel örneğidir. Soğuk Savaş'ın siber savaştan farkı ise, siber savaşın sadece iki kutup arasında yaşanmıyor olmasıdır. Caydırma ve çevreleme stratejisi Soğuk Savaş'ta uygulanırken, siber savaşta hibrit yöntemler ve enformasyon çağı etkili olmuştur. Siber

[2] Ahmet Emre Köker (2021), *Tehdit, Caydırıcılık ve Güvenlik: Çatışma ve Savaş İkileminde Siber Dünya*, İstanbul: Urzeni Yayınları, ss. 279-283.
[3] Hans Joachim Heintze & Pierre Thielbörger (2016), *From Cold War to Cyber War: The Evolution of the International Law of Peace and Armed Conflict over the Last 25 Years*, Cham: Springer, s. 24.

caydırıcılık da, aynı nükleer caydırıcılık gibi, korku salmakta ve cesaret kırmaktadır. Çünkü aynı saldırının kendisine karşı yapılabilme ihtimali, ülkelerin bu yeni silahı aleni kullanmalarını engellemektedir. Yani stratejik davranışın unsurları değişmemiştir; değişen, yalnızca bunların uygulanacağı durumların çok daha karmaşık hale gelmesidir.[4] Siber uzayın asimetrik özellikleri de bu karmaşıklığın asıl sebebidir.

Siber uzayın hâkim olarak kullanıldığı uluslararası ilişkilerde, büyük devletler, küçük devletlere karşı bile her türlü silahlı saldırıdan ziyade siber yöntemleri kullanmaya başlamıştır. Bunun en güzel örneği, 21. yüzyılda bu alanı en başarılı kullanan Rusya'nın NATO üyesi Estonya'ya veya eski Sovyet coğrafyasında olan Gürcistan ve Ukrayna'ya yönelik gerçekleştirdiği saldırgan hamlelerde görülmektedir. Bu hamleler, yeni bir dünya savaşına giden süreçte yeni bir alan olan siber uzayı Rusya'nın aktif bir şekilde kullandığını göstermektedir.

Aynı zamanda, uluslararası örgütlerin uluslararası politika aktörü olarak değerlendirilmesi ve ön plana alınması bir zorunluluktur. Bu zorunluluk kapsamında, Rusya'nın karşısında hem bölgesel, hem de küresel anlamda önemi düzeyde rol üstlenen NATO, bu makalede örnek olarak alınmıştır. NATO, siyasi, ekonomik, kültürel, askeri vb. birçok alanda önemli roller üstlenmekte, bireylerin hayatını ve düşüncelerini şekillendirmekte ve devletlerin politikalarını etkilemektedir. Bu çerçevede, hem coğrafi bir rol üstlenmekte, hem de amacı ve fonksiyonları itibariyle küresel bir etkiye sahip olabilmektedir.

Soğuk Savaş'ın sona ermesiyle, iki karşıt cephede olan ülkelerin ve örgütlerin güvenlik tedbirleri değişmiştir. Bu değişim, uluslararası güvenlik sistemini de tamamen değiştirmiştir. Özellikle Soğuk Savaş'ın getirmiş olduğu tehditlerin ortadan kalkmasıyla birlikte, NATO için "*siber uzay*" en önemli gündem maddelerinden biri haline gelmiştir. Böylece, hem Rusya, hem de NATO için uluslararası sistemde ortaya çıkan yapısal değişikliklerin etkileri "*siber savaş*" kavramının önemini artırmıştır. Bu yeni süreçte hangi sorunlarla karşılaşıldığı, bu sorunlar karşısında çözüme hangi politikalarla ulaşılmaya çalışıldığı ve kavramın uluslararası ilişkiler bağlamındaki önemi bu makalede analiz edilecektir.

Bu makalede tartışılan ilkelerin, kavramların ve fikirlerin çoğu, Rusya ve NATO içerisinde kullanılan sistemler, kurallar, kanunlar, söylemler, demeçler vb. bilişsel işlemlerdeki beklentileri, değerleri ve algıları içermektedir. Bu sebeple, bu süreci açıklamak için Dönüşüm Teorisi ve bu teoriyi açıklamaya yönelik Dönüştürücü Öğrenme Süreci'nin kullanılması

[4] Lawrence Freedman (2014), *Strateji*, İstanbul: Alfa Yayınları, s. 41.

araştırmayı geliştirmiştir. Özellikle NATO'nun siber uzayda ortaya koymaya çalıştığı bütünleşik müfredata yapılan vurgunun temeli, siber savaş sürecinin fikri temelini oluşturmaktadır. Zaten dönüşüm, tek bir bakış açısı olmayıp, farklı bakış açılarına sahip olmaktır. Burada gerçekleştirilen de, farklı bir bakış açısını ortaya çıkarmaktır.

Çalışmanın birinci bölümde, dönüşüm kavramı üzerinden teknolojinin uluslararası sistemdeki etkisi inşa edilerek, içinde bulunduğumuz süreç Dönüştürücü Öğrenme Kuramı çerçevesinde analiz edilmiştir. Böylece, içinde bulunduğumuz siber savaş süreci kavramsal olarak tanımlanmıştır. İkinci bölümde, Rusya'nın siber güvenlik çalışmalarına verdiği önem, siber uzayı bir doktrin haline getirme çabaları ve uluslararası ilişkilerde gerçekleştirdiği faaliyetlere odaklanılmıştır. Ayrıca, NATO'nun siber uzayda güvenliği sağlama çabalarının tarihi ve NATO'nun siber güvenlik stratejileri incelenmiştir. Üçüncü ve son bölümde ise, Rusya ile NATO arasında gerçekleşen siber kriz vakaları incelenerek, aktörler arasında yaşanan iki seviyeli oyun analiz edilerek çalışma sonlandırılacaktır.

1. Teorik Çerçeve

1.1. Dönüştürücülük Üzerine İnşa

Birinin diğerine fayda sağlaması amacıyla geliştirilen ve uygulanan "*teknoloji*" ve "*dönüşüm*" kavramları arasında tamamlayıcı bir ilişki bulunmaktadır. Dönüşüm kavramı, bazılarına göre bir doktrin olarak bağlamlarda gerçekleşmektedir. Bazı teorisyenler ise "*dönüşüm*" kavramını bir teori değil, öğrenmenin doğası hakkında bir epistemoloji veya felsefi bir açıklama şeklinde tanımlamaktadır.[5] "*Teknoloji*" kavramı ise, tasarımlara atıfta bulunmaktadır. Kavramlar arasındaki bu ilişki, uluslararası ilişkilerde aktif rol oynayan Rusya ve NATO'nun karşılıklı siber güç ilişkisinin şekillenmesine yol açmıştır.

Uluslararası ilişkiler özelinde, iki karşıt grubu ortaya çıkaran ilişkilere yönelik inceleme gerçekleştirilirken ampirik araştırmalara odaklanılmaktadır. Bu bağlamda, "*dönüşüm*" ve "*dijitalleşme*" kavramları ile bağlantılı vakalarda siber uzay da denkleme eklenmelidir. Bunun temel sebebi, yapıda ortaya çıkan bir dönüşümü anlamamız için olaya bütünleştirici bir şekilde yaklaşmamız gerektiğidir. Kapsam bu şekilde genişletildiğinde, uluslararası ilişkilerin anarşik yapısında faaliyet gösteren karşıt gruptaki NATO ve Rusya'nın sistemde yeni bir çatışma süreci içinde olduğu görülmektedir. Çünkü içinde bulunulan süreçte faaliyet gösteren her iki aktör de, destekçilerinden daha iyi bir algı kazanmayı amaçlamaktadır. Bu amaç

[5] Dale H. Schunk (2012), *Learning Theories: An Educational Perspective*, Sixth Edition, New Jersey: Pearson Education, ss. 230-233.

doğrultusunda, kendi inançlarını, varsayımlarını, hislerini ve deneyimlerini ön plana çıkaracak şekilde karşılıklı stresi artıracak bir süreci yaratmaktadır. Dönüştürücü Öğrenme Kuramı çerçevesinde içinde bulunulan bu süreç, Soğuk Savaş'tan siber savaşa geçişi içeren bir dönemi simgelemektedir. Böylece, içinde bulunduğumuz bu sürece yönelik ortaya koyduğumuz perspektifler "*siber savaş*" dönüşümünü kolaylaştırmaktadır.

Ortaya koyduğumuz bu perspektifte eleştirel yansıtma ile çatışma ve iş birliğine yönelik iletişim becerileri kuramın olmazsa olmaz temel dayanaklarıdır. Bu temel dayanaklar sonucunda, içinde bulunduğumuz süreci bir teori ile açıklayabilmemiz için siber çatışma sürecinde öğrenilenleri bilimsel olarak ortaya koymamız gerekmektedir.

Dale H. Schunk'a göre, öğrenme; yeni strateji, inanç, bilgi, beceri, davranış veya tutum kazanımı ya da değişimi olarak tanımlamaktadır.[6] Siber uzayda yaşandığını iddia ettiğimiz siber savaş dönemi de, geçmişte öğrenilmiş veya kabul edilmiş geleneksel yapıyı teknolojik gelişmelerin etkisiyle birlikte farklı bir şekilde siber uzay sorunsalı ile öğrenmemizi sağlamaktadır. Ayrıca, teoriler, hipotezlerin üretilmesine ve test edilmesine izin vermektedir. İnşacılar, bilgiyi gerçek olarak görmek yerine, onu çalışan bir hipotez olarak yorumlamaktadır.[7] Bu makalede ortaya koyduğumuz "*siber savaş*" dönemi sorunsalını dayandırdığımız "*dönüşüm*", siber uzay şeklinde beşinci boyutta ortaya çıkan olguların var olduğunu göstermektedir. Ayrıca bu olguları etkileyen ilkelerin var olduğunu ve keşfedilmesi için test edilmesi gerekmediğine bizi ulaştırmaktadır. Bu doğrultuda, dönüşüm kavramı kullanılarak, bu makalede genel tahminlerde bulunulmaktadır. Bu nedenle, araştırma, farklı yorumlara açıktır.

İnşacı teorisyenler, bilimsel gerçeklerin var olduğu ve keşfedilmeyi beklediği fikrini reddetmektedir.[8] Aynı zamanda, hiçbir ifadenin doğru olarak kabul edilemeyeceğini savunmaktadır. O yüzden, uluslararası ilişkilerde aktörlerin içinde bulunduğu süreç yorumlanırken, duruma makul şüphe ile bakılması yeterlidir. Bu makalede, siber uzayda yaşanan olaylara şüpheyle yaklaşılmaktadır. Bu şüphe sonucunda, Rusya ve NATO arasındaki ilişkilerde rol oynayan siber unsurlarla sürece yönelik genel değerlendirmeler gerçekleştirmektedir.

6 *A.g.e.*, s. 123.
7 Paul Cobb & Janet Bowers (1999), "Cognitive And Situated Learning Perspectives in Theory and Practice", *Educational Researcher*, Cilt 28, Sayı: 2, ss. 4-15.
8 Catherine T. Fosnot (2005), C*onstructivism: Theory, Perspectives, And Practice*, Second Edition, New York & London: Teachers College Press.

Uluslararası ilişkilerde aktörlerin faaliyet gösterdiği küresel dünya, zihinsel olarak birçok farklı şekilde inşa edilebilir. Bu nedenle, hiçbir teorinin gerçek doğruyu söylediği sonucuna ulaşamayız. Bu durum, makalenin temel dayanağı olan dönüşüm kavramı için de geçerlidir. Dijitalleşmenin etkisiyle hayatın her alanında ortaya çıkan dönüşüm sonucunda, aktörler, kendi içinde kabul ettikleri doğruları ve sahip oldukları kritik verileri saklamaktadır. Bu veriler gizli bilgilerdir. Dolayısıyla, tüm bilgiler öznel ve kişiseldir. Fakat siber uzayın bilinmez, tahmin edilemez ve öngörülemez özelliği, yapıyı tanımlamaya yönelik ortaya çıkan öznel ve kişisel tanımlamalara yönelik risk ve tehditleri artırmaktadır. Zaten karşıt iki grup olarak Rusya ve NATO üye ülkeleri arasındaki yaşanan siber çatışmalar ve bu çatışmalara yönelik yetkililer tarafından gerçekleştirilen söylemler, bu bilginin izinsiz kullanımı, ele geçirilmesi, engellenmesi vb. konularını içermektedir.

Tüm bu anlatılanlar ışığında, dönüşüm kavramının bir alt dalı olarak gösterilen "*dışsal dönüştürücülük*" kavramı, bilgi edinmenin, dünyada var olan yapıların yeniden inşasını temsil ettiğini belirtmektedir. Bu görüş, deneyimler ile öğretim ve modellere maruz kalma gibi dış dünyanın bilgi üzerinde güçlü bir etkisi olduğunu varsaymaktadır. Bu sebeple, bilgi, gerçeği yansıttığı ölçüde doğru kabul edilmektedir.[9] Ayrıca Rusya'nın siber uzayda güç kazandığı, NATO'nun siber güvenliği sağlama konusunda güç kaybettiği, her iki karşıt grup arasında siber savaş dönemi şeklinde uzunca bir süre hissedilen gerilimli korku sürecinin yaşandığı sonucuna ulaşmamızda, dönüşüm kavramı önemli bir görev üstlenmektedir. Bu bakış açısı, uluslararası ilişkilerin temelini oluşturan Realizm ve Liberalizm gibi birçok çağdaş teoriyle de uyumludur.

1.2. Dönüştürücü Öğrenme Kuramı

Bireylerin hayata bakış açıları, kendi deneyimleri, varsayımları ve inançları doğrultusunda gelişmektedir. Bu doğrultuda, inanç, varsayım ve deneyimler, bireylerin perspektiflerinin oluşmasında farklı bir vizyon kazandırmaktadır. Dönüştürücü Öğrenme kavramı ise, bu noktada ön plana çıkmaktadır. Kavram, deneyim, inanç ve varsayımlara eleştirel bir şekilde yaklaşarak, dünyanın algılanmasında yeni yöntemler geliştirilmesine katkı sağlanmaktadır.[10] Bu perspektif, uluslararası ilişkilerde önemli birer aktör olan devletler ve kurumlar için de aynı şekilde gerçekleşmektedir.

[9] Albert Bandura (1999), "Social Cognitive Theory: An Agentic Perspective, Stanford Uniiversity, USA", *Asian Journal Of Social Psychology*, Cilt 2, Sayı: 1, ss. 21-41.
[10] Burhan Akpınar (2010), "Transformatif Öğrenme Kuramı: Dönüşerek ve Değişerek Öğrenme", *Anadolu University Journal of Social Sciences***,** Cilt 10, Sayı: 2, ss. 185-198.

Dönüştürücü Öğrenme, hayatı yorumlayabilmek için varsayımların, deneyimlerin, duyguların ve inançların sorgulandığı gerilimli bir süreçtir. Öğrenme kuramlarının en yeni üyelerinden biri olan Dönüştürücü Öğrenme kuramının temeli, eleştirel yansıtma ve iletişim becerilerine dayanmaktadır.[11] Çalışmada, uluslararası ilişkilerde içinde bulunduğumuz sürecin tanımlanması, anlamlandırılması ve öğrenilmesi hedeflenmektedir. Bu kapsamda, Dönüştürücü Öğrenmenin anlamı, kapsamı, eleştirel yansıtmaları ve perspektif dönüşüme etkisi gibi temel kavramların etkilendiği felsefi akımlardan yola çıkılarak, süreç, siber savaş dönemi olarak tanımlanmıştır.

Siber savaş döneminin oluşmasıyla birlikte, günümüz uluslararası ilişkiler yapısını oluşturan temel teoriler anarşik yapıyı yeniden biçimlendirmiştir. Dönüştürücü Öğrenme Kuramı, süreci tanımlamak için bu noktada kullanılmıştır. Kullanan bu biçimlendirme, hayata dair daha gelişmiş bir algı geliştirilebilmesi amacıyla deneyimlerin, duyguların ve varsayımların sorgulamasını içermektedir. Çalışmada ortaya koyulan hipoteze yönelik eleştiriler olabilir. Çünkü ortaya konacak ikilemlere yönelik verilecek tek bir cevap bulunmamaktadır. Tek bir cevabın bulunmamasının sebebi ise, kullanılan teorilerin uluslararası toplumun yerleşmiş değerlerini sorgulamıyor olmasıdır. Ayrıca, geleceğin uluslararası sisteminin gerilimli, belirsiz ve karmaşıklıktan kaynaklanacak şekilde oluşacak olması da bir etkendir.

Belirsiz, gerilimli, karmaşık bu süreç, Rusya'nın ve NATO'nun risk ve tehditlere yönelik bakışlarını değiştirmelerine yol açmıştır. Değişen tehdit algısı, düşman tanımlamasını ve risk parametrelerini değiştirmiştir.[12] Bunun en önemli sebebi, siber uzayın sivilleşmesidir. Örneğin, uluslararası sistemde hâkim olarak kullanılan yapı, Vestfalya sisteminin yarattığı ulus-devlet modelinden doğrudan etkilenmiştir. Bu etkinin benzeri, Soğuk Savaş'ın bitmesiyle siber savaş döneminin konuşulmasını doğuran süreçte de görülmektedir.

Ayrıca, Colin S. Gray'a göre, günümüzde artık askeri yetenekler; hava gücü, uzay gücü, bilgiye dayalı savaş, siber savaş ve stratejik bilgi savaşı gibi alanlarda güvenlik, politik ve stratejik mücadeleleri kapsamaktadır.[13] Askeri yeteneklerin genişlediğini belirten Gray'in stratejik kültür bakışı çerçevesinde NATO ve Rusya'nın üst düzey yetkililerinin açıklamaları da değerlendirildiğinde, Soğuk Savaş ruhunun aslında bambaşka bir boyutta içinde tehdit, korku ve riskleri içerecek şekilde tamamen güvenlik kaygısı baz alınacak şekilde devam

[11] Egemen Şen & Hatice Şahin (2017), "Dönüştürücü Öğrenme Kuramı: Baskın Paradigmayı Yıkmak", *Tıp Dünyası Eğitimi*, Cilt 5, Sayı: 49, ss. 39-48.
[12] Salih Bıçakcı (2014), "NATO'nun Gelişen Tehdit Algısı: 21. Yüzyılda Siber Güvenlik", *Uluslararası ilişkiler Dergisi*, Cilt 10, Sayı: 40, ss. 101-130.
[13] Colin S. Gray (2008), *Modern Strateji*, İstanbul: Truva Yayınları.

ettiğini göstermektedir. Bu durum da, geçmişteki korkuların siber savaş boyutunda yaşandığını göstermektedir. Benzer bir süreç olmayan ve birbirlerinden tamamen farklı bir boyutta yaşanan siber savaş yıllarını Soğuk Savaş ile aynı kefeye koyamayız. Her ne kadar içinde bulunduğumuz siber savaş sürecini Soğuk Savaş ile aynı kefeye koyamasak da, Soğuk Savaş'ın bitmesiyle beraber uluslararası sistemin güvenlik dinamiklerinin değişerek siber güvenliği önemli hale getirdiği tartışmasız bir gerçektir.

Soğuk Savaş'ın bitmesinden sonra, özellikle Rusya ve NATO üyesi ülkeler arasında günümüzde siber savaş yaşanmaya başlamıştır. Bu iddianın gerçekliğini ortaya koymamızda Kuzey Atlantik Antlaşması Örgütü-NATO'nun 5. maddesi etkili olmuştur.[14] Bu maddeye göre; müttefiklerden birine yönelik gerçekleştirilecek bir saldırının bütün müttefiklere karşı yapıldığı belirtilmekte ve bu kapsamda karşılık verileceği vurgulanmaktadır. 17.10.2018 tarihinde NATO Genel Sekreteri Jens Stoltenberg'in Rusya tarafından NATO üyesi ülkelere yönelik siber saldırıların gerçekleştirildiğini iddia ettiği ve madde 5'in devreye sokulabileceğini belirttiği sözleri[15], siber uzayın uluslararası ilişkilerin güvenlik literatüründeki önemini gösteren en güzel örneklerden biri olmuştur. Böylece, NATO'nun üyeleriyle iş birliği geliştirmeleri, toplu savunma uygulamaları ve kriz yönetimi stratejilerinin belirlenmesine dayalı güvenlik yaklaşımını ittifakların siber alandaki faaliyetlerinde yürütme niyeti herkes tarafından görülmüştür.

Sonuç olarak, Soğuk Savaş'ın bitmesiyle beraber uluslararası sistemin güvenlik dinamikleri değişmiştir. NATO ve Rusya, yeni durumun gereklerine göre yeniden yapılanmıştır. Bu doğrultuda, dünyanın en büyük askeri örgütlerinden biri olan NATO'nun siber strateji kavramına bakışı, Colin S. Gray'in stratejik kültür bakışını destekler nitelikte olmuştur. Bu bakış, kısaca; stratejik olsun olmasın, geçmişte paylaşılan kültürün bir şekilde davranıştan ayrılmasının mümkün olmadığı sonucuna dayanmaktadır. Bu sebeple, NATO'nun Soğuk Savaş döneminde yaşadığı geçmiş korkularının 21. yüzyıl güvenlik bakışını şekillendirdiği yönünde stratejik kültürle bir bağ kurulabilir. Aynı zamanda, Rusya'nın geçmişten gelen

[14] Madde 5: Taraflar, Kuzey Amerika'da veya Avrupa'da içlerinden bir veya daha çoğuna yöneltilecek silahlı bir saldırının hepsine yöneltilmiş bir saldırı olarak değerlendirileceğini belirtmektedir. Bu bağlamda saldırı gerçekleşmesi halinde BM Yasası'nın 51. Maddesinde tanınan bireysel ya da toplu öz savunma hakkını kullanarak, Kuzey Atlantik bölgesinde güvenliği sağlamak ve korumak için bireysel veya toplu olarak silahlı kuvvet kullanımı dahil olmak üzere tüm eylemlerin gerçekleştirilebileceği konusunda bu maddeyle anlaşılmıştır. Ayrıca bu tarz saldırıların gerçekleşmesi halinde konunun Güvenlik Konseyi'ne bildirileceği ve Güvenlik Konseyi'nin uluslararası barış ve güvenliği sağlamak ve korumak için gerekli önlemleri alması halinde gerçekleştirilen önlemlerin sonlandırılacağı belirtilmiştir. Bakınız; NATO, "The North Atlantic Treaty Washington D.C. - 4 April 1949", Erişim Tarihi: 24.11.2020, Erişim Adresi: https://www.nato.int/cps/fr/natohq/official_texts_17120.htm?selectedLocale=en.

[15] *Türkiye Gazetesi* (2018), "NATO Gözünü Karartı! Büyük Tehdit", 17.09.2018, Erişim Tarihi: 29.01.2020, Erişim Adresi: https://www.turkiyegazetesi.com.tr/fotogaleri/nato-gozunu-karartti-buyuk-tehdit-16610.

Avrupa'ya hâkim olma ve süper güç olma fikirlerinin de, gelecek siber savaş stratejilerine yönelik dış politika oluşturma süreci hakkında bir stratejik kültür yarattığı düşünülebilir. NATO ülkeleri ve Rusya arasında gerçekleştiğini iddia ettiğimiz bu siber çatışma sürecinin gelişimi hakkında şu noktalar ön plana çıkmıştır.

2. Rusya ve NATO'ya Yönelik İncelemeler

2.1. Rusya'nın Siber Güvenlik Stratejisi ve Politikaları

Rusya, kendi siber gündemi olan güçlü bir uluslararası aktördür. Rusya, NATO için çok önemli bir rakip güçtür. Aynı zamanda NATO'ya üye ülkeler için de, Rusya, çok ciddi bir tehdittir. Özellikle son yıllarda yaşanan Estonya, Gürcistan ve Ukrayna sorunları gibi birçok siber saldırıda Rusya'nın etkisinin olduğu yazılmaktadır. Bu kapsamda, siber uzaya yönelik NATO ile Rusya arasındaki dengeyi daha da hassas hale getirmemiz gerekmektedir. Çünkü NATO ile Rusya arasındaki ilişkilerde siber saldırılar sonucunda ortaya çıkabilecek tehditler, günümüzde artık ciddi ve sorunlu konular haline gelmiştir.

Rusya ve NATO arasındaki ikili ilişkilerde birçok açmaz bulunmaktadır. NATO'ya üye devletlerin Rusya'ya yönelik yürüttüğü farklı siber stratejiler ve bu stratejileri uygulamaya yönelik geliştirdikleri çeşitli politikalar, Rusya'nın siber ortamda NATO'dan bir adım önde olmasına yol açmaktadır. Diğer yandan, Rusya, küresel olarak dezenformasyon, propaganda, casusluk ve yıkıcı siber saldırılar yürütmektir. Bu faaliyetleri yürütürken de gelişmiş siber yetenekler kullanmaktadır. Özellikle bu operasyonları yürütmek için, Rusya, çeşitli güvenlik ve istihbarat teşkilatları tarafından denetlenen çok sayıda birim oluşturmuştur. Oluşturulan bu mekanizmalar sayesinde, Rusya'nın güvenlik kurumları birbirleriyle rekabet etmekte ve genellikle aynı hedefler üzerinde benzer operasyonlar yürütmektedir.[16] Bu durum, rakip güçlerin ve dolayısıyla NATO ve üyelerinin belirli atıf ve motivasyon değerlendirmelerini zorlaştırmaktadır.

Rusya'da siber ortamda faaliyet gösteren en önemli birimlerden biri GRU'dur. Genel olarak GRU olarak anılan Genelkurmay Ana Müdürlüğü, Rusya'nın askeri istihbarat teşkilatıdır.[17] Bu teşkilatın, Rusya'nın en kötü şöhretli ve zarar verici siber operasyonlarına karıştığı iddia edilmektedir. GRU'nun siber birimlerine yönelik ABD'nin ciddi suçlamaları bulunmaktadır. Örneğin, ABD Adalet Bakanlığı, 2016 ABD Başkanlık seçimlerine yönelik gerçekleşen çok

[16] Congressional Research Service, "Russian Cyber Units", Erişim Tarihi: 12.12.2022, Erişim Adresi: https://crsreports.congress.gov/product/pdf/IF/IF11718.
[17] Atalay Keleştemur (2015), *Siber İstihbarat*, İstanbul: Level Kitap Yayınevi.

sayıda zarar verici siber saldırılar hakkında GRU'nun ilgili birimlerinde çalışan personelleri suçladı.

Rusya'nın bu siber birimleri, yüksek bir operasyonel güce sahiptir. Aynı zamanda, bilgisayar korsanlığı araçları ve kötü amaçlı yazılım geliştirmeye yardımcı olan birkaç araştırma enstitüsünü de kontrol etmektedir. Bu kabiliyetler, Rusya'nın siber gücünü pekiştirmekte, siber birimlerinin şüpheli operasyonel güvenlik ve gizlilik seviyelerini artırmaktadır. Bu bağlamda, Rusya'nın artan siber güvenlik bilinci hızlı dijitalleşmeye ayak uydurma ihtiyacını pekiştirmektedir. NATO ve üyeleri arasındaki ayrışmalar da Rusya'ya ciddi avantaj kazandırmaktadır. Ayrıca, dijital altyapıya yönelik artan bağımlılık, geleceğin mücadelelerinin de bu alana kayacağını göstermektedir.[18]

2.2. Rusya ve Doktrin Olarak Siber Savaşa Yönelim

NATO'nun izlediği politikalar karşısında Rusya'daki gelişmeleri izlediğimizde, gözümüze çarpan en önemli figür Valery Gerasimov'dir. 27 Şubat 2013 tarihinde dönemin Rusya Genelkurmay Başkanı Gerasimov, *Military Industrial Kurier* dergisinde "The Value of Science in Prediction" isimli bir makale yayınlamıştır. Makalenin genelinde Gerasimov tarafından ortaya konan askeri yaklaşım, "*Gerasimov Doktrini*" olarak adlandırılmaktadır. Gerasimov Doktrini, esasında askeri niteliğe sahip olmayan yöntemlere dayanmaktadır. Bu yöntemin özü, az insan kaybı ve maliyete dayanmaktadır. Böylece, sıcak çatışma süreçlerinin daha kolay yönlendirilmesi ve yönetilmesi hedeflenmektedir. Gerasimov Doktrini'nin ulaşmak istediği bu hedefler, askeri bir müdahale öncesine dayanmaktadır. Böylece, savaş gerçekleşmeden önce siber saldırılar düzenleyerek düşmana göre avantaj sağlanması veya hedefin yıpratılması hedeflenmektedir. Bu hedef doğrultusunda, psikolojik savaş yöntemleri ile de baskı altına alınan düşmanın morali bozulmakta ve savunma direnci kırılmaktadır. Bunun sonucunda da, kritik altyapılarına zarar verilen düşman, ekonomik bir zarara uğramaktadır.[19]

Bu doktrin, yeni bir savaş tarzı, "*genişletilmiş modern savaş teorisi*", hatta "*tam bir melez veya özel bir savaş vizyonu*"dur. Rusya'nın gerçek ama farklı bir meydan okuma tarzıdır. Çevreye korku ve kaos salmayı hedefleyen bu teori gibi, birçok farklı Rus doktrini

[18] Lester Wong (2020), "Cyber Security Awareness Must Keep Pace With Rapid Digitalisation: ST Webinar Panellists", *Straits Times*, 10.12.2020, Erişim Tarihi: 06.01.2020, Erişim Adresi: https://www.straitstimes.com/tech/cyber-security-awareness-must-keep-pace-with-rapid-digitalisation-st-webinar-panellists.

[19] Mark Galeotti (2018), "I'm Sorry for Creating the 'Gerasimov Doctrine'", *Foreign Policy*, 05.03.2018, Erişim Tarihi: 30.01.2020, Erişim Adresi: https://foreignpolicy.com/2018/03/05/im-sorry-for-creating-the-gerasimov-doctrine/.

bulunmaktadır. Fakat Rusya tarafından ortaya konan bu siber strateji, dikkati dağıtmak, bölmek ve demoralize etmek için geniş bir politik hedefi içinde barındırmaktadır.

21. yüzyılda savaşlar artık ilan edilmemekte ve başladıktan sonra da daha önceden bilinmeyen bir şablona göre gelişmektedir. Çünkü zayiat ve yıkım ölçeği, yıkıcı sosyal, ekonomik ve politik sonuçlar açısından bu tür çatışmaların sonucu herhangi bir gerçek savaşın sonuçlarıyla karşılaştırılabilecek bir seviyeye gelmiştir. Artan seviyeyle birlikte, bilgi çatışması eylemleri ile askeri kuvvetlerin eylemleri de dahil olmak üzere gizli bir karaktere sahip askeri ve teknolojik araçlarla çatışmalar desteklenmektedir. Gerasimov'un burada işaret ettiği şey, Rus Ordusu'nun uygun bir şekilde kullanılması gerektiğidir. Bu gereklilik çerçevesinde, Rusya tarafından birçok siber saldırı gerçekleştirilmiştir.

2.3. Rusya ve NATO'nun Dâhil Olduğu Siber Kriz Vakaları

Uluslararası ilişkilerde ihtiyaçların tam olarak karşılanamaması sebebiyle, birçok ülke, siber savunma ağlarının güvenliğinin sağlanmasında kendi geleneksel ordularına güvenmeyi ve siber savaş için kendi stratejilerini geliştirmeyi seçmiştir. NATO üyelerinin hepsinin ortak bir sorunun çözümüne yönelik ortak bir yaklaşımda bulunma çabası ise görülmemektedir. Bu durum da NATO'nun siber güvenlik stratejileri oluşturmasını etkilemekte, ayrıca artan siber tehditleri ve saldırıları etkilemektedir. Örneğin, Estonya ve Gürcistan siber krizleri, NATO'nun Rusya'ya karşı siber strateji oluşturmasında ana tetikleyici unsur olmuştur.

2.3.1. Estonya Siber Savaşı (2007)

2007 yılında Estonya'nın savunma sistemini felç eden büyük çapta siber saldırılar gerçekleşti. Saldırılarda, kamu ve özel kuruluşların internet (web) siteleri hedef alındı. Gerçekleşen bu siber saldırılardan sonra, NATO'nun siber saldırılar ile ilgili tehdit algısı, risk parametreleri ve güvenlik algısı tamamen değişti. Bu çerçevede, Estonya siber savaşından sonra 2008 Bükreş Zirvesi gerçekleştirilmiştir. Zirvede, üye devletlerin siber uzaydaki güçlerinin artırılmasının, siber güvenliklerinin sağlanmasının ve saldırılara karşı kapasitelerinin geliştirilmesinin gerekliliği vurgulanmıştır. Söz konusu stratejik gereklilikler çerçevesinde de politikalar geliştirilmeye başlanmıştır.[20]

Ayrıca, NATO, güvenlik politikası içerisinde siber kavramını kullanarak iş birliğini geliştirmek, çözümler üretmek ve koordine etmek amacıyla Estonya olayından sonra Siber Savunma Mükemmeliyet Merkezi'ni kurmuştur. Estonya siber saldırısını takip eden dönemde,

[20] Merve Seren (2006), "Siber Tehditlerle Mücadelede Farkındalık ve Hazırlık", *Siyaset, Ekonomi ve Toplum Araştırmaları Vakfı (SETA) Analiz,* 183, ss. 16-17.

NATO ve Estonya iki "*stratejik ortak*" gibi hareket etmiştir. Bu ortaklık, üç temel nedene dayanmaktadır. Bunlardan birincisi, Estonya'nın siber saldırılarla nasıl başa çıkacağını bilmemesidir. İkincisi, teknolojik ve ekonomik iş birliği ile NATO üye ülkeleri arasında bağımlılığın önemli bir faktör olmasıdır. Üçüncüsü de, Rusya'nın uluslararası ilişkilerin güçlü bir aktörü olarak NATO karşısında önemli bir konuma sahip olmasıdır. Bir başka ifadeyle, NATO'nun geçmişten günümüze var oluşunun ana sebebini Rusya karşıtlığının beslemesidir. Bu üç sebebe ek olarak, konunun siber savaş kavramını da içermesi, siber konuların da tartışılması gerektiğini göstermiştir. Böylece, Estonya olayı sonrasında, NATO, siber güvenliği hızla ve ciddi olarak gündemine almıştır. Bu olay sonrasında NATO'nun en önemli ülkesi olan ABD'nin o dönemki Başkanı George W. Bush da, ABD sistemlerinin siber saldırılara karşı savunmasızlığını ve hükümetin bunlara karşı savunma geliştirme ihtiyacını kabul etmiştir.[21] Zaten ilerleyen dönemde gerçekleşen siber saldırılar da bunun doğruluğunu göstermiştir. Örneğin, 2020 yılında SolarWinds siber saldırısını düzenlenmiştir. Söz konusu siber saldırı, Rusya'da faaliyetlerini yürüten Nobelium tarafından gerçekleştirilmiştir. Grubun, 2021 yılında ABD bilgisayar sistemlerine bir kez daha sızdığı tespit edilmiştir. Söz konusu saldırı sonrasında ABD'deki yüzlerce şirket ve organizasyon zarara uğramıştır.[22]

2.3.2. Gürcistan Siber Savaşı (2008)

7 Ağustos 2008'de Gürcistan'da ayrılıkçılar ayaklanmıştır. Büyüyen hadiseler, Gürcistan'ı siber saldırılarla birlikte yaşanacak sıcak bir çatışma sürecine götürmüştür. Bu çatışmalarda, Gürcistan'ın bilgi altyapısının Estonya'dan farklı olduğu görülmüştür. Gürcistan'ın gelişmemiş altyapısı, saldırının etkisini hafifletmiştir. Saldırıların etkileri farklı olsa da, hem Gürcistan, hem de Estonya savaşının gelişimi ve saldırı sırasında izlenen yöntemler birbirlerine benzemektedir.[23]

Estonya örneğinde olduğu gibi, bu saldırı sonrasında da, NATO, Gürcistan'a destek olmuştur. 2008 yılında "*Gürcistan'a Karşı Siber Saldırılar: Belirlenmiş Hukuki Dersler*" başlıklı bir rapor, NATO Ortak Siber Savunma Mükemmeliyet Merkezi tarafından yayınlamıştır. Rapor, Rusya-Gürcistan Savaşı sırasındaki siber saldırılara karşı uygulamaları içermiştir.[24] Bu bağlamda, kalıplaşmış iki örnek olan Gürcistan ve Estonya örneklerinde görüldüğü üzere,

[21] Duncan B. Hollis (2007), "Rules of Cyberwar?", *Los Angeles Times*, 08.09.2007, Erişim Tarihi: 17.01.2020, Erişim Adresi: https://www.latimes.com/archives/la-xpm-2007-oct-08-oe-hollis8-story.html.
[22] *Reuters* (2021), "Rus Korsanlar Yeniden Siber Saldırı Düzenledi", 25.10.2021, Erişim Tarihi: 21.09.2021, Erişim Adresi: https://www.amerikaninsesi.com/a/rus-korsanlar-yeniden-siber-saldiri-duzenledi/6284386.html.
[23] Salih Bıçakçı, (2014), "NATO'nun Gelişen Tehdit Algısı: 21. Yüzyılda Siber Güvenlik".
[24] Mehmet Ada & Hüseyin Çakır (2017), "Kuzey Atlantik Antlaşma Örgütü'nün (NATO) Siber Güvenlik Stratejisinin İncelenmesi", *Düzce Üniversitesi Bilim ve Teknoloji Dergisi,* Cilt 5, Sayı: 2, ss. 632-656.

Rusya ve NATO üye ülkeleri arasında ortaya çıkan politik krizlerde siber saldırılar küçük çaplı bir etki unsuru olarak göze çarpmıştır. Ayrıca, bu siber saldırılar şu ana kadar büyük bir kriz yaratmamıştır.

Klasikleşmiş Gürcistan ve Estonya örneklerine ek olarak, Rusya, NATO ve ABD'nin Ortadoğu'daki en büyük düşmanlarından biri olan İran ile siber güvenlik konusunda bir yakınlaşmaya girmiştir. Bu kapsamda, Rusya ve İran arasında 26 Ocak 2021 tarihinde Moskova'da bilgi güvenliğini ve siber güvenliği genişletmek için bir siber güvenlik anlaşması imzalanmıştır. İmzalanan bu anlaşma, her iki ülke açısından da hem ulusal, hem de uluslararası siber güvenlik alanındaki ikili ilişkilerde önemli bir kilometre taşı olmuştur.[25] Bu sebeple, imzalanan bu anlaşmanın NATO'ya karşı bölgesel ve uluslararası iş birliğinin genişletilmesini amaçladığını rahatlıkla söyleyebiliriz. İmzalanan bu anlaşmaya göre, İran ve Rusya, güvenlik, teknik yardım ve siber suçlarla mücadele alanlarında siber iş birliklerini güçlendirmeyi hedeflemiştir. Ayrıca, asıl amacı istihbarat paylaşımı ve siber alanda savunma olan bu anlaşma çerçevesinde, İran'ın özellikle Batı teknolojisine olan bağımlılığının azaltılması planlanmıştır. Böylece, Rusya, NATO ve ABD karşısında İran'ın savunmasız olmasının önüne geçmeyi hedeflemiştir. Bu şekilde, Rusya, siber uzay üzerinde yeni bir güç dengesi oluşturmaya çalışmıştır. Bu çaba neticesinde, dijital altyapılarını saldırı ve savunmaya yönelik olarak geliştirmektedir. Bu yönelim, Rusya'nın siber uzaydaki gücünü pekiştirmektedir. NATO ise, siber uzayda hem kendisinin, hem de üyelerinin güvenliklerini sağlama mücadelesi vermektedir.

3. NATO'nun Siber Güvenlik Stratejisi ve Politikaları

11 Eylül (9/11) saldırısı gerçekleştikten sonra, NATO, Kasım 2002'de "*Prag Yetenek Taahhütleri*"ni kabul etti. Böylece, siber yeteneklerin ve siber saldırılara karşı korunmanın temeli atıldı. 2007 yılında NATO üyesi Estonya saldırıya uğradı. Bu siber saldırı, sürecin hazırlık boyutunu bir üst noktaya taşımıştır. Resmi bir "*NATO Siber Savunma Politikası*"nın hazırlanmasına ve "*Siber Savunma Mükemmeliyet Merkezi*"nin kurulmasına yol açan bu boyut kapsamı genişletmiştir.[26]

2008 yılında Bükreş Zirvesi ile NATO'nun yeniden yapılanmasına ve savaş kavramının dönüşmesine yönelik "*Strateji Belgesi*" oluşturuldu. Zirve Bildirgesi'nin 46. maddesi çok

[25] *Tehran Times* (2021), "CFR says cybersecurity co-op agreement between Russia, Iran likely to create hurdles for U.S.", 16.03.2021, Erişim Tarihi: 21.09.2021, Erişim Adresi: https://www.tehrantimes.com/news/459217/CFR-says-cybersecurity-co-op-agreement-between-Russia-Iran-likely.

[26] Özge Güleç & Zülfükar Aytaç Kişman (2021), "Uluslararası ilişkiler açısından siber güvenlik ve NATO'nun siber güvenlik stratejileri", *Akademik Açı*, Cilt 1, Sayı: 1, ss. 127-154.

önemlidir. Söz konusu maddeyle, NATO'nun güvenlik değişiminin gerçekleştirilmesi amacıyla gereken kaynağın sağlayacağı açıklandı. Bükreş Zirvesi'nin siber güvenliğin sağlanması noktasındaki en önemli sonucu ise, Brüksel Merkezli NATO Siber Savunma Yönetimi Otoritesi ve Tallin (Tallinn) Siber Savunma İşbirliği Mükemmeliyet Merkezi'nin kurulmasıdır.

2010 yılında Lizbon Zirvesi gerçekleştirildi. Zirvede, NATO'nun gündeminde siber saldırılara yönelik gerçekleştirilecek savunmanın sürekli hale getirilmesi yönünde karar alındı. 19 Kasım 2010'da, Lizbon'daki NATO Zirvesi içinde siber sorunları resmen tanıyan ittifak misyonu, yeni bir stratejik kavram yarattı. Siber saldırıların daha sık, daha düzenli ve daha pahalı hale gelmemesi için NATO'nun önleme, tespit etme, savunma yeteneğini geliştirme ihtiyacı belirtildi. Ayrıca, NATO'nun siber saldırılara karşı siber savunma yeteneklerini geliştirmek, planlamak ve koordine etmek yönünde adım atmasına karar verildi.[27]

2011 yılında NATO "*Siber Savunma Politikası*" ve "*Siber Savunma Eylem Planı*"nın detayları kabul edildi. Böylece, ittifakın başlıca görevlerinden olan kolektif savunma ve kriz yönetimini gerçekleştirmek amacıyla iletişim ve bilgi sistemlerinin korunmasında merkezileşmiş ve koordineli bir yaklaşım oluşturuldu.[28] Yeni belirlenen NATO Siber Savunma Politikası'na göre[29]:

- ✓ Siber savunma yetenekleri güçlendirilecek,
- ✓ NATO'nun kolektif ve savunma kriz yönetiminin planlama sürecine siber unsurlar entegre edilecek,
- ✓ Müttefikler için kritik olan siber unsurların korunması ve savunmasına odaklanılacak
- ✓ Merkezileşme sağlanarak NATO'nun kendi ağlarını koruması sağlanacak,
- ✓ Kritik altyapıların korunmasında müttefiklere yardım edilecek,
- ✓ Farkındalık programları geliştirilecek,
- ✓ Çalışmalarda üyelerin yanında bağlı ortaklar, uluslararası kuruluşlar, özel sektör ve akademik çevrede bulunacak,

[27] NATO (2010), "Active Engagement, Modern Defence", 19.11.2010, Erişim Tarihi: 10.10.2022, Erişim Adresi: www.nato.int/cps/en/natolive/official_texts_68580.htm.
[28] NATO (2011), "NATO Defence Ministers Adopt New Cyber Defense Policy", 08.06.2011, Erişim Tarihi: 21.01.2022, Erişim Adresi: https://www.nato.int/cps/en/natolive/news_75195.htm.
[29] Uğur Akyazı (2013), "Uluslararası Siber Güvenlik Strateji ve Doktrinleri Kapsamında Alınabilecek Tedbirler", içinde *6. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı Bildiriler Kitabı*, ss. 216-220.

- ✓ Tallin'den uzmanlık ve destek alınması için müttefikler teşvik edilecektir.

Bu politikalarda, NATO üyelerine yönelik siber savunma konusunda gerçekleştirilecek topluluk bazındaki çabalar belirtilmektedir. Fakat hangi pratik eylemlerin akacağı hala belirsizliğini korumaktadır.[30] Aynı zamanda, siber savunma politikasında açıklanan siber tehditler, 5. maddede belirtilen toplu savunma görevini gerçekleştirmeye yönelik potansiyel kaynak olarak tanımlanmıştır. Potansiyel kaynağı geliştirmek ve operasyonel hale getirmek amacıyla da, 2012 yılında NATO Bilgisayar Olayları Karşılama Kapasitesi tarafından 58 milyon Avroluk bir kontrat imzalanmıştır.[31]

NATO'nun siber güvenlik kapsamında uluslararası seviyede yaptığı ilk çalışmalar, "*Siber Savunma Mükemmeliyet Merkezi*" oluşturulması ve siber savaşta uygulanacak hukuk hakkında "*Tallin El Kitabı*"nın hazırlanmasıdır. Cambridge Üniversitesi uzman grubu görüşlerinden oluşan kitap, 2013 yılında yayınlanmıştır. *Tallin El Kitabı*, NATO destekçi ülkelerinin görüşlerini ya da resmi bir NATO görüşünü temsil etmemektedir.[32] 2014 yılında NATO üyeleri tarafından yeni bir karar alındı. Alınan bu karar çerçevesinde, siber savunma topyekün savunmanın vazgeçilmez bir parçası haline getirildi. 5. maddenin yürürlüğe konmasına imkân veren bu yaklaşım sonrasında, 2016 yılında siber uzay askerî operasyon yürütme yeri görülerek ulusal ağların ve altyapıların siber ortamda savunulmasının öncelikli olarak güçlendirilmesi gerektiği yönünde karara varıldı.[33]

Realizm'in önemli isimlerinden Clausewitz açısından baktığımızda, alınan kararlar ve el kitabının hazırlanması çok önemlidir. Çünkü bir müttefiki savaş alanına getiren manevra, muharebeyi kazanmak kadar önemlidir. Bu doğrultuda, günümüz toplumlarında "*Yıpratma*" stratejisi, klasik bir savaştan daha önemli bir güce sahiptir. Stratejik olarak yaklaştığımızda, siber saldırılar ile ulaşılmak istenen asıl hedef, rakip halkın ve toplumun moralini yok etmektir. Günümüzde de, Clausewiz'in "*savaş bir bütündür*" bakışı[34] doğrultusunda NATO'nun Estonya'da Tallin merkezli bir "*Siber Güvenlik Merkezi*" kurması, NATO'nun

[30] NATO, "Cyber defence", Erişim Tarihi: 20.01.2020, Erişim Adresi: https://www.nato.int/cps/en/natohq/topics_78170.htm.
[31] Neil Robinson (2017), "Başarılı Bir Siber Savunma İçin Harcama Yapmak", *NATO Dergisi*, Erişim Tarihi: 29.01.2020, Erişim Adresi: https://www.nato.int/docu/review/tr/articles/2017/04/06/basarili-bir-siber-savunma-icin-harcama-yapmak/index.html.
[32] Milli Güvenlik Kurulu Genel Sekreterliği, "Siber Savaşa Uygulanacak Hukuk Hakkında Tallinn El Kitabı", Erişim Tarihi: 29.01.2020, Erişim Adresi: https://docplayer.biz.tr/11039588-Siber-savasa-uygulanacak-hukuk-hakkinda-tallinn-el-kitabi.html.
[33] Laura Brent (2019), "NATO'nun Siber Uzaydaki Rolü", *NATO Dergisi*, 12.02.2019, Erişim Tarihi: 29.01.2020, Erişim Adresi: https://www.nato.int/docu/review/2019/Also-in-2019/natos-role-in-cyberspace-alliance-defence/TR/index.htm.
[34] Carl Von Clausewitz (2015), *Savaş Üzerine*, İstanbul: Doruk Yayınları.

siber uzay olarak tanımladığımız savaş alanına konumlanmasının en güzel örneğidir. Fakat NATO üye ülkelerini eğitmek, saldırı tatbikatlarını yürütmek ve uluslararası siber saldırı durumunda NATO'nun yapacağı stratejileri belirlemek üzere kurulan bu merkez, henüz beklentileri karşılayamamıştır.

2018 yılındaki Brüksel Zirvesi'nde, NATO'nun "*Siber Uzay Operasyonları Merkezi*" geliştirmesi yönünde çalışmalara başlandı. Planlanan Siber Uzay Operasyonları Merkezi'nin birçok amacı bulunmaktadır. Bunlar arasında; ittifakın siber operasyon ve misyonlarının planlamasını yapmak, güvenlik konusunda farkındalık yaratmak ve siber uzay operasyonlarının koordinasyonunu gerçekleştirmek bulunmaktadır. 3 Ekim 2018 tarihinde ABD Savunma Bakanlığı'nın uluslararası güvenlik konularında başdanışman olan Katie Wheelbarger'ın yaptığı açıklamayla ise, süreç bambaşka bir boyut kazanmıştır. Açıklamada, NATO'nun talep etmesi halinde, ABD'nin Rusya'ya karşı NATO'ya üye ülkelerle siber savaş yeteneklerini ortak bir çalışma altında kullanmaya hazır olduğunu belirtmiştir. ABD tarafından oluşturulan yeni boyutla birlikte, 2018 yılı içerisinde Rusya meydan okumaya devam etmiştir. Öyle ki, Rusya, 300.000 askerin katılımıyla birlikte düzenlediği tarihinin en büyük ve kapsamlı tatbikatını gerçekleştirmiştir. NATO da, Rusya sınırı yakınında "*Trident Juncture 2018*" askeri tatbikatını yapacağını ilan etmiştir. 2018 yılında yapılan bu tatbikatların en önemli özelliği, NATO'nun Kırım'ın Rusya tarafından ilhakına karşı verilecek tepkilere yönelik senaryoları da içermesidir. Ayrıca, Polonya, Litvanya, Letonya ve Estonya gibi ülkelerin yaşadığı Rusya endişesi de bu süreçte etkili olmuştur. Bu durum, 2021 yılının son aylarında Rusya ve Ukrayna arasında sıcak bir savaşa sürüklenme ihtimali ile ortaya çıkan krizde de aynı şekilde devam etmiştir. Bu krizlerden anlaşıldığı üzere, NATO üyesi küçük ve görece güçsüz ülkeler, güvenliklerini sağlamak için bir çözüm arayışına girmektedir. Bu arayışta da NATO ön plana çıkmaktadır. Bu bağlamda, Peter Katzenstein'ın büyük kısıtlamaların olduğu bir dünyada ulusal seçimlerin olasılığını korumanın küçük devletlerin ana stratejisi olduğunu belirtmiş olduğu sözleri[35,] makalede ortaya koyulan görüşü desteklemektedir.

Sonuç olarak, 2018 yılında Brüksel Zirvesi'nde NATO'nun bütünsellik içermesinin önemi belirtildi. Bu bütünsellik çerçevesinde, NATO, ortak savunma ve ortak caydırıcılık kavramlarının güçlendirilmesinin gerekliliği yineledi. Böylece, NATO, kara, deniz ve havada nasıl ittifak etkili çalışıyorsa, siber ortamda da ittifak olunması gerektiğini teyit etti. Fakat

[35] Peter. J. Katzenstein (1996), *The Culture of National Security: Norms, Identity, and Culture in World Politics*, New York: Columbia University Press. ss. 1-27.

NATO tarafından siber ortamda birlik her ne kadar teyit edilse de, bunda henüz başarılı olunamamıştır. Bu başarısızlıktaki en büyük zorluk ise, sonucunun askeri olmasına rağmen bu sonuca sadece askeri yoldan ulaşılamayacak olmasıdır. İlerleyen dönemlerde üyelerden birisinin kritik altyapısına yönelik gerçekleştirilecek bir siber saldırının NATO üyesi diğer ülkeleri de ilgilendireceği açıktır. İttifakın siber uzayda yeterince güven sağlayamaması ise, üye ülkelerin siber savunma imkân ve kabiliyetlerinin millileşmesine yol açmaktadır. Çünkü NATO özelinde siber güvenliği sağlama yönünde başarılı ve tüm üye devletler tarafından kabul edilen bir yapı üzerinde henüz anlaşılamamıştır.

4. NATO ve Rusya Arasındaki İlişkiler: İki Seviyeli Bir Oyun

NATO, SSCB'nin çöküşünün ardından Rusya ile ilişkilerinin temelini oluşturan bazı politika çizgilerini benimsemiştir. Özellikle bu dönemden itibaren NATO ve Rusya ilişkilerinde birçok anlaşmazlık kaynağı oluşmuştur. Fakat dijitalleşmenin hızlanmasıyla birlikte, geleneksel sorunların bir bölümü siber boyuta taşınmıştır. Siber ortama taşınan sorunlarla birlikte, NATO, Rusya'ya karşı ortak siber strateji belirleme sürecine girmiştir. Bu stratejiyle paralel olarak, NATO üyeleri tarafından NATO'nun siber birlik politikası tam destek görmemiştir. Fakat NATO'nun siber uzaya yönelimi konusundaki tutarlılığı ve etkinliği devam etmektedir. Bu yüzden, NATO ile Rusya arasındaki ikili ilişkilerin konuşulmasında siber konuların dâhil edilmemesi, NATO-Rusya ilişkilerine ilişkin bir çalışmada eksik kalacaktır.

NATO üyelerinin bazılarının güçlü siyasi ve ekonomik bir dijital altyapısı mevcutken, çoğunun siber saldırı veya savunma gücü zayıftır. "*Stratejik*" veya "*özel*" ortaklık olarak ortak bir NATO siber yapısının oluşturulamamış olmasından kaynaklı Rusya'dan geldiği iddia edilen siber saldırılara karşı üye ülkeler tek başlarına kendi sanal sistemlerini korumaya çalışmaktadır. Ülkeler arasındaki siber güç farklılıkları ise, savunma konusunda bazı sorunları ortaya çıkarmaktadır. Bu sorunlar, NATO'nun rekabette zayıf kalmasına yol açmaktadır. Bu sebeple, Rusya'ya yönelik NATO siber güvenlik politikalarını desteklemek için güçlü ülkelerin diğer üye ülkelere desteğini artırması gerekmektedir.

NATO tarafında bu sürecin oluşması aslına bakılırsa bir zorunluluk olmuştur. Çünkü son 20 yılda, Rusya, çok çeşitli siber operasyonları üstlenmek için personelini, yeteneklerini ve kapasitesini artırdı. Tek bir Rus güvenlik veya istihbarat teşkilatı siber operasyonlardan sorumlu değildir. Rus siber birimleri birbirlerinin farkında olmadan benzer operasyonlar bile gerçekleştirmektedir. Aynı zamanda, bazı Rus kurumlar kurum içi yeteneklerin

geliştirilmesine öncelik verirken, diğerleri operasyonlar için dış aktörlerle sözleşme yapmayı tercih etmektedir.

Genel anlamda, iki rakip güç arasında gerçekleşen siber çatışmalar incelendiğinde, medya ve hükümet raporlarının incelenmesi bize veri sunmaktadır. Medya ve hükümet raporları incelendiğinde, Rusya'nın ilk siber operasyonlarının esas olarak Dağıtılmış Hizmet Reddi (DDoS) saldırılarından oluştuğu görülmektedir. Aynı zamanda Rusya tarafından gerçekleştiği iddia edilen bu saldırılar, genellikle suçlu ve sivil bilgisayar korsanları tarafından gerçekleştirilmiştir. 2007 yılında Estonya'ya yönelik gerçekleşen siber saldırın hedefleri de çevrimiçi bankacılık ve medya kuruluşlarından devlet internet siteleri ve e-posta hizmetlerine kadar uzanmaktaydı. 2008 yılında gerçekleşen Rusya-Gürcistan Savaşı'nda da tüm elektronik operasyonları 12 gün süreyle askıya alan National Bank of Georgia da dâhil olmak üzere 54 potansiyel hedefe yönelik DDoS saldırıları kullanıldı.

Görece NATO'nun zayıf halkaları olarak gözüken bu ülkeler, aynı zamanda Rusya için de stratejik öneme sahiptir. Stratejik olarak öneme sahip bu ülkeler, aslında iki rakip güç arasındaki siber mücadelenin görünen yüzünü bize göstermiştir. Bu kapsamda, iki seviyeli bu rekabet içerisinde sürecin iş birliği ve çatışmayı barındıracağı kaçınılmazdır. İş birliğinin ön plana çıktığının en somut göstergesi, NATO ve ABD arasında gerçekleşen siber uzaydaki stratejik ortaklıktır. Bu stratejik ortaklık çerçevesinde, Rusya tarafından gerçekleştirildiği iddia edilen siber saldırılarla ilgili NATO-ABD yönetimleri ortak bir payda içinde olduklarını bildirdi.[36]

Son olarak, günümüze artık bilgisayar saldırıları sadece diğer bilgisayarları değil, daha büyük altyapıları da tehdit etmektedir. Bu durum, virüsleri veya siber saldırıları füzeler kadar tehlikeli hale getirmektedir. Aynı zamanda, siber saldırılar, ölüm riskini ve çatışma maliyetlerini en aza indirme potansiyeline sahiptir. Yani gerçekleşen siber saldırılar, yok etmek veya yıkmak yerine, bozmak veya geçici olarak devre dışı bırakma seçeneği sunmaktadır. Bu süreçte NATO'nun siber güvenliği sağlama noktasında aldığı mesafe tartışmasız ortadadır. Fakat süreçle ilgili ciddi bir sorun bulunmaktadır. Bu sorun, siber saldırıların gerçekleşmesi halinde 5. maddenin ortak savunma olarak ne oranda değerlendireceğidir. Bunu bir başka şekilde ifade edersek, üye ülkelerden birine yönelik gerçekleştirilecek bir siber saldırıda 5. maddenin geçerli olup olmayacağıdır. Bu çerçevede,

[36] Ömer Tuğrul Çam (2021), "NATO ve AB, siber saldırılar karşısında ABD ile dayanışma açıklaması yaptı", *Anadolu Ajansı*, 15.04.2021, Erişim Tarihi: 11.10.2021, Erişim Adresi: https://www.aa.com.tr/tr/dunya/nato-ve-ab-siber-saldirilar-karsisinda-abd-ile-dayanisma-aciklamasi-yapti/2210200.

çatışma hukuku kuralları ve savaş hukukuna ilişkin uluslararası hukuk kurallarının siber savaşta uygulanıp uygulanamayacağına yönelik var olan belirsizlik uluslararası ortamda hala tartışılmaktadır.

Sonuç

Tarih boyunca, birey, kurum, örgüt veya devlet gibi farklı tüm aktörler güvenliklerini sağlamaya yönelik tedbirleri almıştır. Çünkü güvenlik kavramı, her aktör için en temel ihtiyaçlarından biri olmuştur. Tabii ki geçmişte uygulanan ilkel güvenlik tedbirleri zaman içerisinde değişime ve dönüşüme uğramıştır. Teknolojinin gelişmesiyle birlikte modern dijital araçların kullanımı önem kazanmıştır. Artan modern dijital uygulamalar sonrasında siber güvenlik konusu daha da güçlenmiştir.

1949 yılında kurulan NATO'nun temeli, üyeleri arasında iş birliğini geliştirmeye yönelik bir bağ oluşturmaktır. Oluşturulan bu bağ, NATO ittifak ülkelerini her türlü saldırıya karşı korumayı amaçlamaktadır. Bu sebeple, gelişen teknolojilere ayak uydurarak beşinci boyut güvenlik alanı olarak gösterilen siber uzayın NATO'nun güvenlik stratejileri ile politikalarının belirlenmesi sürecine entegre edilmesi oldukça önemlidir.

Soğuk Savaş'ın bitmesiyle birlikte SSCB dağılmıştır. SSCB'nin dağılmasıyla birlikte yeni bir güç olarak Rusya ortaya çıkmıştır. Rusya, Sovyet mirasına sahip olması sebebiyle, kurumsal olarak NATO ve dolayısıyla üyeleri üzerinde bir baskı ve tehdit unsuru olmuştur. İki karşıt güç arasında siber uzayda ortaya çıkan tartışmalar, demeçler ve çatışmalar sonucunda, konunun üzerine gidilmesi ve içinde bulunulan yapının öğrenilmesi ihtiyacı oluşmuştur. Bu kapsamda, inşacı görüşler bizim süreci yorumlamamıza katkı sağlamıştır.

Her iki karşıt grup da, siber uzayda dijital altyapılarını ve sınırlarını korumayı amaçlamaktadır. Bu çerçevede, süreç, bu karşıt grupların vatandaşlarının kritik verilerinin korunmasına yönelik gerçekleştirilen siber önlemleri ön plana çıkardı. Alınan önlemler, siber uzayın küresel anlamda kullanım yaygınlığını artırdı. Dolayısıyla, bu durum, siber risk ve tehditlerin de aynı oranda artmasına yol açtı. Özellikle artan dijitalleşmeyle birlikte çeşitlenen etkinlikler ve çevrimiçi hizmetlerin daha fazla kullanılması, NATO'ya üye ülkeler arasında yürütülen işlerde siber saldırganlar için yeni açıklıklar ortaya çıkardı. Ortaya çıkan bu açıklıklar, süreçte dönüşüm yaşandığını kanıtlamıştır. Yaşanan bu dönüşüm çerçevesinde, NATO'nun kurumsal olarak ortaya koyduğu stratejiler analiz edildi. Bu analiz sonucunda da, Rusya'nın özellikle dış politikada bir baskı unsuru olarak NATO üyesi ülkeler üzerinde etkili olmaya çalıştığı görüldü. Ayrıca Estonya siber saldırısı, NATO-Rusya ilişkilerine ağır bir

darbe getirdi. Özellikle gerçekleşen bu olay sonrasında süreci bir temele oturtmamız için NATO'nun Rusya'ya tepki göstermesi çıkış noktası oldu. Sonrasında da alınan kararlar ve gerçekleştirilen uygulamalar, saldırılara karşı gerçekleştirilebilecek bir misilleme etkisini gösterdi. Çünkü NATO üye ülkeleri düzeyindeki koordineli yaklaşım, ulusal düzeyde karşılık bulmadı. Aktörler arasında ulusal uyum olmaması, NATO üyeleri arasındaki siber birleşmenin ve tek sesliliğin olmasını engelledi. Bu engel, sürecin siber savaş dönemi olarak algılanmasını kolaylaştırdı.

Sonuç olarak, son yıllarda Rusya tarafından bir siber saldırının gerçekleşmiyor olması, Rusya ile NATO arasındaki düşmanlığı hafifletme umutlarını ortaya çıkarmaktadır. Fakat uzun vadede, her iki karşıt grup özelinde Soğuk Savaş'tan siber savaşa giden yapının varlığı inkâr edilemeyecektir. Bu yüzden, krizin çözümü, her iki karşıt güç unsurunun siber ortamda güçlü olması ve karşılıklı olarak oluşabilecek tahribatı düşünerek bir siber saldırı gerçekleştirmemesi özelinde sağlanabilir. Bu sonuca ulaşmamızda, Rusya ve NATO arasında yaşanan belirsiz, gerilimli, karmaşık risk ve tehditlere yönelik yaşanan sürecin dönüşüm kavramı üzerinden incelenmesi katkı sağlamıştır. Böylece, teknolojinin uluslararası sistemdeki etkisi, Dönüştürücü Öğrenme kavramının tecrübe, inanç ve varsayımları eleştirel yansıtmasıyla değerlendirilmiştir. Söz konusu değerlendirme sürecin yorumlanması ve dünyanın algılanmasında alternatif yöntemler geliştirilmesini kolaylaştırmıştır. Bu bağlamda, eleştirel yansıtma ile çatışma ve iş birliğine yönelik iletişim becerileri kuramın olmazsa olmaz temel dayanaklarını oluşturmuştur. Aynı zamanda, siber savaş sürecini açıklamak için dönüşüm teorisi ve bu teoriyi açıklamaya yönelik dönüştürücü öğrenme süreçlerinin kullanılması araştırmayı geliştirmiştir.

KAYNAKÇA

- Ada, Mehmet & Çakır, Hüseyin (2017), "Kuzey Atlantik Antlaşma Örgütü'nün (NATO) Siber Güvenlik Stratejisinin İncelenmesi", *Düzce Üniversitesi Bilim ve Teknoloji Dergisi,* Cilt 5, Sayı: 2, ss. 632-656.
- Akpınar, Burhan (2010), "Transformatif Öğrenme Kuramı: Dönüşerek ve Değişerek Öğrenme", *Anadolu University Journal of Social Sciences,* Cilt 10, Sayı: 2, ss. 185-198.
- Akyazı, Uğur (2013), "Uluslararası Siber Güvenlik Strateji ve Doktrinleri Kapsamında Alınabilecek Tedbirler", içinde *6. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı Bildiriler Kitabı*, ss. 216-220.
- Bandura, Albert (1999), "Social Cognitive Theory: An Agentic Perspective, Stanford Uniiversity, USA", *Asian Journal Of Social Psychology*, Cilt 2, Sayı: 1, ss. 21-41.
- Bıçakcı, Salih (2014), "NATO'nun Gelişen Tehdit Algısı: 21. Yüzyılda Siber Güvenlik", *Uluslararası ilişkiler Dergisi*, Cilt 10, Sayı: 40, ss. 101-130.
- Brent, Laura (2019), "NATO'nun Siber Uzaydaki Rolü", *NATO Dergisi,* 12.02.2019, Erişim Tarihi: 29.01.2020, Erişim Adresi: https://www.nato.int/docu/review/2019/Also-in-2019/natos-role-in-cyberspace-alliance-defence/TR/index.htm.
- Cobb, Paul & Bowers, Janet (1999), "Cognitive And Situated Learning Perspectives in Theory And Practice", *Educational Researcher*, Cilt 28, Sayı: 2, ss. 4-15.
- Congressional Research Service, "Russian Cyber Units", Erişim Tarihi: 12.12.2022, Erişim Adresi: https://crsreports.congress.gov/product/pdf/IF/IF11718.
- Çam, Ömer Tuğrul (2021), "NATO ve AB, siber saldırılar karşısında ABD ile dayanışma açıklaması yaptı", *Anadolu Ajansı,* 15.04.2021, Erişim Tarihi: 11.10.2021, Erişim Adresi: https://www.aa.com.tr/tr/dunya/nato-ve-ab-siber-saldirilar-karsisinda-abd-ile-dayanisma-aciklamasi-yapti/2210200.
- Fosnot, Catherine T. (2005), C*onstructivism: Theory, Perspectives, And Practice,* Second Edition, New York & London: Teachers College Press.
- Freedman, Lawrence (2014), *Strateji*, İstanbul: Alfa Yayınları.

- Galeotti, Mark (2018), "I'm Sorry for Creating the 'Gerasimov Doctrine'", *Foreign Policy*, 05.03.2018, Erişim Tarihi: 30.01.2020, Erişim Adresi: https://foreignpolicy.com/2018/03/05/im-sorry-for-creating-the-gerasimov-doctrine/.
- Gray, Colin S. (2008), *Modern Strateji*, İstanbul: Truva Yayınları.
- Güleç, Özge & Kişman, Zülfükar Aytaç (2021), "Uluslararası ilişkiler açısından siber güvenlik ve NATO'nun siber güvenlik stratejileri", *Akademik Açı*, Cilt 1, Sayı: 1, ss. 127-154.
- Heintze, Hans Joachim & Thielbörger, Pierre (2016), *From Cold War to Cyber War: The Evolution of the International Law of Peace and Armed Conflict over the Last 25 Years*, Cham: Springer.
- Hollis, Duncan B. (2007), "Rules of Cyberwar?", *Los Angeles Times*, 08.09.2007, Erişim Tarihi: 17.01.2020, Erişim Adresi: https://www.latimes.com/archives/la-xpm-2007-oct-08-oe-hollis8-story.html.
- Katzenstein, Peter J. (1996), *The Culture of National Security: Norms, Identity, and Culture in World Politics*, New York: Columbia University Press.
- Keleştemur, Atalay (2015), *Siber İstihbarat*, İstanbul: Level Kitap Yayınevi.
- Köker, Ahmet Emre (2021), *Tehdit, Caydırıcılık ve Güvenlik: Çatışma ve Savaş İkileminde Siber Dünya*, İstanbul: Urzeni Yayınları.
- Lester Wong (2020), "Cyber Security Awareness Must Keep Pace With Rapid Digitalisation: ST Webinar Panellists", *Straits Times*, 10.12.2020, Erişim Tarihi: 06.01.2020, Erişim Adresi: https://www.straitstimes.com/tech/cyber-security-awareness-must-keep-pace-with-rapid-digitalisation-st-webinar-panellists.
- Milli Güvenlik Kurulu Genel Sekreterliği, "Siber Savaşa Uygulanacak Hukuk Hakkında Tallinn El Kitabı", Erişim Tarihi: 29.01.2020, Erişim Adresi: https://docplayer.biz.tr/11039588-Siber-savasa-uygulanacak-hukuk-hakkinda-tallinn-el-kitabi.html.
- NATO, "Cyber defence", Erişim Tarihi: 20.01.2020, Erişim Adresi: https://www.nato.int/cps/en/natohq/topics_78170.htm.

- NATO, "The North Atlantic Treaty Washington D.C. - 4 April 1949", Erişim Tarihi: 24.11.2020, Erişim Adresi: https://www.nato.int/cps/fr/natohq/official_texts_17120.htm?selectedLocale=en.
- NATO (2010), "Active Engagement, Modern Defence", 19.11.2010, Erişim Tarihi: 10.10.2022, Erişim Adresi: www.nato.int/cps/en/natolive/official_texts_68580.htm.
- NATO (2011), "NATO Defence Ministers Adopt New Cyber Defense Policy", 08.06.2011, Erişim Tarihi: 21.01.2022, Erişim Adresi: https://www.nato.int/cps/en/natolive/news_75195.htm.
- *Reuters* (2021), "Rus Korsanlar Yeniden Siber Saldırı Düzenledi", 25.10.2021, Erişim Tarihi: 21.09.2021, Erişim Adresi: https://www.amerikaninsesi.com/a/rus-korsanlar-yeniden-siber-saldiri-duzenledi/6284386.html.
- Robinson, Neil (2017), "Başarılı Bir Siber Savunma İçin Harcama Yapmak", *NATO Dergisi*, Erişim Tarihi: 29.01.2020, Erişim Adresi: https://www.nato.int/docu/review/tr/articles/2017/04/06/basarili-bir-siber-savunma-icin-harcama-yapmak/index.html.
- Schunk, Dale H. (2012), L*earning Theories: An Educational Perspective*, Sixth Edition, New Jersey: Pearson Education.
- Seren, Merve (2006), "Siber Tehditlerle Mücadelede Farkındalık ve Hazırlık", *Siyaset, Ekonomi ve Toplum Araştırmaları Vakfı (SETA) Analiz,* 183, ss. 16-17.
- Şen, Egemen & Şahin, Hatice (2017), "Dönüştürücü Öğrenme Kuramı: Baskın Paradigmayı Yıkmak", *Tıp Dünyası Eğitimi*, Cilt 5, Sayı: 49, ss. 39-48.
- *Tehran Times* (2021), "CFR says cybersecurity co-op agreement between Russia, Iran likely to create hurdles for U.S.", 16.03.2021, Erişim Tarihi: 21.09.2021, Erişim Adresi: https://www.tehrantimes.com/news/459217/CFR-says-cybersecurity-co-op-agreement-between-Russia-Iran-likely.
- *Türkiye Gazetesi* (2018), "NATO Gözünü Karartti! Büyük Tehdit", 17.09.2018, Erişim Tarihi: 29.01.2020, Erişim Adresi: https://www.turkiyegazetesi.com.tr/fotogaleri/nato-gozunu-karartti-buyuk-tehdit-16610.
- Von Clausewitz, Carl (2015), *Savaş Üzerine*, İstanbul: Doruk Yayınları.