NATO'nun Siber Uzay Operasyonları:

Tehditlere Karşı Yeni Stratejiler

Roman ASGAROV[1]

Kahve için BT (Bilgi Teknolojileri) *güvenliğinden daha fazla zaman harcarsanız, saldırıya uğrayacaksınız. Dahası, saldırıya uğramayı hak* ediyorsunuz.

Richard Clarke, Beyaz Saray Siber Güvenlik Danışmanı, 1992-2003

Makale, siber uzayı NATO faaliyetlerinin ana alanlarından birine dönüştürme sürecini incelemektedir. NATO`nun uzayda yüzleştiği tehditler, NATO`nun sadece "sert caydırıcılık" konusunda uzmanlaşmasını değil, aynı zamanda yeni siber güvenlik stratejilerinin geliştirilmesinde önemli aktörlerden biri olmasını gerektirmektedir. İttifak`ın siber politikalarının adım adım gelişimi yapılan zirveler, kabul edilen konseptler ve hem İttifak hem de bireysel devletler bazında siber altyapıların geliştirilmesi amacıyla alınan kararlar hesaba katılarak yorumlanıyor. Makalede, NATO`nun tam teşekküllü siber güvenlik sistemi kurma ve kendi siber uzayının güvenliğini sağlama yolunda karşılaştığı engeller ve mevcut eksikler de mercek altına alınmıştır.

Anahtar Kelimeler: NATO, Siber Uzay, Siber Güvenlik, Toplu Güvenlik, Siber Strateji, Hibrit Savaş

The article examines the process of transforming cyberspace into one of the main areas of NATO activity. The threats that NATO faces in this space give rise to the need for NATO to specialize not only in "harsh deterrence", but also to become one of the leading actors in the development of new cybersecurity strategies. The step-by-step improvement of the Alliance's cyber policy is considered on the example of the summits, adopted concepts, as well as decisions aimed at developing cyberinfrastructure both at the level of the entire alliance and at the level of individual allied countries. The article highlights the shortcomings and obstacles in the way of NATO, which does not allow it to build a full-fledged cyber defense system and fully ensure the security of its cyberspace.

Keywords: NATO, Cyberspace, Cyber Security, Collective Security, Cyber Strategy, Hybrid War

[1] romanasgarov@gmail.com

Giriş

Modern dünyada, dijitalleşme süreçlerinin ve ülkelerin silahlı kuvvetlerinin teknolojik olarak daha gelişmiş cihazlarla donatılmasının bir sonucu olarak siber savunma ve siber güvenlik konuları giderek daha önemli hale gelmektedir. Bu teknolojik yenilikler, diğer bir deyişle "akıllı cihazlar", silahların kontrolü krizi ve genel olarak güvenlik konularında yeni yaklaşımlara ihtiyaç duyulmasına yol açmıştır. Askeri birliklerin operasyonel yeteneklerini artıran bu teknolojik gelişmeler, sürekli büyüyen ve giderek karmaşıklaşan siber saldırılar karşısında savunmasızlık derecesini de artırmaktadır. Özellikle hibrit nitelikteki çatışmalarda, siber saldırılar, geleneksel savaşın aksine, bilgi, ekonomik, diplomatik ve diğer hayati alanlarda kullanılabilecek en etkili araçlardan birine dönüşmüş durumda.

Siber saldırıların bir diğer ayırt edici özelliği, bu tür saldırılardan yalnızca müşteri devletlerinin değil, bireysel siber teröristlerin de sorumlu olabileceğidir ve böyle bir olasılık, söz edilen olguyla mücadeleyi daha da karmaşık hale getirmektedir.

Askeri ve askeri olmayan araçların bu karşılıklı bağımlı kullanımı, savaş ile barış arasındaki çizgiyi bulanıklaştırarak çatışmaları gittikçe daha melez hale getirdi. Bütün bunlar, savaşın doğasının büyük değişikliklere uğradığını ve yeni durumun NATO'nun hibrit çatışmalar bağlamında siber saldırılara özel dikkat göstermesini gerektirdiğinin altını çizmektedir.

Siber ile İlgili Kavramlar

"Siber uzay" terimi ilk olarak 1982'e yayınlanan William Gibson'ın "Burning Chrome" hikayesinde kullanılmıştır.[2] Bununla birlikte, terim, yazarın 1984'te, bilgisayarlar ve bilgisayar kümeleri arasında dolaşan ve insanların bilgi üreteci ve kullanıcısı haline geldiği üç boyutlu bir saf bilgi alanını tanımlayan romanı "Neuromancer"ı yayınladıktan sonra popülerlik kazandı. Cyberpunk tarzı bir eser olan bu roman, geleceğin sanal alanına fütürist bir bakış açısı sunan ilk çalışmalardan biridir. Yazar, eserin kendisinde bu kavramın net bir tanımını vermese de "Her ulustan milyarlarca yasal kullanıcının, matematiksel kavramları öğrenen çocukların her gün yaşadığı bilinç ve duyguyla ilerleyen istem dışı halüsinasyon", "İnsan sistemindeki her bilgisayarın kayıtlarından yansıyan verilerin grafiksel sunumu", "kavranamayacak bir karmaşa" gibi tanımlamalara dayanarak siber uzayın yüzeysel bir resmini oluşturmuştur.[3]

ABD Savunma Bakanlığı siber uzayı, "internet, telekomünikasyon ağları, bilgisayar sistemleri ve gömülü işlemciler ve denetleyiciler" dahil olmak üzere bilgi teknolojisi ile yerleşik veri altyapıları arasında bağlantılar oluşturan iç içe geçmiş bir ağ üzerinde çalışan küresel bir bilgi alanı olarak tanımlamakta.[4]

Siber uzay, yazılımlar, düzenlemeler, fikirler, yenilikler ve etkileşimler üzerine inşa edilmiş, dinamik olarak gelişen çok katmanlı bir sistemdir. Buna ilaveten, siber alandaki artan katılımcı sayısı da süreçlerin genel gelişimi üzerinde bir etkiye sahiptir.[5]

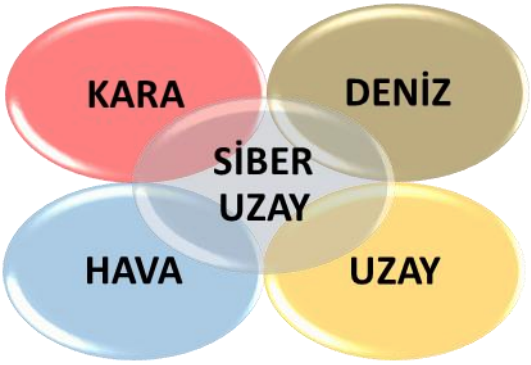
[2] Encyclopedia, "Cybercpace" https://www.encyclopedia.com/science-and-technology/computers-and-electrical-engineering/computers-and-computing/cyberspace , e.t. 04.04.2021

[3] William Gibson, Neuromancer, 1. baskı, çev. Gonca Gülbey, İstambul: Altıkırkbeş Yayın, Şubat 2012.

[4] Library of Congress. Congressional Research Service, "Defense Primer: Cyberspace Operations", 2020 https://crsreports.congress.gov/product/pdf/IF/IF10537/5, e.t. 04.04.2021

[5] Ronald Deibert, Rafal Rohozinski, "Liberation vs. Control: The Future of Cyberspace", Journal of Democracy, C. 21, S. 4, Ekim 2010, s. 45.

Siber uzay, beşinci boyut olarak bilinmesinin yanı sıra kara, hava, deniz ve uzay gibi diğer boyutların olanaklarını kullanır (şekil 1) ve kendisini tamamen bağımsız bir boyut olarak temsil eder.[6] Siber uzayı diğer boyutlardan farklı kılan temel değeri, insan faaliyetinin bir ürünü olmasıdır.[7]



Şekil 1 - **Beşinci Boyut Olarak Siber Uzay**

NATO, siber güvenlik müfredatında ABD Ulusal Standartlar ve Teknoloji Enstitüsü (NIST) tarafından sunulan siber güvenlik tanımına atıfta bulunmaktadır. Bu tanım, siber *güvenliği*, bilgi ve iletişim sistemlerinin ve burada yer alan bilgilerin her türlü "hasara, yetkisiz kullanıma, modifikasyon ve istismara" karşı korunduğu bir etkinlik veya durum olarak karakterize eder.[8]

Buna dayanarak, NATO için siber güvenliğin öncelikli olarak potansiyel tehditleri yansıtmaya ve saldırgan önlemler almaya hazır bir durum olduğu söylenebilir.

Şekil 2 - **Uluslararası Telekomünikasyon Birliği Tarafından Belirlenen Siber Güvenliğin Temel** Hedefleri[9]

RAND Corporation, siber *savaşı*, bilgisayar virüsleri ve çeşitli saldırı türleri ("Hizmet Reddi" örnek olarak gösterilmiş) aracılığıyla başka bir ülkenin bilgi ağlarının işleyişini istikrarsızlaştırmak için bir ulus devlet veya uluslararası kuruluş tarafından gerçekleştirilebilecek eylemler olarak tanımlar.[10]

Uluslararası ilişkiler alanında uzmanlaşmış ünlü İngiliz düşünce kuruluşu Chatham House'a göre siber savaşın ayırt edici bazı özellikleri aşağıdaki başlıklar altında sıralamıştır.

- Aktörlerin silahlı çatışmaya ihtiyaç duymadan siyasi ve stratejik hedeflerine ulaşmalarını sağlayabilir.
- Küçük ve nispeten önemsiz aktörlere orantısız güç imkânı verir.
- Sahte IP adresleri, yabancı sunucular ve takma adlar arkasında çalışan saldırganların kısa vadede neredeyse tamamen anonim olarak hareket etmesini sağlar.

[6] Mehmet Ada, Hüseyin Çakır, "Kuzey Atlantik Antlaşma Örgütü'nün (NATO) Siber Güvenlik Stratejisinin İncelenmesi", *Düzce Üniversitesi Bilim ve* Teknoloji Dergisi, C. 5, S. 2, (2017), s. 634.
[7] Martın C. Lıbıckı, Cyberdeterrence and Cyberwar, Santa Monika: RAND Corporation, 2009, s. 11.
[8] Sean S. Costigan, Michael A. Hennessy, "Cybersecurity: A Genetic Reference Cirruculum", Kingston: National Defence Office of the Commander Military Personnel Generation, Ekim 2016, s. 15.
[9] İnternational Telecommunication Union, "X-Series: Data Networks, Open System Communications and Security", Telecommunication Standardization Sector of ITU, 2008, ss. 2-3.
[10] RAND Corporation, "Cyber Warfare", https://www.rand.org/topics/cyber-warfare.html, e.t. 06.04.2021

- Konvansiyonel savaşın aksine, kara, deniz, hava ve uzay hariç, siber uzay olarak tanımlanan beşinci boyutta icra edilir.

- Siber savaşlar diğer baskı ve çatışma biçimleri ile aynı anda meydana gelebilmesine rağmen, yöntemleri ve araçları diğer çatışma biçimlerinden farklı kalır.[11]

NATO Siber Stratejisinde Siber **Güvenliğin Artan Rolüne Katkıda Bulunan Siber Savaşlar**

NATO-Kosova Krizi (1999). NATO'nun "Müttefik Güç" olarak adlandırılan ilk büyük askeri angajmanı, 1990'larda İnternet'in hızlı büyümesinden sonra geldi. Vietnam Savaşı dünyanın ilk televizyon savaşı olduğu gibi, Kosova Savaşı da ilk büyük ölçekli İnternet savaşına dönüştü.[12] İnternet daha önce Rus Çeçen savaşlarında bir araç olarak kullanılmış olsa da Kosova Savaşı'nda bu tür yöntemlerin kullanımı daha geniş, sonuçlarıysa daha yıkıcıydı. Ayrıca siber uzayda yaşanan bu olay, NATO'ya karşı yapılan ilk siber savaş olarak da bilinir.[13]

Kosova krizini daha geniş bölgesel Yugoslav savaşlarının bir parçası haline getiren ana tetikleyici, Kosovalı Arnavutlar ve Sırp nüfusu arasındaki uzun süren etnik çatışma olmuştur. 1989'te Sırbistan Cumhurbaşkanı Slobodan Miloseviç, Kosova'nın özerkliğini sınırlamak için attığı adımlar 1991'te Arnavutların referandum düzenlemesine ve bağımsızlık ilan etmesiyle sonuçlandı (bağımsızlık sadece Arnavutluk tarafından tanındı). Bunu takiben, Arnavutlar eyalet ve federal yapıları görmezden gelmeye ve kendi yönetim yapılarını oluşturmaya başladılar. Bu gelişmelerdeki diğer önemli bir olay, Batı Avrupa'da var olan organize bir yeraltı ağına dayanan ve 1990'ların ortalarında yaratılan Kosova Kurtuluş Ordusunun aktifleşmesiydi. Bu ağ, Kosova Kurtuluş Ordusu'nun silah rezervini tamamlamak için uyuşturucu kaçakçılığı ve adam kaçırma ile ün kazanmıştır.

1998'de Yugoslav polislerine ve ordusuna saldırılar düzenlenmesinin ardından iyi donanımlı Yugoslav ordusu, bu saldırılara bazen izin verilenin ötesine geçerek sert bir şekilde tepki gösterdi. Kötüleşen durumun bir sonucu olarak NATO, Yugoslavya Cumhuriyeti güçlerine karşı kendi operasyonunu başlatmaya karar verdi.

Sırbistan'a yönelik NATO hava harekatının başlamasıyla birlikte, birçok Sırp vatandaşı da bir şekilde NATO ile ilgili olan siteleri, sunucuları veya diğer altyapıları yok etmek veya zarar vermek için harekete geçti. Savaş esnasında, adını Birinci Dünya Savaşı'nın başlamasına sebep olan Pan-Slav gizli toplumundan alan "Black Hand" adlı bir grup korsan, faaliyetleriyle dikkat çekmeyi başardı. Başlangıçta grubun yıkıcı eylemleri, kosova.com ve İsveç merkezli Arnavut haber portalı zik.com gibi siteler de dahil olmak üzere daha çok Kosova ve Arnavut bazlı internet segmanı üzerine yoğunlaşmıştı. Ayrıca Kosova Kurtuluş Ordusu'nun internet sitesine zarar vermeyi de başardılar. Sırp bilgisayar korsanları, başta ABD Donanması sitesi olmak üzere ABD askeri sitelerine ve İnternet altyapısına saldırılar düzenleyen Rus bilgisayar korsanların da desteğini aldı. NATO'nun Belgrad'daki Çin büyükelçiliğini yanlışlıkla bombalaması Çinli bilgisayar korsanlarının da siber savaş alanına katılmalarıyla sonuçlandı.

NATO sunucuları devasa saldırılara maruz kalırken, NATO e-posta sunucuları günlük olarak 20.000'den fazla kötü amaçlı içeriğe sahip mesaj alarak çalışmayı durdurmak zorunda kaldı.[14]Sırp bilgisayar korsanları ayrıca, müttefik bilgisayarların

[11] Paul Cornish vd., "On Cyber Warfare", Londra: Chatam House, Kasım 2010, s. 1.
[12] Kenneth Geers, "Cyberspace and the Changing Nature of Warfare", Tallinn: U.S. Representative Cooperative Cyber Defence Centre of Excellence, t.y., s. 4.
[13] Piret Pernik, "Improving Cyber Security: NATO and the EU", Tallinn: International Centre for Defence Studies, Eylül 2014, s. 4.
[14] Mohan B. Gazula, Cyber Warfare Conflict Analysis and Case Studies, (Yüksek Lisans Tezi), Massachusetts: Massachusetts Institute of Technology, 2017, ss. 36-38.

İnternet ile düzgün bir şekilde etkileşime girmesini engelleyen ve ekranlarını havai fişek animasyonlarıyla çökerten "Happy 1999" kendi kendine yayılan makro virüsünü kullanarak NATO'nun e-posta altyapısını tahrip etmeyi başardı. Hatta halkla ilişkilerin sağlandığı web sitesi birkaç gün boyunca çalışamaz hale geldiğinden, NATO olayların kendi versiyonunu sunmak fırsatını bile kaybetmişti.[15] ABD, genel olarak büyük bir "etki altında" kalmadıklarını iddia ederken, İngiltere en azından bazı veritabanı bilgilerini kaybettiğini itiraf etti.[16]

78 gün süren askeri operasyonlar bitmesinin ardından İnternet alanındaki savaş da sona erdi. Askeri yeteneklerin düşmanla karşılaştırıldığında daha iyi olduğu için NATO'nun, birçok askeri görevi yerine getirebilmesine[17] rağmen, siber uzayda mevcut altyapısını zayıflatabilecek büyük boşluklar, NATO'nun gelecekte siber yeteneklerini geliştirmesini teşvik edecek olan ana nedenler olarak gösterilebilir.

Anıttan siber savaşa. Estonya örneği. (2007). Daha önce Tallin'in Merkez kavşaklarından birinde bulunan Sovyet askerlerine adanmış olan anıtın 26 Nisan 2007 tarihinde Tallinn'in askeri mezarlığına taşınması kararı, Rusya ile Estonya arasındaki ilişkilerin bozulmasına ve 22 gün süren siber savaşın başlamasına yol açtı.

Estonya hükümetin bu kararı aslında, anıtı bir kurtuluş sembolü olarak gören Estonya'nın Rus azınlığı ile anıtın ülkenin sömürücü Sovyet geçmişini temsil ettiğini düşünen Estonyalılar arasındaki gerilimi hafifletmeyi amaçlıyordu.

Estonya, internet ağına son derece bağlı bir ülke olduğu için, siber saldırıların hem sıradan vatandaşların günlük yaşamlarını hem de iş dünyasını sarsan olumsuz sonuçları oldu. Estonya bankaları, yalnızca ülke içindeki müşteriler için erişilebilirliği korurken tüm yabancı trafiği kısıtlamak zorunda kaldı. Temel olarak, siber saldırılar Hizmet Reddi (DoS) veya Dağıtılmış Hizmet Reddi (DdoS), 'Ping Flood', hatalı biçimlendirilmiş web sorguları, e-posta spam ve diğer tür saldırılarla tanımlanıyordu. Saldırıların esas hedefleri cumhurbaşkanı, parlamento, bankalar, küçük işletmelerin internet siteleri ve internet sağlayıcılarının bilgi sistemleriydi.

Tallinn'deki NATO Kooperatif Siber Savunma Mükemmeliyet Merkezi'nde araştırmacı Ottise'e göre, saldırganlar tarafından kullanılan trafiğin genellikle politik motifler içerdiği açıkça ortadaydı. Aynı zamanda Ottis, Rusça forumların saldırı için talimatların dağıtımının ana noktaları olduğuna da dikkat çekmektedir.

İki ülke arasındaki imzalanan "Karşılıklı Hukuki Yardım Anlaşması"na rağmen, Estonya Devlet Savcılığının Rusya Federasyonu Yüksek Savcılığına Mayıs 2007'de Rusya'da yaşayan saldırganları adalete teslim etme talebi hiçbir sonuç vermedi. Estonya soruşturmasına olan ilgisizlik, Rus hükümetinin, siber saldırılarla doğrudan bir bağlantısı olmasa bile, saldırganları tanımlamakla ilgilenmediğini ve bu nedenle aslında onları koruduğunu göstermektedir.

Ottis, bu olayı, hükümetin insanları düşmanlarına herhangi bir yolla saldırmaya motive ettiği Çin Halk Savaşı kavramının dijital versiyonuyla karşılaştırarak, dijital versiyonun, hükümete makul bir inkâr sağlamasıyla birlikte, yabancı araştırmacılarla işbirliği yapmayı reddederek saldırganları kolayca koruma fırsatı yarattığı belirtiyor.[18]

Estonya'ya yönelik siber saldırılar, bazı NATO ülkelerini siber savunma yeteneklerini gözden geçirmeye ve kapasitelerini güçlendirmek için bazı adımlar atmaya teşvik etti. Sonuç olarak Estonya, Mayıs 2008'de İtalya, İspanya, Slovakya, Almanya, Litvanya

[15] Dan Verton, "Serbs Launch Cyberattack on NATO", FWC, 04.04.1999 https://fcw.com/articles/1999/04/04/serbs-launch-cyberattack-on-nato.aspx, e.t. 07.04.2021
[16] Geers, a.g.m., s. 5.
[17] Gazula, a.g.e., s. 38-39.
[18] Rain Ottis, "Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective," Proceedings of the 7th European Conference on Information Warfare and Security, ed. Day Remenyi, UK: Academic Conferences Limited, 2008, ss. 164-168.

ve Letonya ile birlikte kooperatif bir Siber Savunma Mükemmeliyet Merkezi (CCDCOE/ Cooperative Cyber Defence Centre of Excellence) kurulması çağrısında bulundu.[19] Bu merkez üye devletlerin her yıl dünyanın en büyük siber savaş tatbikatı için bir araya geldiği "Kilitli Kalkanlar" a ev sahipliği yapıyor.

Tallinn Siber Savaşa Uygulanacak Uluslararası Hukuk Kılavuzu, Estonya'ya yönelik siber saldırıların bir diğer önemli sonucuydu. Bu kılavuz 2009 yılında 20 güvenlik uzmanı, hukuk uzmanı ve akademisyen tarafından hazırlandı. Mükemmeliyet Merkezi, sorumluluk sınırlarını fiziksel düzeyde değişikliklerle belirlerken, Tallinn Kılavuzu uluslararası siber hukukun bir aracına dönüşmekle birlikte siber güvenlik tartışmasını uluslararası alana taşıyan ilk belgelerden biri olarak, NATO ve BM'nin tutarlı bir siber güvenlik stratejisi oluşturması ve geliştirmesi için sağlıklı bir temel olarak kabul edilmektedir. [20]

Saldırıların ve toparlanmanın ardından Estonya, teknolojik güvenlikte lider olarak ilan edildi. Başkent Tallinn ise, NATO'nun siber güvenlik merkezlerinden birine dönüştü.

Gürcistan Siber Savaşı (2008). 2008'de Rusya ile Gürcistan arasındaki savaş sırasında, Rusya, geleneksel savaş tarihinde ilk kez askeri operasyonlarla birlikte bir siber saldırı gerçekleştirmiş oldu.[21]

Silahlı savaş Ağustos 2008'de başlamasına rağmen, bazı Amerikalı uzmanlar aynı yılın 20 Temmuz'unda Gürcü web sitelerinin etkinliklerini sınırlayan DDoS saldırılarına maruz kaldığını belirtti.[22] Bu siber saldırılar, Rus bilgisayar korsanlarının savaş öncesi provaları olarak da görülmektedir.[23]

Hudson Enstitüsü araştırmacısı Richard Weitz'e göre, bu teknikler savaştan çok daha önce hazırlanmış, ancak ana olaya kadar kullanılmamıştır. İnternet sitelerinde saldırganlar tarafından Gürcü kuvvetlerine operasyonun hazırlanması konusunda ipucu verecek "sitelerin herhangi bir ön araştırması veya haritalandırması yapılmadı", ancak bunun yerine özel olarak tasarlanmış yazılım uygulanmıştır.[24]

Estonya örneğinde olduğu gibi, Rus askeri komutanlığı botnet'ler oluşturarak bu saldırıları dünyanın farklı yerlerinde bulunan bilgisayarlar aracılığıyla organize etmiştir. Saldırılara katılanlardan bazılarıysa, doğrudan Rus askeri komutanlığı ile bağlantılı olmayan, ancak İnternet ve sosyal programlar aracılığıyla işe alınan sıradan İnternet kullanıcılarıydı.[25]

Askeri savaşın başladığı ağustos ayında gerçekleşen olayları incelediğimizde, ilk saldırı serisinin 6-7 Ağustos 2008 tarihlerinde botnet ve komuta kontrol sistemleri ile gerçekleştirildiğini görüyoruz. Siber saldırılardan 24 saat sonra Rus birlikleri askeri operasyona başladı. Askeri operasyonun ardından gelen ikinci siber saldırı dalgası, Gürcü İnternet platformlarında siber saldırıların gerçekleştirilmesine yönelik talimatların yayınlanmasıyla doğrudan ilgiliydi. Bu talimatlar, özellikle saldırıları gerçekleştirmek için kullanılan araçların ve nihai hedeflerin bir listesini içeriyordu. Bu saldırının ilginç tarafı Gürcü korsan forumunun bile bu hedefler arasında yer almasıydı. Gürcü bilgisayar korsanlarına yönelik saldırı,

[19] Häly Laasme, "Estonia: Cyber Window into the Future of NATO", Future of Defence, Washington: National Defense University Press, S. 63, 2011, s. 61.
[20] Madelena Anna Miniats, "War of Nerves: Russia's Use of Cyber Warfare in Estonia, Georgia and Ukraine", Senior Projects Spring, 2019, ss. 41-42
[21] Steffen Westerburger, Cyber Conflict in the 21st Century The Future of War and Security in a Digitalizing World, (Yüksek Lisans Tezi), Radboud University, Aralık 2014, s. 74
[22] The New York Times, "Before the Gunfire, Cyberattacks", https://www.nytimes.com/2008/08/13/technology/13cyber.html, e.t. 07.04.2021
[23] Max Gordon, "Lessons from the Front:A Case Study of Russıan Cyber Warfare", Alabama: Maxwell Air Force Base, Aralık 2015, s. 12.
[24] Richard Weitz, "Global Insights: Russia Refines Cyber Warfare Strategies", https://www.worldpoliticsreview.com/articles/4218/global-insights-russia-refines-cyber-warfare-strategies, e.t. 07.04.2021
[25] Alexander Melikishvili, "The Cyber Dimension of Russia's Attack on Georgia", https://jamestown.org/program/the-cyber-dimension-of-russias-attack-on-georgia/, e.t. 07.04.2021

kendileri tarafından olası bir misilleme saldırısını önlemeyi, bu sayede yapılan saldırıların etkinliğini mümkün olduğunca arttırmayı ve böylelikle gerçekleştirilen operasyonların öngörülemezliği duygusunu oluşturmayı amaçlıyordu.

Bu saldırılar, Gürcistan hükümeti ile toplum arasındaki iletişim kaybına neden olmuş, birçok finansal işlemi kesintiye uğratmış ve Gürcistan toplumunda kafa karışıklığına neden olmuştu.[26] Örneğin, Gürcistan parlamentosunun web sitesi hacklendikten sonra, Başkan Mikheil Saakashvili'yi Adolf Hitler ile karşılaştıran görüntüler yayınlanmıştır.[27]

Bir başka ilginç olay, başlangıçta belirtilen hedefler arasında, Rus bilgisayar korsanlarının zarar verme fırsatlarına sahip olmasına rağmen, gösterişli bir şekilde saldırıya uğramayan enerji tesisleri gibi önemli altyapı nesnelerin bulunmasıydı. Rus tarafının bu adımı, düşmanı korkutmayı ve onu fazla aşırılıktan alıkoymayı amaçlayan bir sinyal olarak görülebilir. Bu sinyal sadece Gürcistan'a değil, aynı zamanda eylemlerin ilerlemesini ayrıntılı olarak izleyen diğer ülkelere de hitap ediyordu.[28]

Bununla birlikte, Estonya ile karşılaştırıldığında, Gürcistan'a verilen hasar daha küçük bir ölçekte idi, bu da çoğunlukla Estonya'nın daha gelişmiş bir internet alanına sahip olmasıyla açıklanmaktadır.

Ukrayna senaryosu (2013-2015). Ukrayna Cumhurbaşkanı Yanukoviç'in 2013 yılının sonunda AB ile Ortaklık Anlaşmasını imzalamayı reddetmesi, başkent Ukrayna'da protestolara neden oldu.[29] Durumun daha da kötüleşmesi ve özellikle 100'den fazla kişinin öldüğü protestoların ardından Yanukoviç hükümetine yönelik acil tehditlerin ortaya çıkması, onu Rusya'ya kaçmaya zorladı.[30] Tüm bu olayların doruk noktası ise, Kırım'ın Mart-Şubat 2014'te Rusya Federasyonu tarafından ilhak edilmesi olayı oldu. Bu süre boyunca hem Rusya hem de Ukrayna'daki devlet kurumları ve medya, "DDoS saldırıları, web sitesi tahrifatı ve hedeflenen Kimlik Avı e-postaları gönderilen Uzaktan Yönetim Araçları (RAT) da dahil olmak üzere çeşitli siber saldırılara maruz kaldı.[31]

Ukrayna'ya karşı siber saldırıların yükselişi 2013 yılında başlamıştı. Ancak o zaman, bu girişimler DDoS saldırıları ile yürütülen ve Ukrayna sitelerinin içeriğine zarar vermeyi amaçlayan basit yapılardan oluşuyordu. E-posta hesaplarının hacklenmesi, çalınan bilgilerin yayınlanması ve propaganda amaçlı kısa mesajlarının gönderilmesi de Rus bilgisayar korsanlarının faaliyetlerinin bir parçasıydı. Haber portalları, medya, devlet kurumları, bankalar ve siyasi partiler ise siber saldırıların ana hedefleri haline gelmişti.

2013/2015 döneminde gerçekleştirilen saldırıların daha basit nitelikte olmasına rağmen, Ukrayna'nın enerji sektörünün saldırıların ana hedefi haline geldiği Aralık 2015'ten bu yana siber saldırılar daha sofistike ve karmaşık şekillere büründü. Bu tür saldırılar 2016 yılında da devam etti ve Kiev elektrik şebekesi gibi enerji altyapısının önemli bileşenlerine, Kiev havaalanına, devlet hazinesi ve Emeklilik Fonu da dahil olmak üzere finans sektörüne büyük zarar verdi. Ancak en büyük hasar, Haziran 2017'de, Rus askeri istihbaratı tarafından geliştirilen Notpetya Ransomware/Wipeware adlı fidye yazılımın Ukrayna'daki tüm bilgisayarların yaklaşık %10'unu devre dışı bırakması ve aynı zamanda Ukrayna'nın toplam GSYİH'sinin %0,5'i oranında mali kayıplara neden olmasıyla sonuçlanan siber saldırının sonucunda meydana geldi.

[26] Stephen Blank, "Cyber War and Information War à la Russe", From Understanding Cyber Conflict: Fourteen Analogies, ed. George Perkovich and Ariel E. Levite, Published by Georgetown University Press November 2017, s. 90.
[27] Westerburger, a.g.e., s. 74.
[28] Blank, a.g.e., ss. 88-90.
[29] BBC NEWS, "Ukraine protests after Yanukovych EU deal rejection", https://www.bbc.com/news/world-europe-25162563, e.t. 08.04.2021
[30] BBC NEWS, "Putin: Russia helped Yanukovych to flee Ukraine", https://www.bbc.com/news/world-europe-29761799, e.t. 08.04.2021
[31] Marie Baezner, Patrice Robin, "Hotspot Analysis: Cyber and Information warfare in the Ukrainian conflict", *Zürich: Center for Security Studies*, Ekim 2018, s. 3.

2014 yılında Rus Gelişmiş Kalıcı Tehdit (Advanced Persistent Threat/APT) grubunun Ukrayna Merkez seçim Komisyonu ağlarında keşfedilmesiyle[32] başka bir kriz meydana geldi. ABD ve bir dizi başka ülkenin güvenlik sersisleri tarafından yapılan açıklamalarda, bu korsan grubu, Rus özel servislerinin bir ürünü olarak tanımlandı. Bu olay aynı zamanda, Ukrayna seçimlerine Rusya'nın müdahalesi konusunda da tartışmalara yol açtı. Söz konusu korsan grubun Rus "Kanal Bir" TV istasyonu ile Ukrayna'nın seçim merkezlerindeki durum hakkında bilgi alışverişinde bulunmak için işbirliği yaptığı da belirtilmiştir.[33]

Saldırılara Rus özel servisleri ile birlikte Rusya yanlısı ayrılıkçı hacker gruplarının katılması olayı da tespit edildi. Özellikle CyberBercut adlı hacker grubu, Nisan ve Mayıs 2014'te Ukrayna Merkez Seçim Komisyonu ağlarına zarar vererek kendinden söz etmeyi başarmıştı.[34]

Rus yetkililer, özel servisler ve hacker grupları tarafından organize edilen siber alandaki tüm bu eylemler sonucunda Kırım olaylarının Rus versiyonu bilgi alanında baskın hale gelmiş ve Ukrayna hükümeti kendi vatandaşlarının itibarını kaybetmiştir.[35]

NATO **ve Siber Güvenlik**

Zamanla siber uzayın öneminin artacağının farkına varan NATO, çağın gereksinimlerini karşılamak için 1990'lardan itibaren bu yönde aktif adımlar atmaya başladı. Nesnel bir teknolojik gelişmenin bir sonucu olarak siber uzayda yeni risklerin ortaya çıkması, bu alanda Rusya ve Çin gibi tehdit oluşturan ülkelerin varlığı, NATO ve ortak ülkelerin tesislerine yönelik sürekli artan siber saldırılar bu süreçleri daha da hızlandırdı.

Konvansiyonel zorluklarla veya sözde "sert güvenlik" ile mücadelede uzmanlaşmış olan NATO'nun, büyük olasılıkla "yumuşak" güvenlik olarak sınıflandırılabilecek farklı nitelikteki tehditlerle karşı karşıya olduğunu da belirtmek gerekir.[36]

Bu açıdan "Yeni Stratejik Konsept"in kabul edildiği 1999 Washington zirvesi dikkat çekicidir. Söz konusu Konsepte göre teknolojinin gelişmesi, devlet dışı aktörlerin de silah üretme yöntemlerine erişmesine ve ülkelerle birlikte bu devlet dışı aktörlerin de NATO'nun güvenliğine tehdit oluşturan nesneler arasında yer almasına neden olmuştur.[37]

Bilgi altyapısının güvenliğinin sağlanması NATO için her zaman bir öncelik olmasına rağmen, siber savunma konusu İttifak'ın siyasi gündemine ancak 2002 yılında Prag Zirvesinde girmiş oldu.[38] 2002'deki Prag Zirvesi'nden bu yana, siber güvenlik savunma sisteminin bir parçası olarak giderek daha önemli hale geldi.

Siber güvenliğin artan önemi, resmi NATO belgelerinde "siber" kelimesinin kullanım miktarı ile de açıkça görülmektedir. Riga'daki zirveyi (2006) izleyen bildirgede "siber" kelimesi 1 kez, Bükreş'te 5 kez, Yeni NATO Konseptinde (2010) 5 kez, 2012 Chicago Zirvesi bildirisinde 10 kez, Galler Zirvesi'nin nihai bildirisinde ise 21 kez kullanılmıştır.[39]

[32] Nikolai Koval, "Revolution Hacking," Cyber War in Perspective: Russian Aggression against Ukraine, ed. Kenneth Geers, Tallinn: NATO CCD COE, 2015, s. 55-58.
[33] The New York Times, "In Ukraine, a Malware Expert Who Could Blow the Whistle on Russian Hacking" https://www.nytimes.com/2017/08/16/world/europe/russia-ukraine-malware-hacking-witness.html, e.t. 08.04.2021
[34] Piret Pernik, "The early days of cyberattacks: the cases of Estonia, Georgia and Ukraine", European Union Institute for Security Studies, 2018, ss. 61-62.
[35] Baezner, Robin, a.g.e., s. 3.
[36] Алексей Васильевич Казаковцев, "Нато и Кибербезопасность", *Вестник Волгоградского государственного университета, Серия 4: История. Регионоведение. Международные отношения*, 2012, s. 110.
[37] Doğan Şafak Polat, "Nato'nun Yeni Operasyon Alanı: Siber Uzay", *Güvenlik Bilimleri Dergisi*, ,UGK Özel Sayısı, Şubat 2020, s. 143.
[38] NATO, "Cyber Defence" https://www.nato.int/cps/en/natohq/topics_78170.htm, 09.04.2021
[39] Александр Ревский, "Кибербезопасность - новый повод для коллективной обороны", *Европейская*

Siber uzayda yeni yeteneklerin oluşumu, ilgili anlaşmaların başlangıçta resmi olarak imzalandığı ve ardından organizasyon yapılarının yaratıldığı geleneksel senaryodan (Tablo 1) kaynaklanıyor.

Tablo 1 - **NATO Kuzey Atlantik Konseyi Zirve Toplantılarında Temel Siber Sorunlar**

NATO Kuzey Atlantik Konseyi Zirve **Toplantıları**	**Zirve Sonucu Alınan Siber Güvenlikle İlişkili Önemli** Stratejik Kararlar
Prag Zirvesi **(Prag, Çek** Cumhuriyeti, 21 **Kasım 2002)**	NATO'nun siber güvenlikle ilgili başlangıç tutumu Prag Zirvesi Beyannamesi'nde "Siber saldırılara karşı savunma yeteneklerimizin güçlendirmek"[40] olarak yer ifade edilmiştir. Prag Zirvesinin en önemli sonuçlarından biri, İttifak'ın "siber olayları önlemek, tespit etmek ve bunlara müdahale etmek için "ilk müdahale ekipleri" olan NATO Bilgisayar Olaylarına Müdahale Yeteneğinin (NCIRC) oluşturulması kararı oldu."[41] Ayrıca, ordunun yeteneklerini zamanın talepleriyle uyumlu hale getirmek için "NATO Ağ Destekli Yetenekler" (Nato Network Enabled Capability/NNEC) olarak adlandırılan bir dönüşüm kursu başlattı. NNEC, ülkeler arasındaki işbirliğinin önemli ölçüde genişletilmesi, bilgi paylaşımının güvenli yollarının oluşturulması, daha hızlı karar vermenin teşvik edilmesi ve takım hızının artırılması gibi ortak faaliyetlerin özelliklerini geliştirmeyi amaçlamaktadır.[42]
Riga Zirvesi (Riga, Letonya, 29 **Kasım 2006)**	Riga Zirvesi Beyannamesinde, "… İttifak operasyonlarında güvenilir, emniyetli ve gecikmeden bilgi, veri ve istihbaratı paylaşmak için NATO Ağı Destekli bir Yetenek"[43] geliştirmeye sesleyen alt Madde bulabiliriz. Müttefikler ayrıca, NATO'nun bilgi sistemlerinin siber saldırılara direnme kapasitesini artırmaya kararlı olduklarını vurguladılar.
Bükreş Zirvesi (Bükreş, Romanya, 2-4 Nisan 2008)	NATO müttefiklerinden Estonya, Rus bilgisayar korsanları tarafından büyük ölçekli bir siber saldırıya maruz kaldığından, siber güvenlik konusu Bükreş zirvesinin gündeminin merkezinde yer aldı. Zirve Beyannamesinde "NATO'nun siber saldırılara karşı İttifak'ın önemli bilgi sistemlerini güçlendirmeye kararlı olduğu" belirtildi. Zirvenin ana katkısı, ilk Siber Savunma Politikasının kabul edilmesi ve bunu uygulamak için destekleyici yapıların ve otoritelerin geliştirilmesiydi.[44] Bükreş Zirvesi kararlarının bir sonucu olarak; • İttifak genelinde siber savunma operasyonları yeteneklerini merkezileştirmek için Brüksel'de, tehditleri tespit etmek ve kritik siber bilgileri gerçek zamanlı olarak paylaşmak için gelişmiş gerçek

безопасность: события, оценки, прогнозы, S. 35 (2014), s. 12.

[40] NATO, "Prague Summit Declaration" https://www.nato.int/cps/en/natohq/official_texts_19552.htm, e.t. 10.04.2021

[41] Jason Healey, Klara Tothova Jordan, "NATO's Cyber Capabilities: Yesterday, Today, and Tomorrow", *Washington: Atlantic Council*, Eylül 2014, s. 1.

[42] NATO, "NATO Network Enabled Capability (archived)" https://www.nato.int/cps/en/natolive/topics_54644.htm#:~:text=At%20the%20Prague%20Summit%20in,%2DEnabled%20Capabilities%20(NNEC), e.t. 10.04.2021

[43] NATO, "Riga Summit Declaration" https://www.nato.int/cps/en/natohq/official_texts_37920.htm?selectedLocale=en, e.t. 10.04.2021

[44] NATO, "Bucharest Summit Declaration" https://www.nato.int/cps/en/natolive/official_texts_8443.htm, e.t. 10.04.2021

	zamanlı elektronik izleme yetenekleri içerdiği düşünülen Siber Savunma Yönetim Otoritesi (Cyber Defence Management Authority/CDMA) tesis edildi. • Ekim 2008'de Tallinn'de, Kooperatif Siber Savunma Mükemmeliyet Merkezi (Cooperative Cyber Defence Centre of Excellence/CCDCoE) kuruldu. Bu merkezin kurulmasının temel amacı, uzun vadeli NATO siber savunma doktrini ve stratejisinin geliştirilmesiydi.[45] Merkezin görevleri arasında eğitim kursları düzenlemek, araştırmalar yapmak, geçmiş siber saldırıları inceleyerek dersler çıkarmak ve yeni siber saldırı durumunda önerilerde bulunmak da yer alıyordu. Siber güvenlik tartışmasını uluslararası alana taşıyan Tallinn Siber Savaşa Uygulanacak Uluslararası Hukuk Kılavuzu'nun hazırlanması da merkezin en büyük başarılarından biridir.
Lizbon Zirvesi (Lizbon, Portekiz, 19-**20 Kasım** 2010)	2010 Lizbon Zirvesi, NATO'nun siber güvenlik yeteneklerinde keskin bir artış için başlangıç noktası olarak kabul edilebilir. Zirve'nin en önemli sonucu, toplu savunma, kriz yönetimi ve kooperatif güvenlik olarak belirlenen üç temel göreve odaklanan "Aktif Katılım, Modern Savunma" adı altında yeni Stratejik Konsept'in kabul edilmesiydi.[46] Konsept, siber saldırıların değişen ve giderek daha karmaşık hale gelen doğasının yanı sıra, bu saldırıların yalnızca devlet idareleri, iş dünyası, ekonomi için değil, aynı zamanda ulaşım ve tedarik ağları gibi kamusal yaşamın diğer kritik alanları için de tehdit oluşturduğu gerçeğinin üzerinde durmaktaydı. Ayrıca, "Yabancı istihbarat ve askeri hizmetler, terörizm ve radikal gruplar saldırıların ana kaynakları"[47] olarak belirlenmiştir. Zirve'nin temel siber-stratejik hükümleri şu şekilde özetlenebilir; • NATO'nun siber uzaya sınırsız erişimini sağlamak ve kritik sisteminin bütünlüğünü korumak için modern çatışmaların siber boyutlarını dikkate almak ve İttifak için kritik öneme sahip sistemlere yönelik bir siber saldırı durumunda tespit, değerlendirme, önleme, savunma ve kurtarma yeteneklerinin geliştirilmesi. • 2012'ye kadar NATO Bilgisayar Olaylarına Müdahale Yeteneğini (NCIRC) tamamen operasyonel hale getirilmesi. • Tüm NATO organlarının merkezi siber koruma altına alınması. • Müttefiklerin siber savunma yeteneklerinin gelişimini teşvik etmek için NATO'nun savunma planlama süreçlerinin kullanılması ve ayrıca bilgi paylaşımını, işbirliğini ve birlikte çalışabilirliğin optimize edilmesi. • Siber uzaydan kaynaklanan güvenlik risklerini ele almak için BM ve AB gibi diğer aktörlerle yakından çalışmak. • Haziran 2011'e kadar güncellenmiş bir NATO derinlemesine siber savunma politikası ve destekleyici bir eylem planının sağlanması.[48]

[45] Rex B. Hughes, "NATO and Cyber Defence. Mission Accomplished?", Amsterdam: Atlantisch Perspectief, 2009.
[46] Jeffrey L. Caton, "Nato Cyberspace Capability: a Strategic and Operational Evolution", Strategic Studies Institute, US Army War College, 2016, s. 5.
[47] Wiesław Goździewicz vd., "NATO Road to Cybersecurity", Krakow: The Kosciuszko Institute, 2016, s.12.
[48] NATO, "Lisbon Summit Declaration" https://www.nato.int/cps/en/natolive/official_texts_68828.htm, e.t. 10.04.2021

	Lizbon Zirvesi'nin ardından, Haziran 2011'de Siber Savunma Konsepti, Politikası ve Eylem Planı kabul edildi. Ekim 2011'de, Eylem Planı'nın temel amacı bakanlar tarafından, siber saldırıları önlemek için yeni mekanizmalar geliştirmek ve tüm üye devletler bazında bir politika oluşturmak için müttefik ülkelerin politikalarını daha uyumlu bir duruma getirmek olarak belirlenmiştir. Ocak 2012'de, Bilgisayar Olayları Karşılama Yeteneği'ni tam anlamıyla faaliyete geçirmek için 58 milyon Avro değerinde bir sözleşme imzalanmıştır. Buna ek olarak, "İstihbarat paylaşımı ve durumsal farkındalık için "Siber Tehdit Farkındalık Birimi" oluşturulmuştur."[49]
Chicago Zirvesi (Chicago ABD, 20-21 Mayıs 2012)	Chicago Zirvesi bildirisinde, NATO'nun tüm kurumları merkezi bir siber savunma sistemi altında birleştirmeyi ve bu amaca ulaşmak için gerekli tüm önlemleri almayı amaçladığı belirtiliyor. AB, Avrupa Konseyi, BM ve AGİT gibi uluslararası kuruluşlarla işbirliğinin ortak bir avantaj sağladığının da altı çizilmiştir.
Galler Zirvesi (Cardiff, **Birleşik Krallık,** 4-**5 Eylül** 2014)	Galler zirvesi gelişmiş koruma politikasını onayladı. Bu politika kapsamında, siber savunma, toplu savunmanın temel misyonunun bir parçası olarak kabul edildi ve NATO, siber uzayda uluslararası hukukun uygulanmasına karar verdi. Siber saldırıların oluşturduğu tehlikenin geleneksel bir saldırı kadar yıkıcı olabileceği belirtildi. Zirvenin açıklamasına göre, siber saldırı durumunda 5.Madde'nin uygulanmasına ilişkin karar, Kuzey Atlantik Konseyi tarafından bireysel bazda alınacaktı. Gelişmiş siber savunma politikalarının tam olarak uygulanması için teknolojik yenilik ve özel sektör uzmanlığının özel rolünün altı çizildi. Siber savunma alanındaki NATO eğitim, öğretim ve tatbikatlarının seviyesinin iyileştirilmesi planlandı.[50]
Varşova Zirvesi (**Varşova,** Polonya, 8-9 Temmuz 2016)	Bu zirve, genel olarak siber güvenlik ve güvenlik konusunun güncelliğinin artırılması bakımından büyük önem taşıyordu. Güncel genel durum hem doğudan hem de güneyden, devlet ve devlet dışı aktörlerden, askeri güçlerden ve terör örgütlerinden, siber veya hibrit saldırılardan kaynaklanan tehditler ile sunuldu. En dikkat çekici ve önemli nokta, siber uzayın "NATO'nun havada, karada ve denizde olduğu kadar etkili bir şekilde savunması gereken operasyonların aynı alanı" olarak kabul edilmesiydi. Siber saldırı, geleneksel bir saldırı olarak değerlendirildi ve açık bir güvenlik sorunu olarak kabul edildi. "Ulusal ağların ve altyapının siber savunmasının" güçlendirilmesi de Müttefikler için bir öncelik olarak görüldü. "Uluslararası kuruluşların ve ortak ülkelerin, sanayi ve akademiyle işbirliğinin" daha da güçlendirileceği ifade edildi.[51] Aynı yıl NATO, Avrupa-Atlantik Bölgesi'ndeki "hızla gelişen siber tehdit ortamına ayak uydurmak" için Siber Savunma Taahhüdü'nü onayladı.[52]
Brüksel Zirvesi (**Brüksel, Belçika,** 11-12 Temmuz)	"Durumsal farkındalığı sağlamak ve NATO siber operasyonlarını koordine etmek" için, Belçika'da 2023'te tam olarak faaliyete geçecek bir Siber Uzay Operasyonları Merkezi kurulmasına karar verildi.[53]

[49] Polat, a.g.m., s. 148.
[50] NATO, "Wales Summit Declaration" https://www.nato.int/cps/en/natohq/official_texts_112964.htm, e.t. 10.04.2021
[51] NATO, "Cyber Defence" https://www.nato.int/cps/en/natohq/topics_78170.htm?selectedLocale=en, e.t. 11.04.2021
[52] Laura Brent, "The Past, Present and Future aof Nato's Cyber Defence", The Three Swords Magazine, 2020, s. 8.
[53] NATO, "Brussels Summit Declaration" https://www.nato.int/cps/en/natohq/official_texts_156624.htm, e.t. 11.04.2021

Londra Zirvesi **(Watford, Birleşik Krallık,** 3-**4 Aralık** 2019)	Bu zirvede, teknolojik üstünlüğün garantörü olarak hizmet etmesi, kritik altyapının dayanıklılığını daha da artırması ve güvenliğin sağlanmasına katkıda bulunması gereken yeni teknolojilerin rolüne özel bir vurgu yapıldı. Aynı zamanda enerji güvenliğinin sağlanmasının önemi belirtildi. Zirve bildirisinde, Müttefik ülkelerin siber saldırılara ve düşmanın hibrit taktiklerine müdahale araçlarını genişletmek niyetinde oldukları ve bu alandaki girişimlerinin devam edeceği de vurgulandı. NATO ve müttefiklerinin 5G de dahil olmak üzere iletişim güvenliğini sağlama taahhüdüne de dikkat çekilmiştir.[54]

Alınan kararlara ve atılan adımlara göre NATO'ya yönelik tehditlerin niteliği ve toplu savunmanın önceliklerinin değişmeye devam ettiği sonucuna varılabilir. Hibrit yüzleşmenin rolü ve yerinin güçlendirilmesi bağlamında alışılmadık yüzleşme yöntemlerinin ağırlığının nasıl arttığını görmek zor değil. Geleneksel olmayan türden tehditler bir tür rekabete dönüşmüş, giderek daha sofistike biçimler kazanmış, böylece karşıt tarafları yeteneklerini sürekli olarak artırmaya ve tehditleri ortadan kaldırmak için yaklaşımları değiştirmeye zorlamıştır.

Şüphesiz siber savunmayı ön plana çıkaran olaylara örnek olarak, siber savunmanın toplu savunmanın temel görevinin bir parçası olarak tanınması, uluslararası hukukun siber uzaya uygulanması, Galler Zirvesi'nin ardından siber saldırılara yanıt olarak Toplu Savunma Antlaşması'nın 5 Maddesini uygulama kararının kabul edilmesi ve siber uzayın hava, kara ve denizin yanı sıra yeni bir operasyon alanı ilan edilmesi gösterilebilir.

Ayrıca, Müttefikler de ulusal ağlarının ve altyapılarının siber savunmasını güçlendirmeye odaklanmıştır. 2016 yılında kabul edilen Siber Savunma Taahhüdü, özellikle siber direnci artırmayı ve siber saldırılara hızlı yanıt verme yeteneğini geliştirmeyi hedefliyor.

NATO, bilgi ve deneyimi paylaşarak, hızlı müdahale ekiplerini destekleyerek, siber savunma yeteneklerini geliştirmek için programlar - en ünlüsü Siber Koalisyon (Cyber Coalition) olan – düzenleyerek, eğitim, öğretim ve tatbikatlara yatırım yaparak bu konuda Müttefiklerin kapasitesini geliştirmeye yardımcı oluyor.

Ayrıca NATO'nun kendi saldırgan siber yeteneklerini geliştirme niyetinde olmadığını, ancak diğer alanlarda olduğu gibi, uluslararası hukuka uygun savunma eylemlerine bağlı kalmaya çalıştığını[55] belirtmek de önemlidir.

Şubat 2019'da NATO'nun ilk siber harekât doktrini kabul edildi. Bu doktrin, kötü niyetli saldırılara karşı savunma yeteneklerini daha da genişleterek ve NATO komutanlarına rehberlik ederek NATO'nun konumunu güçlendirecek.[56]

Rusya Bilimler Akademisi'nin önde gelen araştırmacısı Siyasal Bilimler Doktoru Andrei Manoilo'ya göre, NATO stratejik ve propaganda görevlerini çözmek için "5 göz", "9 göz", "14 göz"[57] gibi etkileşim formatlarının olanaklarını kullanıyor. Bu formatlar NATO üyelerini içermesine rağmen, daha çok Batı ülkeleri arasında İttifak ile doğrudan ilgisi olmayan istihbarat alışverişine ilişkin anlaşmalar olarak bilinirler.

Hibrit tehditler, NATO ve Avrupa Birliği arasında bir yakınlaşmayı teşvik ederek siber olaylara müdahale ekipleri arasında bilgi

[54] NATO, "London Declaration" https://www.nato.int/cps/en/natohq/official_texts_171584.htm, e.t. 11.04.2021
[55] Vsenato, "Киберзащита НАТО" http://vsenato.ru/cyber-zashita-nato/, e.t. 11.04.2021
[56] Laura Brent, "NATO's Role in Cyberspace" https://www.nato.int/docu/review/articles/2019/02/12/natos-role-in-cyberspace/index.html, e.t. 11.04.2021

[57] Андрей Викторович Манойло, "Современные стратегии кибербезопасности и кибероборонь НАТО", *Актуальные проблемы Европы*, 2020, 172-173.

paylaşımına neden oldu. 2016 yılında imzalanan Siber Savunma Düzenlemesi, bu tür bir işbirliğinin uygulamasını resmileştirdi.

AB'nin yanı sıra, bilgi alışverişi, eğitim ve öğretim alanında da benzer bir işbirliği uygulaması, NATO'nun teknolojik bileşeninin sürekli iyileştirilmesinin garantörü haline gelen sanayi ile de mevcuttur.

NATO Siber Güvenlik Yapıları

NATO Bilgisayar Olaylarına Müdahale Yeteneği (NCIRC) NATO'nun kendi ağlarının yirmi dört saat siber savunmasının yanı sıra siber uzay analizi sağlamasıyla bilinir.[58]

2023'te tam olarak faaliyete geçecek olan Mons Siber Operasyon Merkezi, durumsal farkındalık sağlayarak ve NATO'nun siber uzay operasyonlarını koordine ederek NATO'nun çevikliğini ve hareket özgürlüğünü artıracak.[59]

Şekil 3 - NCIRC Metodolojisi[60]

Tallinn'deki NATO Kooperatif Siber Savunma Mükemmeliyet Merkezi (CCDCoE), teknoloji, strateji, operasyonlar ve hukuk alanlarında disiplinler arası eğitim, araştırma ve geliştirmeye adanmış bir NATO araştırma ve geliştirme merkezi olarak tanınmaktadır.[61]

Oberammergau'daki NATO Okulu, İttifak'ın operasyonlarını, stratejisini, politikasını, doktrini ve prosedürlerini desteklemek için siber operasyonlar yürütmektedir.

Portekiz'in Oeiras kentindeki NATO İletişim ve Enformasyon Akademisi siber savunma uzmanlarına eğitim vermeyi, Roma merkezli NATO Savunma Koleji ise siyasi-askeri konularda stratejik düşünmenin geliştirilmesini esas hedef olarak belirlemiştir.[62]

NATO'nun Önündeki Engeller

NATO'nun temel hedeflerinden biri, 5. Madde ile ilgili olarak siber savaş ilkeleri konusunda bir fikir birliği bulmak olacaktır.

Tarihte ilk kez, Washington Antlaşması'nın 5. Maddesi, 11 Eylül'de ABD'ye yönelik terör saldırılarının ardından uygulandı. İttifakın 1999'da kabul edilen Stratejik Konseptinde, terörizm müttefiklerin güvenliği için bir tehdit olarak kabul edilmiştir. Kuzey Atlantik Konseyi, soruşturmasının sonuçlarına dayanarak, saldırının dışarıdan yapıldığına ve böyle bir saldırının 5. Madde kapsamına girdiği sonucuna vardı. Bu, NATO'nun Ekim 2001 ortasından Mayıs 2002 ortasına kadar "Eagle Assist" adli ilk anti-terör operasyonunu başlatmasına sebep oldu.

5. Maddeye göre, "Taraflar, Kuzey Amerika'da veya Avrupa'da içlerinden bir veya daha çoğuna yöneltilecek silahlı bir saldırının hepsine yöneltilmiş bir saldırı olarak değerlendirileceği ve eğer böyle bir saldın olursa BM Yasası'nın 51. Maddesinde tanınan bireysel ya da toplu öz savunma hakkını kullanarak, Kuzey Atlantik bölgesinde güvenliği sağlamak ve korumak için bireysel olarak ve diğerleri ile birlikte, silahlı kuvvet kullanımı da dahil olmak üzere gerekli görülen eylemlerde bulunarak saldırıya uğrayan Taraf ya da Taraflara yardımcı olacakları konusunda anlaşmışlardır. Böylesi herhangi bir saldın ve

[58] Vsenato, "Киберзащита НАТО" http://vsenato.ru/cyber-zashita-nato/, e.t. 13.04.2021
[59] NATO, "Cyber Defence" https://www.nato.int/cps/en/natohq/topics_78170.htm, e.t. 13.04.2021
[60] David P. Fidler, Richard Pregent, Alex Vandurme, "NATO, Cyber Defence, and International Law", *St. John's Journal of International & Comparative Law*, C. 4, S. 1 (2016), s. 10.
[61] CCDCOE https://ccdcoe.org/about-us/, e.t. 13.04.2021
[62] NATO, "Cyber Defence" https://www.nato.int/cps/en/natohq/topics_78170.htm, e.t. 13.04.2021

bunun sonucu olarak alınan bütün önlemler derhal Güvenlik Konseyi'ne bildirilecektir. Güvenlik Konseyi, uluslararası barış ve güvenliği sağlamak ve korumak için gerekli önlemleri aldığı zaman, bu önlemlere son verilecektir."[63]

Siber savunmanın kolektif korumanın temel görevinin bir parçası olarak tanınması ve siber uzay operasyonlarının önemini havada, karada ve denizde yapılan operasyonlarla eşit olarak görmesi, siber uzayın NATO'nun öncelikli alanlarından birine kademeli olarak dönüşmesini göstermektedir. Galler Zirvesi ise, bir siber saldırının 5. Maddenin kriterlerini karşıladığını doğrulamış oldu. NATO Genel Sekreteri Stoltenberg, siber saldırıların giderek daha karmaşık ve sık hale geldiğine, NATO ülkelerini siber güvenlik konusunda daha da titiz olmaya zorladıklarına defalarca dikkat çekerek, "NATO'nun bile siber saldırılara bağışıklığı yok ve sistemlerimize yönelik günlük şüpheli faaliyetlere" tanıklık ettiklerini belirtti. Toplu güvenlik sözleşmesinin 5. Maddesinin kullanımına değinen Stoltenberg, "ciddi bir siber saldırı"nın yukarıdaki maddenin kullanımına yol açacaktır.

Ancak NATO 5. Maddeyi tetikleyebilecek "ciddiyet" seviyesini henüz belirlemediğinden burada "Kırmızı Çizgi" sorunu ön plana çıkıyor.[64] Siber saldırı ile basit bir provokasyon arasındaki sınırı net bir şekilde tanımlayabilecek hiçbir kriter hala bulunmadığından,[65] bu boşluk 5. Maddenin en zayıf tarafı olarak kabul edilebilir. Bu sınırın bulanıklığından kaynaklanan sorunlu sonuçların açık bir örneği, nihayetinde bu maddenin caydırıcı doğasını sorgulayan ve gün geçtikçe artan siber saldırılardır.

NATO güvenlik yetkilisi L. Brent'e göre, Danimarka, Estonya, Litvanya, Hollanda, İngiltere ve ABD gibi bazı müttefikler, düşman bir devleti "davranışları değiştirmeye" zorlamak maksadiyla kötü niyetli siber faaliyetler için "açıkça suçlu" mekanizmalara başvuruyor. Örneğin, ABD Siber Komutanlığı'nın tutumuna gerekçe olarak, "rakiplerin kurumsal yapıları zayıflatmak ve stratejik avantajlar elde etmek için sürekli olarak silahlı çatışma eşiğine kadar hareket ettiği" ve ABD'nin siber uzayın güvenlik açıklarından yararlanarak siber saldırılar düzenleyenlere bu şekilde karşılık vereceği belirtiliyor.

Brent, NATO'nun silahlı çatışma eşiğine ulaşmayan kötü niyetli siber faaliyetlere karşı eylemlerinin diğer alanlarda olduğu kadar aktif olması gerektiğine inanıyor, çünkü bu tür faaliyetlerin bile yeteri kadar zararlı olduğunu düşünüyor. Soruna çözüm olarak, bir üye devletin toprak bütünlüğüne, siyasi bağımsızlığına veya güvenliğine tehdit olarak algılayabileceği kötü niyetli eylemlere maruz kaldığı takdirde, Washington Antlaşması'nın istişare sağlayan 4. Maddesi uygulanabilir.[66]

Security Lancaster merkezi araştırmacısı Oliver Fitton'ın işaret ettiği gibi, NATO'nun yolundaki bir sonraki engel, gri bölgede hareket eden düşmanın müdahalesini makul bir şekilde reddedebilmesidir. Bu nedenle, anonimlik, siber uzayın ana özelliği olarak tanımlanmaktadır, çünkü gerçek müşterinin tam olarak kim olduğunu belirlemek, özellikle de 2007'de Estonya'da olduğu gibi, başka bir devletin topraklarından gerçekleştiriliyorsa, genellikle imkansızdır. Ek olarak, saldırgan katılımını reddedebilir ve başka birini işaret edebilir. Dolayısıyla bu durum, düşmana karşı misilleme tedbirlerini tam olarak gerekçelendirmenin imkansızlığı olarak nitelendirilebilir.

NATO'ya engel olabilecek veya faaliyetlerinin özgürlüğünü kısıtlayabilecek faktörleri sıralayan Fitton, liberal-demokratik ilkelerin rolünü özellikle vurguluyor. Bu ilkeler,

[63] NATO, "Collective defence - Article 5" https://www.nato.int/cps/en/natohq/topics_110496.htm#:~:text=NATO%20invoked%20Article%205%20for,of%20the%20Russia%2DUkraine%20crisis. e.t. 13.04.2021

[64] Джон Нил, "Сдерживание в условиях гибридной войны, Сухопутные силы США", Per Concordiam, C. 10, S. 1 (2020), ss. 21-23.

[65] NATO, "Cyber Defence" https://www.nato.int/cps/en/natohq/topics_78170.htm, e.t. 13.04.2021

[66] Laura Brent, "NATO's Role in Cyberspace" https://www.nato.int/docu/review/articles/2019/02/12/natos-role-in-cyberspace/index.html, 13.04.2021

teknik konulara kıyasla, NATO`nun düşmanı caydırma amaçlı operasyonlarındaki eylemlerini daha da sınırlandırıyor. "Hukukun üstünlüğü, hükümetin hesap verebilirliği ve şeffaflığı"nı içeren bu ilkeler, yasal bileşene sıkı sıkıya bağlılık gerektirirken, otokratik rejimler ve devlet dışı aktörler, stratejik bir dengesizliğe yol açan göreceli özgürlük kazanırlar.[67]

NATO ülkeleri arasındaki belki de en göze batan çelişki, bazıları "yumuşak güvenlik" konularına odaklanırken, "sert" askeri misyonlar üstlenen diğer müttefikler arasındaki "iş bölümü"nden kaynaklanıyor. Bu nedenle, caydırıcılığa yönelik yaklaşımlardaki temel farklılık da sorunlu bir faktör olarak kabul edilebilir. ABD, Fransa, İngiltere ve Almanya gibi ülkeler bilgi güvenliğini askeri stratejiyle eşleştirdiğinde, askeri potansiyele sahip olmayan Estonya, sivil toplumun ve özel sektörün önemine vurgu yapmaktadır.[68]

Sonuç

Böylece, durumun bütünsel bir resmini oluşturmak için, NATO'nun geçtiği yolu üç aşamaya ayırmak gerekir. İlk aşamada siber güvenlik, teknik gelişmeler, siber saldırılara karşı ortak merkezlerin ve yapıların oluşturulması ve özellikle sanayi çevreleri arasındaki işbirliği aracılığıyla büyük ölçüde çözülmüş ve çözülmeye devam eden teknik bir sorun olarak algılanabilir. İkinci aşama, siber güvenliğin politik bir sorun haline gelmesi açısından burada önemlidir. Bu noktada Prag Zirvesi siber güvenlik konusunun gündeme gelmesinin resmi başlangıcı olarak bilinirken, 2007 yılında Estonya'ya yapılan siber saldırılar bu konuya öncelikli önem verilmesine neden olmuştur. Son olarak üçüncü aşama, siber güvenliğin stratejik önem kazanması ve gerekirse toplu savunma sözleşmesinin 5. Maddesinin etkinleştirilmesiyle tanımlanmaktadır.

NATO siber stratejisinin analizi, bir dizi sonuca varmayı mümkün kılıyor.

- ✓ Siber güvenlik sorunları NATO için giderek daha öncelikli hale geliyor.
- ✓ NATO, siber güvenlik vizyonunu doktrinsel bir şekilde formüle etmeye çalışıyor.
- ✓ NATO yalnızca siber güvenlik birleşeninin asker sayısını artırmakla kalmaz, aynı zamanda onları teknik olarak da destekler, tatbikatlar ve özel eğitim merkezleri kurarak birliklerin işlevsel kalitesini iyileştirir.
- ✓ Şimdiye kadar yapılan yasal normlar ve taahhütler, NATO'nun siber saldırılara mümkün olan en sert şekilde yanıt vermesine olanak tanır. Bu durumda nihai hedef, fiziksel saldırıların yanı sıra siber saldırı ve siber güvenlik yöntemlerini kullanarak düşmanın askeri yenilgisini sağlamak olarak tanımlanmaktadır.

Ancak NATO'nun siber uzay güvenliğini en üst düzeye çıkarma yeteneğini sınırlayan ve yine de onu çoklu siber saldırıların hedefi haline getiren bazı eksiklikler hala kalmaya devam etmektedir. Belki de bunların arasındaki en büyük eksiklik, ihlaline 5. Maddenin imasıyla eşlik edebilecek olan "Kırmızı Çizginin" olmamasıdır. Ayrıca, "Kırmızı Çizgi", düşmanı önceden siber suç işlemeyi reddetmeye ikna etmek için önleyici bir mekanizma olarak hizmet etmeli ve mümkün olduğunca sert olması gereken gerçek bir tehdit ve karşıt adımlarla takip edilmelidir. Her yıl NATO yapılarına yönelik artan sayıda siber saldırı, NATO politikasındaki bu eksikliklerin bir sonucu olarak gösterilebilir.

Siber saldırılar söz konusu olduğunda, saldırganın kimliğinin tespit edilememesi ve saldırganların kendi müdahalelerini inkâr etme ve diğerlerini suçlu olarak tanımlama eylemleri NATO'nun bu saldırılara karşılıklı bir şekilde

[67] Oliver Fitton, "Cyber Operations and Gray Zones: Challenges for NATO", Connections: The Quarterly Journal 15, no. 2, 2016, ss. 113-118.

[68] Казаковцев, a.g.e., s. 112.

tepki göstermesini kısıtlayan ana nedenlerden biri olarak algılanabilir.

Bir sonraki engel, siber güvenlikle ilgili, kabul edilebilir eylem kapsamını tanımlayabilecek uluslararası anlaşmaların olmamasıdır. Bu tür kısıtlayıcı önlemlerin yokluğu, saldırganların eylem aralığını genişletebilecek ve onlara siber uzayda geniş özgürlük verebilecek ana neden olarak tanımlanabilir. Ayrıca, büyük siber potansiyele sahip bazı ülkeleri bu tür anlaşmaları imzalamaya ikna etmek çok zordur çünkü çoğu durumda bu tür bir anlaşma onların çıkarlarıyla çelişir.

Son olarak, geleneksel silahlar ve siber silahların kombinasyonunun, gelecekteki çatışmalarda stratejik ve operasyonel eylem için temel oluşturmasının kuvvetle muhtemel olduğu unutulmamalıdır. NATO'nun siber uzaydaki bu tür boşlukları doldurması yalnızca siber saldırıların yol açabileceği zarar açısından değil, aynı zamanda dünyanın önde gelen askeri bloklarından biri olarak etkisini ve imajını sürdürmesi açısından da önemlidir.

Kaynakça

ADA Mehmet, ÇAKIR Hüseyin, "Kuzey Atlantik Antlaşma Örgütü'nün (NATO) Siber Güvenlik Stratejisinin İncelenmesi", *Düzce Üniversitesi Bilim ve Teknoloji Dergisi*, C. 5, S. 2, (2017), s. 634.

BAEZNER Marie, ROBİN Patrice, "Hotspot Analysis: Cyber and Information warfare in the Ukrainian conflict", Zürich, Center for Security Studies, Ekim (2018), s. 3.

BBC NEWS, "Putin: Russia helped Yanukovych to flee Ukraine", https://www.bbc.com/news/world-europe-29761799, e.t. 08.04.2021

BBC NEWS, "Ukraine protests after Yanukovych EU deal rejection", https://www.bbc.com/news/world-europe-25162563, e.t. 08.04.2021

BLANK Stephen, "Cyber War and Information War à la Russe", From Understanding Cyber Conflict: Fourteen Analogies, ed. George Perkovich and Ariel E. Levite, Published by Georgetown University Press November (2017), ss. 88-90.

BRENT Laura, "The Past, Present and Future aof Nato's Cyber Defence", The Three Swords Magazine (2020), s. 8.

CATON Jeffrey L., "Nato Cyberspace Capability: a Strategic and Operational Evolution", Strategic Studies Institute, US Army War College (2016), s. 5.

CCDCOE https://ccdcoe.org/about-us/, e.t. 13.04.2021

CORNİSH Paul vd., "On Cyber Warfare", Londra: Chatam House, Kasım 2010, s. 1.

COSTIGAN Sean S., HENNESSY Michael A., "Cybersecurity: A Genetic Reference Cirruculum", Kingston: National Defence Office of the Commander Military Personnel Generation, Ekim 2016, s. 15.

DEIBERT Ronald, ROHOZİNSKİ Rafal, "Liberation vs. Control: The Future of Cyberspace", Journal of Democracy, C. 21, S. 4, Ekim 2010, s. 45.

Encyclopedia, "Cybercpace" https://www.encyclopedia.com/science-and-technology/computers-and-electrical-engineering/computers-and-computing/cyberspace, e.t. 04.04.2021

FIDLER David P., PREGENT Richard, VANDURME Alex, "NATO, Cyber Defence, and International Law", St. John's Journal of Internatıonal & Comparatıve Law, C. 4, S. 1 (2016), s. 10.

GAZULA Mohan B., Cyber Warfare Conflict Analysis and Case Studies, (Yüksek Lisans Tezi), Massachusetts: Massachusetts Institute of Technology (2017), ss. 36-38.

GEERS Kenneth, "Cyberspace and the Changing Nature of Warfare", Tallinn: U.S.

Representative Cooperative Cyber Defence Centre of Excellence, t.y.,ss. 4-5.

GİBSON William, Neuromancer, 1. baskı, çev. Gonca Gülbey, İstambul: Altıkırkbeş Yayın, Şubat 2012.

GORDON Max, "Lessons from the Front:A Case Study of Russıan Cyber Warfare", Alabama: Maxwell Air Force Base, Aralık 2015, s. 12.

GOŹDZİEWİCZ Wiesław vd., "NATO Road to Cybersecurity", Krakow: The Kosciuszko Institute, (2016), s. 12.

HEALEY Jason, JORDAN Klara Tothova, "NATO's Cyber Capabilities: Yesterday, Today, and Tomorrow", *Washıngton: Atlantic Council*, Eylül 2014, s. 1.

HUGHES Rex B., "NATO and Cyber Defence. Mission Accomplished?", Amsterdam: Atlantisch Perspectief, 2009.

İnternational Telecommunication Union, "X-Series: Data Networks, Open System Communications and Security", Telecommunication Standardization Sector of ITU (2008), ss. 2-3.

KOVAL Nikolai, "Revolution Hacking," Cyber War in Perspective: Russian Aggression against Ukraine, ed. Kenneth Geers, Tallinn: NATO CCD COE (2015), ss. 55-58.

LAASME Häly, "Estonia: Cyber Window into the Future of NATO", Future of Defence, Washington: National Defense University Press, S. 63 (2011), s. 61.

BRENT Laura, "NATO's Role in Cyberspace" https://www.nato.int/docu/review/articles/2019/02/12/natos-role-in-cyberspace/index.html, e.t. 11.04.2021

Library of Congress. Congressional Research Service, "Defense Primer: Cyberspace Operations", 2020 https://crsreports.congress.gov/product/pdf/IF/IF10537/5, e.t. 04.04.2021

MARTIN C. Lıbıckı, Cyberdeterrence and Cyberwar, Santa Monika: RAND Corporation (2009), s. 11.

MELIKISHVILI Alexander, "The Cyber Dimension of Russia's Attack on Georgia", https://jamestown.org/program/the-cyber-dimension-of-russias-attack-on-georgia/, e.t. 07.04.2021

MINIATS Madelena Anna, "War of Nerves: Russia's Use of Cyber Warfare in Estonia, Georgia and Ukraine", Senior Projects Spring (2019), ss. 41-42.

NATO, "Brussels Summit Declaration" https://www.nato.int/cps/en/natohq/official_texts_156624.htm, e.t. 11.04.2021

NATO, "Bucharest Summit Declaration" https://www.nato.int/cps/en/natolive/official_texts_8443.htm, 10.04.2021

NATO, "Collective Defence - Article 5" https://www.nato.int/cps/en/natohq/topics_110496.htm#:~:text=NATO%20invoked%20Article%205%20for,of%20the%20Russia%2DUkraine%20crisis. e.t. 13.04.2021

NATO, "Cyber Defence" https://www.nato.int/cps/en/natohq/topics_78170.htm, e.t. 13.04.2021

NATO, "Lisbon Summit Declaration" https://www.nato.int/cps/en/natolive/official_texts_68828.htm, e.t. 10.04.2021

NATO, "London Declaration" https://www.nato.int/cps/en/natohq/official_texts_171584.htm, e.t. 11.04.2021

NATO, "NATO Network Enabled Capability (archived)" https://www.nato.int/cps/en/natolive/topics_54644.htm#:~:text=At%20the%20Prague%20Summit%20in,%2DEnabled%20Capabilities%20(NNEC), e.t. 10.04.2021

NATO, "Prague Summit Declaration" https://www.nato.int/cps/en/natohq/official_texts_19552.htm, e.t. 10.04.2021

NATO, "Riga Summit Declaration" https://www.nato.int/cps/en/natohq/official_texts_37920.htm?selectedLocale=en, e.t. 10.04.2021

NATO, "Riga Summit Declaration" https://www.nato.int/cps/en/natohq/official_texts_37920.htm?selectedLocale=en, e.t. 10.04.2021

NATO, "Wales Summit Declaration" https://www.nato.int/cps/en/natohq/official_texts_112964.htm, e.t. 10.04.2021

New York Times, "In Ukraine, a Malware Expert Who Could Blow the Whistle on Russian Hacking" https://www.nytimes.com/2017/08/16/world/europe/russia-ukraine-malware-hacking-witness.html, e.t. 08.04.2021

Oliver Fitton, "Cyber Operations and Gray Zones: Challenges for NATO", Connections: The Quarterly Journal 15, no. 2 (2016), ss. 113-118.

OTTİS Rain, "Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective," Proceedings of the 7th European Conference on Information Warfare and Security, ed. Day Remenyi, UK: Academic Conferences Limited (2008), ss. 164-168.

PERNİK Piret, "Improving Cyber Security: NATO and the EU", Tallinn: International Centre for Defence Studies, Eylül 2014, s. 4.

PERNİK Piret, "The early days of cyberattacks: the cases of Estonia, Georgia and Ukraine", European Union Institute for Security Studies (2018), ss. 61-62.

POLAT Doğan Şafak, "Nato'nun Yeni Operasyon Alanı: Siber Uzay", *Güvenlik* Bilimleri Dergisi, UGK Özel Sayısı, Şubat 2020, ss. 143-148.

RAND Corporation, "Cyber Warfare", https://www.rand.org/topics/cyber-warfare.html, e.t. 06.04.2021

The New York Times, "Before the Gunfire, Cyberattacks", https://www.nytimes.com/2008/08/13/technology/13cyber.html, e.t. 07.04.2021

VERTON Dan, "Serbs Launch Cyberattack on NATO", FWC, 04.04.1999 https://fcw.com/articles/1999/04/04/serbs-launch-cyberattack-on-nato.aspx, e.t. 07.04.2021

Vsenato, "Киберзащита НАТО" http://vsenato.ru/cyber-zashita-nato/, e.t. 11.04.2021

WEİTZ Richard, "Global Insights: Russia Refines Cyber Warfare Strategies", https://www.worldpoliticsreview.com/articles/4218/global-insights-russia-refines-cyber-warfare-strategies, e.t. 07.04.2021

WESTERBURGER Steffen, Cyber Conflict in the 21st Century The Future of War and Security in a Digitalizing World, (Yüksek Lisans Tezi), Radboud University, Aralık 2014, s. 74.

КАЗАКОВЦЕВ Алексей Васильевич, "Нато и Кибербезопасность", *Вестник Волгоградского государственного университета, Серия 4: История. Регионоведение. Международные отношения* (2012), ss. 110-112.

МАНОЙЛО Андрей Викторович, "Современные стратегии кибербезопасности и кибероборонь НАТО", Актуальные проблемы Европы (2020), ss. 172-173.

НИЛ Джон, "Сдерживание в условиях гибридной войны, Сухопутные силы США", Per Concordiam, C. 10, S. 1 (2020), ss. 21-23.

РЕВСКИЙ Александр, "Кибербезопасность - новый повод для коллективной обороны", Европейская безопасность: события, оценки, прогнозы, S. 35 (2014), s. 12.