Elektronik Sosyal Bilimler Dergisi
Electronic Journal of Social Sciences
Ocak/January(2025) - Cilt/Volume:24 - Sayı/Issue:1

www.esosder.org
e-ISSN:1304-0278
(1-20)

Uluslararası Güvenlikte Siber Tehditlerin Yükselişi ve Stratejik Savunma Politikaları

The Rise of Cyber Threats and Strategic Defence Policies in International Security

Gülşah ÖZDEMİR[1]

Öz

Bu çalışma, uluslararası güvenlik alanındaki siber tehditlerin karmaşık yapısını incelemekte ve bu tehditlerin küresel istikrar için temel bir endişe olarak hızlı yükselişini vurgulamayı amaçlamaktadır. İlk bölüm, siber tehditlerin evrimine ilişkin özlü bir genel bakış sunmakta, bu tehditlerin kökenlerini küçük dijital rahatsızlıklardan ulusal güvenliği baltalayabilen, kritik altyapıyı kesintiye uğratabilen ve jeopolitik dinamikleri etkileyebilen sofistike araçlara kadar izlemektedir. Bu bölüm, siber operasyonların casusluk ve sabotajın gölgelerinden ulusal savunma cephaneliklerinde ön saflardaki araçlara geçişini işaret eden önemli olayları öne çıkarmaktadır. İnceleme, bu tehditlerin çok yönlü doğasını, devlet destekli saldırılar, siber terörizm ve siber suç dahil olmak üzere, her biri uluslararası barış ve güvenliğe benzersiz zorluklar sunan alanları kapsamaktadır. Sonraki bölüm, artan siber tehdit manzarasına yanıt olarak uluslar ve uluslararası organlar tarafından formüle edilen stratejik savunma politikalarının kapsamlı bir özetini sunmaktadır. Ulusal siber güvenlik çerçevelerinin geliştirilmesinden adanmış siber komuta birimlerinin kurulmasına, Birleşmiş Milletler ve NATO gibi örgütlerin himayesinde uluslararası iş birlikleri ve norm belirleme çabalarına kadar benimsenen strateji spektrumu incelenmektedir. Tartışma, bu politikaların siber riskleri hafifletmede, direnci artırmada ve dijital çağda işbirlikçi bir uluslararası güvenlik ortamını teşvik etmede etkililiğini yansıtmaktadır. Uluslararası İlişkilerden teorik içgörüler ile siber olaylar ve politika yanıtları üzerine ampirik verilerin entegrasyonu yoluyla, çalışma, ulusal savunma önlemlerini uluslararası iş birliği zorunluluğu ile uyumlu hale getirmede ortaya çıkan eğilimleri ve gelecekteki zorlukları belirleyerek sonuçlanmakta ve siber sınırı etkili bir şekilde yönlendirmek için uyarlanabilir ve ileriye dönük politikalara duyulan ihtiyacı vurgulamaktadır.

Anahtar Kelimeler: Uluslararası Güvenlik, Siber Tehditler, Stratejik Savunma Politikaları

Abstract

This study aims to examine the complex nature of cyber threats in the field of international security and highlight their rapid emergence as a fundamental concern for global stability. The first section provides a concise overview of the evolution of cyber threats, tracing their origins from minor digital disruptions to sophisticated tools capable of undermining national security, disrupting critical infrastructure, and impacting geopolitical dynamics. This section highlights significant events marking the transition of cyber operations from the shadows of espionage and sabotage to forefront tools in national defense arsenals. The review encompasses the multifaceted nature of these threats, covering areas such as state-sponsored attacks, cyber terrorism, and cybercrime, each presenting unique challenges to international peace and security. The subsequent section presents a comprehensive summary of strategic defense policies formulated by nations and international bodies in response to the escalating cyber threat landscape. The spectrum of strategies adopted, ranging from the development of national cybersecurity frameworks to the establishment of dedicated cyber command units under the auspices of organizations like the United Nations and NATO, is examined. The discussion reflects on the effectiveness of these policies in mitigating cyber risks, enhancing resilience, and promoting a cooperative international security environment in the digital age. Through the integration of empirical data on cyber incidents and policy responses with theoretical insights from international relations, the article provides a nuanced understanding of how cyber threats have reshaped strategic thinking in global security. The study concludes by identifying trends and future challenges in aligning national defense measures with the imperative of international cooperation, emphasizing the need for adaptable and forward-looking policies to effectively navigate the cyber frontier.

Keywords: International Security, Cyber Threats, Strategic Defense Policies

1 Dr. Öğr. Üyesi, Balıkesir Üniversitesi, gulsah.ozdemir@balikesir.edu.tr, https://orcid.org/0000-0001-8900-2560, https://ror.org/02tv7db43

Makale Türü/Article Type: Araştırma Makalesi/Research Article
Geliş Tarihi/Received Date: 27.03.2024 – Kabul Tarihi/Accepted Date: 30.10.2024
Atıf İçin/For Cite: Özdemir G., "Uluslararası Güvenlikte Siber Tehditlerin Yükselişi ve Stratejik Savunma Politikaları", Elektronik Sosyal Bilimler Dergisi, 2025;24(1):1-20
https://doi.org/10.17755/esosder.1459973

Giriş

Uluslararası ilişkilerin çağdaş manzarasında, siber alan, jeopolitik gerilimlerin ve çatışmaların giderek açığa çıktığı kritik bir alan olarak ortaya çıkmıştır. Siber alanın uluslararası güvenliğin kritik bir unsuru olarak evrimi, internetin ortaya çıkışına ve ardından dijital teknolojilerin yayılmasına kadar izlenebilir. Başlangıçta iletişim ve bilgi paylaşımı aracı olarak tasarlanan internet, dünya çapında ekonomik, siyasi ve sosyal sistemlerin temelini oluşturan karmaşık bir altyapıya dönüşmüştür (Nye, 2010: 22). Bu dönüşüm, ulusal altyapıların giderek dijitalleşmesiyle paralel olarak gerçekleşmiş ve bunlar siber tehditlere karşı savunmasız hale gelmiştir (Clarke ve Knake, 2019: 219). Siber uzayın savaşın beşinci alanı olarak tanınması, uluslararası güvenliğin kavramsallaştırılmasında önemli bir değişimi işaret etmektedir (Klimburg, 2017: 23-24). Siber tehditler, geleneksel çatışma ve savaş kavramlarını aşarak çağdaş jeopolitik gerilimlerde merkezi bir unsur haline gelmiştir. Devletler ve devlet dışı aktörler, siber uzayı casusluk faaliyetleri, etki operasyonları, kritik altyapıyı bozmak ve bilgi savaşı yürütmek için kullanmaktadırlar, böylece barış ve çatışma arasındaki çizgileri bulandırmaktadırlar (Rid, 2013: 5-8). 2007'de Estonya'ya yapılan siber saldırılar ve İran'ın nükleer programına karşı Stuxnet operasyonu, siber yeteneklerin jeopolitik hedeflere ulaşmak için stratejik olarak nasıl kullanıldığını gösteren önemli örneklerdir (Farwell ve Rohozinski, 2011: 36). Bu olaylar, siber teknolojilerin çift kullanım niteliğini vurgulamakta, ekonomik kalkınmayı desteklemenin yanı sıra ulusal güvenliği de tehlikeye atabileceklerini ortaya koymaktadır (Gercke, 2012: 80; NATO, 2016). Sonuç olarak, siber tehditlerin ortaya çıkması, geleneksel güvenlik paradigmalarının yeniden değerlendirilmesini ve siber alan için özel olarak tasarlanmış stratejik savunma politikalarının oluşturulmasını gerektirmiştir (Segal, 2016; Tikk vd., 2010: 12).

Bu çalışma, ABD, Çin, Rusya ve Avrupa Birliği gibi büyük güçlerin ulusal siber güvenlik stratejilerine odaklanmakta ve bu ülkelerin siber tehditlere karşı nasıl yanıt verdiklerini incelemektedir. Anahtar küresel aktörler ve uluslararası kuruluşlar tarafından benimsenen stratejik savunma politikalarının ayrıntılı bir şekilde incelenmesi ile bu araştırma, siber tehditleri azaltmaya ve siber alanda dayanıklılığı artırmaya yönelik kolektif çabaları aydınlatmayı amaçlamaktadır. Bu analiz, siber suçlarla mücadelede uluslararası anlaşmaların, örneğin Siber Suçlar Üzerine Budapeşte Sözleşmesi'nin ve Birleşmiş Milletler ile NATO gibi uluslararası örgütlerin öncülük ettiği girişimlerin rolünü de inceleyecektir.

1. Literatür

Siber tehditlerin yükselişi ve stratejik savunma politikalarının oluşturulması, Uluslararası İlişkiler (UI) alanındaki uluslararası güvenlik tartışmalarında merkezi konular haline gelmiştir. Bu literatür incelemesi, siber teknolojideki önemli gelişmeleri, siber güvenlikle ilgili teorik çerçeveleri, siber tehditlerin etkisi üzerine mevcut araştırmaları ve literatürdeki boşlukları, özellikle ortaya çıkan tehditler ve savunma stratejileri konusundaki eksiklikleri keşfetmektedir.

Siber teknolojinin tarihsel evrimi ve erken dönem siber tehdit örnekleri, siber güvenlik alanındaki mevcut manzarayı anlamak için temel oluşturur. İnternetin öncüsü olan ARPANET'ten küresel dijital altyapıya geçiş, potansiyel siber tehditler için saldırı yüzeyini genişletmiştir (Abbate, 1999). 1988 Morris Worm gibi erken örnekler, kötü amaçlı siber faaliyetlerin neden olduğu yaygın bozulmanın potansiyelini göstermiştir (Shemakov, 2019). Siber tehditlerin evrimi o zamandan beri hızlanmış olup, 2007'deki Estonya siber saldırıları ve 2010'daki Stuxnet solucanı gibi önemli olaylar, ulusal altyapıların siber operasyonlara karşı savunmasızlığını vurgulamaktadır (Farwell ve Rohozinski, 2011: 35-36 ; Singer, 2015: 79).

Uluslararası İlişkiler dahilindeki çeşitli teorik çerçeveler, siber güvenlik dinamikleri hakkında içgörüler sağlar. Geleneksel olarak nükleer stratejiye uygulanan caydırıcılık teorisi, siber tehditleri ele almak için adapte edilmiş olup, siber uzaydaki tespit sorunlarına ve misilleme tehditlerinin inandırıcılığına odaklanmaktadır. Nye'nin (2010) tartıştığı siber güç kavramı, devletlerin dijital yeteneklerini stratejik hedeflerine ulaşmak için nasıl kullandığını araştırmakta ve siber uzayda sert ve yumuşak gücün önemini vurgulamaktadır. Uluslararası İlişkiler'deki köşe taşı kavramlarından biri olan güvenlik ikilemi, siber alanında da önemli bir yere sahiptir. Devletler siber savunmalarını ve saldırgan yeteneklerini geliştirdikçe, artan güvensizlik ve tırmanma potansiyeli ortaya çıkabilir, bu da geleneksel güvenlik ikilemlerini yansıtabilir (Rid ve Buchanan, 2015: 4-6). Bu teorik bakış açıları, dijital dünyada güvenliği sağlamanın karmaşıklıklarını vurgular.

Siber tehditler üzerine mevcut araştırmalar, bunların ulusal ve uluslararası güvenlik mimarilerine olan etkilerini kapsamlı bir şekilde belgelemiştir. Çalışmalar, siber tehditlerin devlet egemenliğini nasıl zayıflatabileceğini, kritik altyapıyı nasıl bozabileceğini ve jeopolitik dinamikleri nasıl etkileyebileceğini incelemiştir (Lin, 2016: 86-88). Hackerlar ve terörist örgütler de dahil olmak üzere devlet dışı aktörlerin, siber yetenekleri kötü amaçlar için nasıl kullandığı araştırmaların odak noktalarından biri olmuş ve güvenlik düşüncelerinin kapsamını devletler arası çatışmanın ötesine genişletmiştir (Denning, 2011: 170-173). Stratejik savunma politikaları üzerine yapılan araştırmalar, devletlerin ve uluslararası örgütlerin benimsediği çeşitlilikteki yaklaşımları vurgulamıştır. Budapeşte Siber Suçlar Sözleşmesi gibi girişimler ve NATO'nun siber savunma politikaları, siber tehditlere karşı normatif çerçeveler ve işbirlikçi savunma mekanizmaları oluşturma çabalarını yansıtmaktadır (Gercke, 2012, 84; NATO, 2016). Bununla birlikte, bu politikaların etkinliği ve siber uzayda uluslararası işbirliğinin zorlukları hala devam eden tartışma konularıdır. Mevcut literatür, siber tehditler ve savunma politikaları konusunda temel bir anlayış sağlasa da, özellikle ortaya çıkan siber tehditler ve yenilikçi savunma stratejileri konusunda boşluklar mevcuttur. Yapay zekâ ve kuantum hesaplama gibi siber teknolojinin hızlı evrimi, mevcut araştırmalarda yeterince ele alınmayan yeni zayıflıkları ortaya koymaktadır. Ayrıca, literatür genellikle ulusal güvenlik mimarilerinin siber tehditlere karşı dayanıklılığını etkileyen insan faktörleri ve kurumsal kültür gibi sosyo-teknik boyutları göz ardı etmektedir (Valeriano ve Maness, 2018: 17-18). Siber tehditlerin dinamik doğası, savunma stratejilerinin sürekli olarak uyarlanmasını gerektirir. Ancak, devletlerin ve uluslararası örgütlerin nasıl yenilik yapabileceklerini ve politikalarını etkin bir şekilde nasıl geliştirebileceklerini araştıran çalışmalarda bir kıtlık bulunmaktadır. Ayrıca, siber tehditlerin diğer savaş alanlarıyla, örneğin bilgi ve psikolojik operasyonlarla kesiştiği nokta, kapsamlı güvenlik stratejileri geliştirmek için daha fazla keşif gerektirir (Farwell ve Rohozinski, 2011: 23-25).

Netice itibariyle, uluslararası güvenlikte siber tehditler ve stratejik savunma politikalarıyla ilgili literatür değerli içgörüler sağlamakla birlikte önemli boşlukları da ortaya koymaktadır. Bu boşlukların ele alınması, özellikle ortaya çıkan tehditlerin bağlamında ve yenilikçi savunma stratejilerinin geliştirilmesinde, siber tehditlerin evrilen manzarası karşısında ulusal ve uluslararası güvenlik mimarilerinin direncini artırmak için hayati öneme sahiptir.

2. Siber tehditlerin anlaşılması ve sınıflandırılması

Dijital çağ, siber tehditlerin uluslararası güvenlikte merkezi bir endişe haline gelmesiyle yeni bir çatışma ve rekabet dönemini başlatmıştır. Küresel bağlantı ve bilgi teknolojilerine olan bağımlılık arttıkça, siber alandaki tehditlerin karmaşıklığı da artmaktadır. Siber tehditler

artık uluslararası ilişkilerde önemli bir rol oynamakta, diplomasiyi, askeri stratejiyi ve ulusal güvenliği etkilemektedir.

Devlet sponsorluğundaki siber tehditler: Devlet destekli siber operasyonlar sıklıkla dijital alandaki ulusal çıkarların karmaşık etkileşimini yansıtan çeşitli siyasi, askeri ve ekonomik hedefler tarafından yönlendirilir. Bu çok yönlü operasyonlar, hassas ve gizli bilgilerin edinilmesine yönelik casusluk, ulusal güvenliği destekleyen kritik altyapının kasıtlı sabotajı ve kamuoyunu etkilemek veya hedef ülkelerdeki yerleşik siyasi süreçleri bozmak için tasarlanmış etki kampanyalarının uygulanması dahil ancak bunlarla sınırlı olmamak üzere çok çeşitli faaliyetleri kapsayabilir. Devlet aktörlerinin bu siber operasyonlara katılımı, öncelikle operasyonel etkinliklerini ve stratejik erişimlerini önemli ölçüde artıran geniş kaynaklar ve sofistike yetenekler nedeniyle ek bir karmaşıklık katmanı ortaya çıkarır. Devlet destekli siber tehditler genellikle karmaşık doğaları ve gelişmiş operasyonel yeteneklerini vurgulayan sofistike tekniklerin uygulanması ile karakterize edilmektedir. Bu tür tehditler tipik olarak önemli finansal kaynaklarla desteklenir ve stratejik hedeflerini gerçekleştirmek için bir dizi son teknoloji araç ve metodoloji kullanabilirler (Sujayraj, 2019: 290).

Terörist siber tehditler: Siber terörizm, devlet dışı aktörlerin ideolojik, dini veya siyasi hedeflere ulaşmak için hükümetleri ve sivilleri korkutmak veya zorlamak için siber araçları kullanmasıyla ilgilidir. Siber terörizm, kapsamlı siber güvenlik stratejileri ve topluluklarda farkındalık artırma çabalarını gerektiren siber suçlar ve siber saldırılar da dahil olmak üzere daha geniş bir siber tehdit yelpazesinin bir parçasıdır. Kimlik hırsızlığı, finansal dolandırıcılık ve veri ihlalleri gibi faaliyetleri içeren siber suçlar gibi diğer siber tehdit türleri ile kıyaslandığında daha az sıklıkla gerçekleşse de, teröristlerin kritik altyapıya zarar verme veya çevrimiçi propaganda yayarak zarar verme potansiyeli ciddi bir güvenlik endişesidir.(Wagas, 2024,1-5)

Hacktivist siber tehditler: Hacktivizm, sosyal veya politik bir amaç için hacklemeyi içerir ve hedefler genellikle hükümet, kurumsal ve diğer kuruluşların web siteleri ve ağlarıdır. Hacktivizm, siber terörizm, spam, web sitesi parodileri, memler, kültür sıkışması ve e-posta bombalaması gibi faaliyetleri içerir. Bu eylemler genellikle fiziksel alanlardan ziyade sanal alanı işgal eden sanal oturma eylemleri gibi sivil itaatsizliğin elektronik biçimlerini içerir. (Romagna, 2024:744) Her zaman teknik olarak karmaşık olmasa da, hacktivist saldırıları hizmetleri kesintiye uğratabilir ve kamuya dikkat çekerek nedenlerini vurgulayabilir, bu da hukuk dışı çevrimiçi faaliyetler ile özgür konuşma kesişimine ilişkin soruları gündeme getirir.

3. Önemli siber saldırılara ilişkin ana vaka çalışmaları

Stuxnet worm: Stuxnet'in 2010'da keşfi, İran'ın nükleer programını hedef alarak stratejik hedeflere geleneksel olarak kinetik askeri eylemlerle takip edilen önemli fiziksel hasarlara neden olarak siber savaşta bir dönüm noktası olarak işaret etti. Bu sofistike siber silah, ABD ve İsrail tarafından geliştirildiğine inanılan, siber saldırıların stratejik hedeflere ulaşma potansiyelini göstermiştir (Karnouskos, 2011: 4490-4494).

DNC hack ve etki operasyonları: Rus devlet destekli aktörlere atfedilen 2016 siber saldırıları, Demokrat Ulusal Komitesi'ni (DNC) hedef alarak e-postaların çalınması ve stratejik olarak sızdırılmasıyla ABD başkanlık seçimlerini etkilemeyi amaçladı. Bu durum, siber casusluğun ve bilgi savaşlarının kesişimini vurguladı ve demokratik süreçlerin bütünlüğü için derin etkilere sahipti.

NotPetya saldırısı: 2017'de, NotPetya kötü amaçlı yazılımı başlangıçta Ukrayna'yı hedef alsa da hızla küresel olarak yayılarak çok uluslu şirketlere milyarlarca dolar zarar verdi. Bir

fidye saldırısı olarak çerçevelendirilmesine rağmen, yaygın yıkıcı etkisi ve Rus devlet destekli aktörlere atfedilmesi, jeopolitik bir motivasyona işaret etti ve siber suç ve devlet destekli siber saldırı arasındaki çizgiyi bulanıklaştırdı (Buchanan, 2020: 102).

4. Devlet dışı aktörlerin rolü ve atfetme zorluğu

Teröristler, siber suçlular ve hacktivistler gibi çeşitli varlıkları kapsayan devlet dışı aktörler, siber uzayın doğasında bulunan dağıtılmış ve anonim özelliklerden yararlanarak kendilerini uluslararası ilişkiler alanında giderek daha önemli oyuncular olarak belirlemişlerdir. Çeşitli faaliyetleri, halihazırda karmaşık olan uluslararası güvenlik ortamına karmaşık bir komplikasyon katmanı getiriyor, çünkü yüksek derecede cezasızlıkla faaliyet gösterme yeteneğine sahip oldukları ve genellikle ani yansımalarla karşılaşmadan ulusal sınırları aşma yeteneğine sahip oldukları göz önüne alındığında. Ayrıca, siber saldırıların belirli bireylere veya gruplara doğru bir şekilde atfedilmesiyle ilgili zorluklar durumu daha da kötüleştiriyor, çünkü belirli aktörleri belirli siber olaylara kesin olarak bağlayan kesin kanıtlar elde etmek sıklıkla göz korkutucu bir görev olduğunu kanıtlıyor, dolayısıyla ulus-devletlerin uygun bir yanıt formüle etme veya uluslararası hukukun yerleşik çerçevesi içinde herhangi bir misilleme biçimini düşünme yeteneğini karmaşıklaştırmaktadır.

Devlet dışı aktörlerin uyguladığı etki, geleneksel jeopolitik sınırların sınırlarının çok ötesine uzanır ve böylece hem ulusal güvenliği hem de karmaşık uluslararası ilişkiler ağını önemli ölçüde etkiler. Bu aktörler, siber tehditleri düzenlemekten küresel politika oluşturmaya katılmaya kadar uzanan sayısız faaliyette bulunurlar ve bu, çağdaş güvenlik paradigmalarını şekillendirmede kritik ve giderek daha önemli rollerini toplu olarak vurgulamaktadır (Luitel, 2024: 58). Siber tehditleri belirli aktörlere atfetme süreci, etkili yanıtları daha da engelleyen çok sayıda teknik ve yasal zorlukla doludur. İnternetin doğal anonimliği, siber aktörlerin kimliklerini gizlemek için kullandıkları gelişmiş tekniklerle birleştiğinde, saldırıların kökenlerini gerçek kaynaklarına kadar izleme görevini son derece zorlu ve karmaşık hale getirmektedir (Jolley, 2019: 62).

Siber operasyonların devlet aktörlerine atfedilmesini çevreleyen tartışmalarda sıklıkla başvurulan etkili kontrol ilkesi, belirli bir devletin devlet dışı bir aktörü aktif olarak yönlendirdiğini veya kontrol ettiğini belirlemek genellikle komplikasyonlar ve belirsizliklerle dolu olduğundan, kendi yasal ve teknik engeller sunmaktadır (Delerue, 2019: 235). Siber tehditlerin atfedilmesinin yarattığı önemli zorluklara rağmen, bu çok yönlü sorunları gelişmiş uluslararası iş birliği ve yenilikçi yasal çerçevelerin geliştirilmesi yoluyla ele almayı amaçlayan devam eden ve uyumlu çabalar vardır. Genellikle devlet ve devlet dışı aktörler arasında dinamik bir etkileşimi içeren siber operasyonların doğal karmaşıklığı, bu ortaya çıkan zorluklarla etkin bir şekilde başa çıkmak için teknik, yasal ve politik boyutları bütünleştiren kapsamlı ve çok yönlü bir yaklaşım gerektirir. Uluslararası toplum bu acil konularda gezinmeye ve bunlarla boğuşmaya devam ederken, devlet dışı aktörlerin rolü, atfedilmenin sürekli zorluğuyla birlikte, şüphesiz siber güvenlik ve uluslararası hukukun evrimi ile ilgili devam eden tartışmaların merkezinde olmaya devam edecektir.

5. Siber güvenlikte stratejik savunma politikaları

Siber tehditlere karşı etkili savunma politikalarının geliştirilmesi, teknik, hukuki ve diplomatik stratejileri bir araya getiren çok yönlü bir yaklaşım gerektirir. Uluslararası işbirliği ve bilgi paylaşımı kritiktir, ayrıca siber alanda sorumlu devlet davranışı için normlar ve

anlaşmaların geliştirilmesi de önemlidir. Ayrıca, kritik altyapıyı korumak ve genel siber direnci artırmak için kamu-özel ortaklıkların güçlendirilmesi esastır.

Siber tehditler uluslararası güvenliğe önemli ve giderek artan bir tehdit oluşturmakta, etkilerini hafifletmek için kapsamlı ve uyarlanabilir stratejilere ihtiyaç duymaktadır. Bu tehditlerin taksonomisini anlamak ve geçmiş siber olaylardan ders çıkarmak, etkili savunma politikalarının geliştirilmesi için hayati öneme sahiptir. Dahası, devlet dışı aktörlerin rolünü ele almak ve atfetme zorluğunu aşmak, istikrarlı ve güvenli bir siber alan kurmak için zorunludur. Siber alanın evrimi devam ettikçe, tehditlerine karşı savunma stratejileri değişmek zorundadır ve bu da uluslararası paydaşlar arasında sürekli işbirliği ve yenilik gerektirir (Singer, ve Friedman, 2014: 144).

5.1. Stratejik savunma politikaları ve uluslararası işbirliği

Siber tehditlerin yaygınlaşması, küresel güvenliği korumak için güçlü stratejik savunma politikaları ve uluslararası iş birliğinin gerekliliğini ortaya koymuştur. Dijital çağda siber güvenlik, ulusal ve uluslararası güvenliğin temel taşı haline gelmiştir. Siber tehditlerin yükselişi, geleneksel savunma paradigmalarını zorlamakta ve ulusları ve uluslararası kuruluşları siber savunma için stratejik politikalar ve çerçeveler geliştirmeye teşvik etmektedir.

5.1.1. Amerika Birleşik Devletleri

Amerika Birleşik Devletleri, siber savaş ve siber saldırıların yarattığı artan tehditleri ele almak için kapsamlı ve gelişen bir dizi siber savunma politikası geliştirdi. Bu politikalar, her biri kendi odak noktasını ve stratejilerini masaya getiren çeşitli yönetimler tarafından şekillendirilmiştir. ABD'nin siber savunma politikaları, ulusal altyapıyı korumayı, uluslararası işbirliğini geliştirmeyi ve hızla değişen teknolojik manzaraya uyum sağlamayı amaçlamaktadır.

Amerika Birleşik Devletleri, kamu-özel ortaklıkları vurgulayan, siber olaylara müdahale yeteneklerini artıran ve uluslararası iş birliğini teşvik eden kapsamlı siber güvenlik stratejileri belirlemiştir. Cybersecurity and Infrastructure Security Agency (CISA) gibi girişimler, kritik altyapıyı savunma ve ulusal siber direnci artırma taahhüdünü örneklemektedir (Cybersecurity, U. S., 2021).

Amerika Birleşik Devletleri, Ulusal Altyapı Koruma Planı (NIPP) ve Ulusal Standartlar ve Teknoloji Enstitüsü (NIST) Siber Güvenlik Çerçevesi dahil olmak üzere kritik ulusal altyapıyı korumayı amaçlayan bir dizi çerçeve ve girişim başlatmıştır. Bu girişimler, enerji, ulaşım ve finans gibi sektörlerin siber tehditlere karşı dayanıklılığını artırmak için hükümet organları, düzenleyici kuruluşlar ve özel işletmeler arasındaki işbirliğini kapsamaktadır (Adegbite vd, 2023: 202-203).

5.1.2. Çin

Çin'in siber güvenliğe yaklaşımı, siber egemenliği ve uluslararası işbirliğini vurgulayan ekonomik, politik ve yasal boyutları bütünleştiren kapsamlı bir strateji ile karakterize edilir. Bu yaklaşım, Çin'in benzersiz siyasi ve ekonomik bağlamı ve siber bir süper güç olma istekleri tarafından şekillenmektedir. Çin'in siber güvenlik stratejisinin merkezinde, devletlerin kendi sınırları içinde siber alanı yönetme hakkını öne süren siber egemenlik kavramı yer almaktadır. Bu yaklaşım, Batılı ülkelerin tercih ettiği daha açık, çok paydaşlı modellerle tezat oluşturmaktadır. (Zu ve Chen, 2022:193). Ayrıca Çin, siber güvenliği yönetmek için internet içeriği ve altyapısı üzerinde sıkı kontrol içeren sağlam bir düzenleyici çerçeve geliştirmiştir. Çin Siber Uzay İdaresi (CAC) bu politikaların uygulanmasında çok önemli bir rol oynamaktadır. (Creemers, 2023:180)

Çin'in siber güvenlik yaklaşımı, kritik bilgi altyapısını korumaya ve siber uzay egemenliğini ileri sürmeye odaklanan 2017 Siber Güvenlik Kanunu gibi sıkı düzenleyici çerçevelerle karakterizedir. Çin'in stratejisi, siber savunmayı ulusal kalkınma ve güvenlik hedefleriyle entegre etmeyi vurgular. (Cybersecurity Law of the People's Republic of China, 2017).

Çin'in siber güvenlik stratejisi kapsamlı ve proaktif olsa da, devlet kontrolünü inovasyonla dengelemek ve özellikle ABD ile uluslararası gerilimleri yönetmek gibi zorluklarla karşı karşıyadır. Çin'in yaklaşımının küresel etkileri önemlidir, çünkü siber egemenlik ve devlet liderliğindeki yönetişim üzerindeki vurgusu uluslararası siber normları ve politikaları etkilemektedir.

5.1.3. Rusya

Rusya siber güvenliği, siber uzaydaki artan tehditler ve jeopolitik manzaranın yönlendirdiği ulusal güvenlik çerçevesinde değerlendirmektedir. Bu algı, ülkenin rejim güvenliğini, kamu güvenliğini ve toplumsal normları korumak için tasarlanmış siber güvenlik konusundaki stratejik, yasal ve operasyonel yaklaşımlarına yansımaktadır.

Rusya, siber güvenliği ulusal güvenlik açısından ayrılmaz bir parça olarak algılamakta, kritik devlet bilgi kaynaklarını korumaya odaklanmaktadır. Rus stratejisi, yerel teknolojik yetenekler geliştirmeyi ve siber casusluğa ve sabotaja karşı devletin tepki verme yeteneğini artırmayı içerir.

Rusya, siber güvenlik zorluklarını ele almak için karmaşık bir yasal ve düzenleyici çerçeve geliştirmiştir. Bu çerçeve, bilgi teknolojilerini düzenleyen ve siber alan alanında ulusal çıkarları korumayı amaçlayan 149-FZ sayılı Federal Yasayı kapsamaktadır. Ülke, küresel siber güvenlik ölçütleri oluşturmak için çok paydaşlı diplomasiye katılarak uluslararası siber güvenlik normlarının formülasyonuna aktif olarak katılmıştır. Bununla birlikte, Rusya, dijital egemenlik kavramının altını çizerek İnternet yönetimi için devlet merkezli bir paradigmayı tercih etmektedir (Andrey, 2023: 171). Rusya'nın 2017-2030 bilgi güvenliği stratejisinde tanımlanan stratejik hedefler, ulusal güvenliği desteklemek için bilgi ve iletişim teknolojilerini çeşitli sektörlerde entegre etmenin gerekliliğini vurgulamaktadır (Stepanova, 2024:98).

5.2. Uluslararası Örgütlerin Siber Savunma Çabalarını Koordine Etmedeki Rolü

Uluslararası kuruluşlar, ulusal sınırları aşan siber tehditlerin doğasında bulunan sınırsız ve çoğu zaman öngörülemeyen özellikler ışığında özellikle önemli olan siber savunma girişimlerini organize etmenin karmaşık sürecinde vazgeçilmez bir işlev üstlenirler ve bu nedenle çeşitli aktörler arasında ortak bir çaba gerektirir. Bu saygın kuruluşlar, yalnızca evrensel olarak kabul edilen norm ve standartların oluşturulmasını kolaylaştırmakla kalmaz, aynı zamanda kritik bilgi ve uzmanlık alışverişini geliştirirken, aynı zamanda çeşitli ülkeler arasında yeteneklerin gelişimini teşvik ederek daha sağlam bir küresel siber savunma duruşu sağlar. Bu tür kuruluşlar tarafından üstlenilen çabalar, doğası gereği ulusötesi olan siber tehditleri etkili bir şekilde ele almak için uyumlu ve birleşik bir küresel strateji formüle etmede hayati önem taşır ve sonuç olarak, birden fazla paydaşın güçlü yönlerinden yararlanan işbirlikçi bir yaklaşım gerektirir. Sonuç olarak, sürekli gelişen bir siber ortamın yarattığı riskleri azaltmak için gerekli olan bir uluslararası işbirliği ortamını teşvik etmek için temel olduğundan, rollerinin önemi abartılamaz.

5.2.1 Birleşmiş Milletler (BM)

Birleşmiş Milletler'in siber savunma alanındaki katılımı çok yönlüdür. Yasal çerçevelerin oluşturulması, uluslararası işbirliğinin teşvik edilmesi ve Dijital Mavi Miğferlerin girişimi gibi çabaları kapsar. Bununla birlikte, mevcut jeopolitik gerilimlerin yanı sıra evrensel olarak kabul edilen bir yasal aracın olmaması önemli zorluklar ortaya çıkarmaktadır.

Evrensel bir yasal çerçevenin yokluğuna atfedilen kademeli ilerleme hızına rağmen, BM, siber suçla mücadele için uluslararası işbirliğini ilerletmede çok önemli bir rol oynamıştır. Siber suçu ele almayı amaçlayan yeni bir yasal aracın kurulmasını çevreleyen devam eden tartışmalar, devletler arası işbirliğini güçlendirmeye çalıştıkları için esastır (Walker ve Tennant, 2023: 72). Siber suçu yöneten kapsamlı bir uluslararası yasal çerçevenin eksikliği, devletler arasındaki koordinasyonu zorlaştırıyor. Bununla birlikte, BM'nin uzman grupları oluşturma ve bölgesel örgütleri destekleme girişimleri, uyumlu bir uluslararası hukuk sisteminin kurulması yolunda olumlu bir ilerleme anlamına gelmektedir.

BM Hükümet Uzmanları Grubu (GGE), uluslararası siber normların formülasyonunda kayda değer ilerlemeler kaydetti, ancak bu normların operasyonelleştirilmesi zorluklar yaratmaya devam ediyor. GGE'nin çabaları, işbirliği stratejileri ve normatif çerçeveler üzerinde anlaşmayı teşvik etmek için hayati öneme sahiptir (Pauletto, 2020: 361). BM tarafından tanıtılan Dijital Mavi Kasklar (DBH) girişimi, siber huzuru korumak için yeni bir metodoloji anlamına geliyor. Hala başlangıç aşamasındayken, DBH, geleneksel barışı koruma operasyonlarına benzer şekilde siber alanı denetlemeyi hedefliyor. Siber tehditlerin tespiti için BM Global Pulse gibi projelerle işbirliği (Nabeel, 2020) (Akatyev ve James, 2017) potansiyelinin altını çiziyor.

BM, siber güvenlik konusunda uluslararası diyalog ve işbirliğini teşvik etmede kilit bir rol oynamaktadır ve uluslararası güvenlik bağlamında ICT'ler alanındaki gelişmeleri değerlendirmek için Hükümetlerarası Uzmanlar Grubu (GGE) ve Açık Sonlu Çalışma Grubu (OEWG) gibi platformlar aracılığıyla çok taraflı tartışmaları kolaylaştırmaktadır. BM'nin siber güvenlik konusundaki katılımı, siber suçtan siber savaşa kadar çeşitli endişeleri ele alan bir dizi komite ve uzman kuruluşu kapsar. Bununla birlikte, bu organların karmaşıklığı, entegre eylemleri kolaylaştırmak için gelişmiş diyalog ve iletişim gerektirir (Henderson, 2015:468).

5.2.2 Kuzey Atlantik Antlaşması Örgütü (NATO)

NATO'nun siber savunma çabalarını koordine etmedeki rolü çok yönlüdür ve stratejik, operasyonel ve işbirlikçi boyutları içerir. Siber tehditler gelişmeye devam ederken, NATO siber alanı kara, deniz ve hava gibi askeri operasyonlar için kritik bir alan olarak giderek daha fazla kabul ediyor. Bu tanınma, üye devletler arasında kolektif siber savunmayı geliştirmek için kapsamlı stratejiler ve çerçevelerin geliştirilmesine yol açmıştır.

NATO, siber saldırıların üye ülkelerin kritik altyapıları üzerindeki potansiyel etkisini kabul ederek siber savunmayı temel kolektif savunma misyonuna entegre etmiştir (Ferenț ve Preja, 2023: 190). Bu entegrasyon, NATO'nun bir üyeye yönelik saldırıyı herkese saldırı olarak değerlendiren ve bu ilkeyi siber tehditlere genişleten 5. Madde taahhüdünün bir parçasıdır.

İttifak, siber alanı askeri operasyonlar için bir alan ilan etmek de dahil olmak üzere siber güvensizliği ele almak için kurumsal mekanizmalar ve doktrinler geliştirmiştir (Burton, 2023:310). Bu stratejik çerçeve siber saldırıları caydırmayı ve üye devletlerin dayanıklılığını artırmayı amaçlamaktadır.

NATO, siber uzayı bir operasyon alanı olarak tanımış olup siber savunma duruşunu güçlendirmeyi ve üye devletlerin siber güvenliklerini desteklemeyi taahhüt etmiştir. NATO'nun Cyber Defence Pledge ve Cooperative Cyber Defence Centre of Excellence (CCDCOE) gibi girişimleri, NATO'nun siber tehditlere karşı proaktif tutumunu vurgulamaktadır (Cybersecurity, 2018).

5.2.3 Avrupa Birliği (AB)

Avrupa Birliği (AB) siber savunma çabalarını koordine etmede, kurumsal yeteneklerinden yararlanmada ve üye devletler ve uluslararası ortaklar arasında işbirliğini teşvik etmede çok önemli bir rol oynamaktadır. Bu koordinasyon, birleşik ve stratejik bir yaklaşım gerektiren siber tehditlerin karmaşık ve gelişen doğasını ele almak için gereklidir. AB'nin çabaları kapsamlı bir siber güvenlik politikası çerçevesi, uluslararası işbirliği ve dayanıklılık ve dijital egemenliğe odaklanma ile karakterizedir.

AB'nin üye devletler arasında siber savunmayı koordine etme çabaları, düzenleyici önlemleri, kapasite oluşturma girişimlerini ve ENISA gibi kuruluşlar aracılığıyla işbirliğini teşvik etmeyi içermektedir. AB'nin Dijital Onyıl için Siber Güvenlik Stratejisi, kolektif direnç, teknolojik egemenlik ve siber güvenlikte liderlik vizyonunu belirlemektedir (ENISA, 2020).

AB, 1990'ların sonlarından bu yana önemli ölçüde gelişen sağlam bir siber güvenlik politikası çerçevesi geliştirmiştir. Bu çerçeve, bir Avrupa uyarı ve bilgi sisteminin kurulmasını, siber güvenlik teknolojilerine yatırım yapmayı ve ortak siber güvenlik standartlarının oluşturulmasını içermektedir (Muzhanova v.d., 2024: 135-136).

AB'nin siber güvenlik stratejileri, özellikle 2013, 2017 ve 2020'deki stratejiler, siber dayanıklılığı artırmayı, siber tehditlere etkili yanıt vermeyi ve güvenli ve açık bir küresel siber alanı teşvik etmeyi amaçlamaktadır (Renda, 2022: 490).

AB'nin 2020-2025 stratejisi, siber tehditlere karşı dayanıklılığı güçlendirmeye ve vatandaşlar ve işletmeler için güvenilir dijital hizmetler sağlamaya odaklanmaktadır. Bu, siber güvenliği desteklemek için düzenleyici, yatırım ve politika araçlarını içermektedir.

5.3 Siber güvenliği artırmayı amaçlayan uluslararası anlaşmalar, normlar ve düzenlemelerin analizi

Siber güvenliği geliştirmek için tasarlanmış uluslararası anlaşmalar, standartlar ve düzenlemeler, siber tehditlerin karmaşık ve sınırsız doğasını ele almak için gereklidir. Bu girişimler, küresel siber güvenlik yönetimi için tutarlı bir çerçeve oluşturmak için anlaşmaların, yerleşik yasaların ve işbirlikçi paydaş stratejilerinin bir karışımını kapsar.

Siber güvenlik için uluslararası anlaşmaların ve standartların formüle edilmesindeki kayda değer ilerlemelere rağmen, sayısız zorluk devam ediyor. Teknolojinin hızlı ilerlemesi ve çelişen ulusal öncelikler, uyumlu bir çerçevenin arayışını engelliyor. Bununla birlikte, işbirlikçi paydaş yönetimi potansiyeli ve mevcut yasal mekanizmaların uyarlanması, küresel siber güvenliğin geliştirilmesi için cesaret verici yollar sunmaktadır. Uluslararası toplum bu zorluklarla yüzleşmeye devam ederken, güvenli ve esnek bir siber alanı teşvik etmek için hem devlet hem de devlet dışı kuruluşları içeren kapsamlı bir yaklaşım gerekli olacaktır.

5.3.1. Budapeşte siber suçlarla mücadele sözleşmesi

Avrupa Konseyi tarafından öncülük edilen Budapeşte Sözleşmesi, siber suçlarla etkili bir şekilde mücadele etmek için işbirliğini kolaylaştıran ve ulusal yasaları uyumlaştıran en önemli uluslararası antlaşmalardan biri olarak kalmaktadır (Council of Europe. 2001).

Avrupa Konseyi tarafından kurulan Budapeşte Siber Suç Sözleşmesi, siber suçla ilgili karmaşıklıklarla yüzleşmek için tasarlanmış çığır açan uluslararası bir anlaşmayı temsil ediyor. Ulusal mevzuatın senkronizasyonu, araştırma etkinliğinin artırılması ve küresel işbirliğinin teşvik edilmesi için kapsamlı bir çerçeve sunar. Önemine rağmen, Sözleşme, teknolojik gelişmelere uyum sağlamadaki yetersizlikleri ve mahremiyet ve sivil özgürlükler üzerindeki yansımaları konusunda eleştiriye maruz kalmaktadır.

Sözleşme, yetkisiz erişim, veri manipülasyonu ve bilgisayarla ilgili dolandırıcılık dahil olmak üzere belirli siber suç eylemlerini tanımlayarak ulusal mevzuatları birleştirmeyi amaçlamaktadır. Bu standardizasyon, çeşitli yargı bölgelerinde siber suçu ele almak için tutarlı bir yasal metodoloji oluşturmak için gereklidir (Archick, 2005: 3-4). Model, başlı başına bir yasa değil, ulusların farklı siber suç sorunlarını ele almak için mevzuatlarını değiştirmelerine olanak tanıyan ve böylece teknolojik evrime uyum sağlamak için gerekli esnekliği sağlayan bir çerçeve oluşturmaktadır (Clough, 2012: 363). Sözleşmenin göze çarpan bir yönü, karşılıklı yardımı ve imzacı ülkeler arasında bilgi alışverişini teşvik eden uluslararası işbirliğine odaklanmasıdır. Siber suçun ulusötesi karakteri göz önüne alındığında, bu ortaklık çok önemlidir. Sözleşme, yerel girişimler için bir ölçüt görevi görür ve siber suçlarla mücadeleyi amaçlayan çeşitli uluslararası, bölgesel ve ulusal projelerle desteklenmektedir (Clough, 2014: 378).

Budapeşte Sözleşmesi siber suçla mücadelede çok önemli bir araç olmaya devam etse de, etkinliği ulusal güvenlik, siyasi dinamikler ve kamusal algı gibi çok sayıda yasal olmayan husus tarafından şekillendirilmektedir. Sözleşmenin uygulanması yalnızca yasal uygulanabilirliğine değil, aynı zamanda ulusların hükümlerini benimseme ve değiştirme taahhüdüne de dayanır. Küresel topluluk siber suçun değişen çerçevesiyle ısrarla mücadele ederken, kapasite geliştirmeye ve daha kapsamlı uluslararası anlaşmaların formüle edilmesine artan bir vurgu mevcuttur.

5.3.2. Tallinn el kitabı

Siber Savaşa Uygulanabilir Uluslararası Hukuk Tallinn El Kitabı, mevcut uluslararası yasal çerçevelerin siber operasyonlarla ilişkisini inceleyen kapsamlı bir kaynak olarak hizmet vermektedir. NATO Kooperatif Siber Savunma Mükemmeliyet Merkezi'nin himayesinde uluslararası hukuk akademisyenlerinden oluşan bir meclis tarafından hazırlanan bu El Kitabı, geleneksel uluslararası hukuku hızla değişen siber savaş ortamına uygulamanın karmaşık zorluklarını araştırarak devletler ve hukuk uygulayıcıları için içgörüler ve öneriler sunar.

Tallinn El Kitabı, siber "saldırıların" yorumlanmasına ve bunları yöneten düzenleyici çerçevelere odaklanarak uluslararası insancıl hukukun (IHL) siber operasyonlara uygulanması için bir çerçeve oluşturur. Siber faaliyetlerin stratejik önemini kabul ederken sivil nüfusu korumayı amaçlayan müsamahakâr ve kısıtlayıcı perspektifleri uzlaştırmayı amaçlayan yeni bir yaklaşım getirilmiştir (Schmitt, 2014:12-18). El kitabının savaşın gerekçesiyle ilgili analizi, siber operasyonlarda tehditlerin veya gücün yasaklanmasını kapsar, kendini savunma parametrelerini tanımlar ve atıf ve müdahaleyle ilgili sorunları ele alır. Bu ilkelerin siber saldırılarla, özellikle devlet dışı aktörleri içeren siber saldırılarla nasıl ilişkili olduğunu titizlikle değerlendirir.

Ayrıca, yönergeler, siber operasyonlarda devlet hesap verebilirliğinin karmaşıklığıyla mücadele ediyor ve siber tehditlerle ilişkili doğal "ilişkilendirme asimetrisinden" kaynaklanan ilişkilendirmenin zorluklarını vurgulamaktadır. Devlet desteğiyle özel kuruluşlar tarafından yürütülen siber faaliyetler için devletlerin hesap verebilirliğini artırmak için bir "sanal kontrol" testini savunur (Margulies, 2013:496).

5.3.3. BM GGE ve OEWG önerileri

Uluslararası hukukun siber savaşa uygulanabilirliği, özellikle Birleşmiş Milletler Hükümet Uzmanları Grubu (BM GGE) ve Açık Uçlu Çalışma Grubu (OEWG) çerçevesinde yoğun bir tartışma ve analiz konusu olmuştur. Bu tartışmalar, BM Şartı ve uluslararası insancıl hukuk gibi mevcut uluslararası yasaların, siber operasyonların yarattığı benzersiz zorlukları ele almak için nasıl yorumlanabileceğine veya uyarlanabileceğine odaklanmaktadır. BM GGE ve OEWG, siber uzayda sorumlu devlet davranışının bir dizi gönüllü, bağlayıcı olmayan normunu önermiş, uluslararası hukukun siber faaliyetlere uygulanabilirliğini vurgulamış ve siber tehditleri önleme ve yanıtlama konusunda işbirliği gerekliliğine işaret etmiştir (United Nations General Assembly, 2015).

5.3.4. Paris'te siber uzayda güven ve güvenlik için çağrı

Paris Barış Forumu'nda başlatılan çağrı, güvenli ve istikrarlı bir siber uzayı teşvik etmek için çok paydaşlı bir girişimi temsil eder ve bireyleri ve altyapıyı koruma, seçim süreçlerini savunma ve dijital ekonominin bütünlüğünü sağlama gibi prensipleri savunur (Paris Peace Forum, 2018). Siber tehditlerin yükselişi, siber savunmaları güçlendirmek ve siber güvenlik için işbirlikçi çerçeveler oluşturmak için ulusal ve uluslararası çabaları harekete geçirmiştir. Önde gelen siber güçlerin stratejik politikaları, uluslararası örgütlerin koordinasyon rolleri ve uluslararası anlaşmaların, normların ve düzenlemelerin geliştirilmesi, siber uzayı güvence altına almak için kolektif bir çabanın altını çizer. Siber tehditlerin evrimine devam etmesiyle, uyumlu stratejiler ve artan uluslararası işbirliği gerekliliği giderek daha açık hale gelmekte, siber güvenlik politikası ve uygulamalarında sürdürülebilir katılım ve yenilik gerekmektedir (Cybersecurity, 2018).

6. Teknolojik ilerlemeler ve siber savunma

Teknolojinin hızlı evrimi, siber güvenlik alanını önemli ölçüde etkileyerek hem yenilikçi savunma mekanizmaları sunmakta hem de yeni zayıflıklar ortaya çıkarmaktadır. Dijital çağda, siber tehditlerin artması ulusal ve uluslararası güvenliğe kritik bir meydan okuma oluşturmaktadır. Yapay zekâ, makine öğrenimi ve kuantum hesaplama gibi yeni teknolojiler, siber savunma mekanizmalarını güçlendirmede kilit bir rol oynamıştır. Ancak, bu teknolojiler aynı zamanda yeni zayıflıklar ve etik sorunlar da ortaya çıkarmaktadır. Yükselen teknolojilerin siber savunma yeteneklerini artırmadaki rolüne, sunmuş olduğu zorluklara ve fırsatlara bu bölümde yer verilmektedir.

Yapay zeka ve makine öğrenimi: Yapay zeka ve makine öğrenimi, tehdit tespiti ve yanıt süreçlerinin otomatikleştirilmesini sağlayarak siber savunma stratejilerini dönüştürmüştür. Bu teknolojiler, siber tehditlere işaret eden desenleri ve anormallikleri belirlemek için geniş veri kümelerini analiz edebilir, erken tespit ve önlemeyi kolaylaştırır. Yapay zekâ destekli sistemler, evrilen tehditlere uyum sağlayabilir, sürekli olarak yeni verilerden öğrenerek öngörü yeteneklerini artırabilirler (Taddeo ve Floridi, 2018: 296-298).

Kuantum hesaplama: Kuantum hesaplama, bilgi işleme hızını eşi benzeri görülmemiş hızlarda gerçekleştirebilmesiyle siber savunmayı devrimleştirmeyi vaat etmektedir. Bu yetenek, veri şifreleme yöntemlerini önemli ölçüde geliştirerek, verilerin siber saldırılara karşı daha sağlam bir şekilde şifrelenmesini sağlayabilir. Ancak, kuantum hesaplamanın mevcut kriptografik standartlara da bir tehdit oluşturduğu, bu nedenle kuantum dirençli algoritmaların geliştirilmesini gerektirdiği unutulmamalıdır (Mosca, 2018: 38-39).

Siber güvenlikte teknolojik ilerlemelerin sunmuş olduğu zorluklar şu şekilde belirtilebilir:

Etik ve gizlilik endişeleri: Yapay zekâ ve makine öğreniminin siber savunmada kullanılması, önemli etik ve gizlilik endişelerini gündeme getirmektedir. Bu teknolojilerin etkinliği için gereken verilerin toplanması ve analizi, bireysel gizlilik haklarının ihlal riski taşımaktadır. Bu endişeleri ele almak için etik kuralların belirlenmesi ve yapay zekâ operasyonlarında şeffaflığın sağlanması son derece önemlidir (Taylor vd., 2016).

Yapay zeka sistemlerinin bağımlılığı ve güvenliği: Siber savunmada yapay zeka ve makine öğrenimine olan bağımlılık, bu sistemlerin kendilerinin karmaşık siber saldırıların hedefi haline gelme riskini beraberinde getirmektedir. Yapay zeka tabanlı savunma mekanizmalarının güvenliği ve bütünlüğünün sağlanması, kötü niyetli aktörler tarafından sömürülmesini önlemek için büyük önem taşımaktadır (Brundage vd., 2018).

Kriptografiye karşı kuantum tehdidi: Kuantum hesaplamanın siber güvenliği artırma potansiyeli taşıdığına rağmen, aynı zamanda geleneksel kriptografik yöntemlere ciddi bir tehdit oluşturur. Kuantum hesaplamanın ortaya çıkması, mevcut şifreleme tekniklerini işlevsiz hale getirebilir ve güvenli iletişim ve veri korumasına yönelik bir zorluk oluşturabilir (Proakis, 2008: 840).

Siber güvenlikte teknolojik ilerlemeler tarafından sunulan fırsatlar ise şunlardır:

Geliştirilmiş tehdit istihbaratı ve öngörü analitiği: Yapay zekâ ve makine öğrenimi, daha sofistike tehdit istihbaratı yetenekleri sunarak potansiyel siber tehditlere yönelik öngörülere imkân tanır. Bu proaktif yaklaşım, kuruluşların ortaya çıkan tehditlere daha etkili bir şekilde hazırlanmasına ve yanıt vermesine olanak sağlar (Taddeo ve Floridi, 2018: 299).

Kriptografi alanındaki gelişmeler: Kuantum hesaplama ve diğer teknolojik ilerlemeler, daha gelişmiş kriptografik teknikler geliştirme fırsatı sunar, bu da kuantum anahtar dağıtımı (QKD) gibi teorik olarak çözülmez şifreleme sağlayabilir ve veri güvenliğini önemli ölçüde artırabilir (Satyanarayanan, 2017: 30-34).

Siber güvenliğin demokratikleştirilmesi: Yükselen teknolojiler, daha gelişmiş araç ve tekniklerin daha geniş bir oyuncu yelpazesine, bunlar arasında daha küçük ülkeler ve kuruluşlar da dahil olmak üzere erişilebilir hale gelmesiyle siber güvenliği demokratikleştirebilir, böylece siber savunmada oyun alanını eşitleyebilir (Mittelstadt, 2019). Yapay zekâ, makine öğrenimi ve kuantum hesaplama gibi teknolojik ilerlemeler, siber güvenlik alanında çift yönlü bir kılıç sunar. Bu teknolojiler siber savunma yeteneklerini artırmak için önemli potansiyel sunarken, aynı zamanda yeni zayıflıklar ve etik ikilemler de ortaya çıkarabilir (Mosca, 2018: 41-43; Chesterman, 2020: 821-823). Siber güvenliğin geleceği, bu ilerlemelerin faydalarını kullanırken, etik kurallar, güvenli geliştirme uygulamaları ve uluslararası işbirliği yoluyla risklerini azaltmaktadır. Dijital peyzajın evrimine devam etmesiyle, teknoloji ve siber güvenlik arasındaki etkileşim, uluslararası ilişkiler alanındaki araştırmacılar, politika yapıcılar ve uygulayıcılar için önemli bir endişe ve fırsat alanı olarak kalacaktır (Apruzzese vd., 2023: 158-160).

7. Zorluklar ve gelecek yönelimler

Siber tehditlerin dinamik doğası, uluslararası güvenlik alanında stratejik savunma politikalarının oluşturulması ve uygulanmasına önemli zorluklar getirmektedir. Siber savunma önlemlerinin uygulanmasıyla birlikte ortaya çıkan yasal, etik ve gizlilik hususları derinlemesine tartışılması gereken konular olarak karşımıza çıkmaktadır. Bu hususta öncelikle siber tehditlerin gelecekteki eğilimlerini öngörerek, bunların uluslararası güvenlik politikası ve işbirliğinin etkilerine odaklanılması gerekmektedir. Dijital çağda, siber güvenlik, uluslararası ilişkilerde kritik bir endişe olarak ortaya çıkmıştır; siber tehditlerin yaygınlaşması, geleneksel güvenlik ve savunma anlayışlarını sorgulamaktadır. Siber tehditlerin hızlı evrimi, eşit derecede dinamik ve adapte olabilir stratejik savunma politikalarını gerektirmektedir.

7.1.1. Yükselen siber tehditlerin karakterizasyonu

Siber tehditler, zayıflıkları sömürmek için gelişmiş teknolojileri ve taktikleri kullanan giderek sofistike hale gelmiştir. Devlet destekli siber faaliyetlerin artışı, siber suç örgütleri ve siber operasyonların jeopolitik kaldıraç için kullanılması, çağdaş siber tehditlerin çok yönlü doğasını örneklemektedir (Kello, 2017: 119; Nye, 2010: 25).

Stratejik savunma politikalarında uyumluluk

Etkili bir siber savunma, politika oluşturma ve uygulamada çeviklik gerektirir; bu da gerçek zamanlı tehdit istihbaratını dahil etmek, kamu-özel ortaklıkları geliştirmek ve kritik altyapının direncini sağlamak anlamına gelir. Savunma stratejilerinin uyum sağlayabilmesi, siber tehditlerin hızla evrildiği hızlı tempoya karşı etkili bir karşı önlem alınması için kritiktir (Rid, ve Buchanan, 2015: 122; Healey, 2012).

Siber savunmada hukuki, etik ve gizlilik düşünceleri

Hukuki çerçeveler ve uluslararası normlar: Siber savunma stratejilerinin geliştirilmesi ve uygulanması, siber alandaki kabul edilebilir davranışları belirlemeyi amaçlayan hukuki çerçeveler ve uluslararası normlar tarafından sınırlıdır. Siber normlar konusunda fikir birliği olmaması ve siber saldırıları atfetmenin zorluğu, hukuki manzarayı karmaşıklaştırmaktadır (Tikk vd., 2010: 103; Schmitt, 2013:56-58).

Etik ve gizlilik etkileri: Siber savunma önlemleri, özellikle gözetim ve veri toplama içerenler, etik ve gizlilik endişelerini gündeme getirir. Ulusal güvenlik çıkarlarını bireysel haklarla dengelemek kritik bir zorluk olup, şeffaf ve sorumlu siber savunma uygulamalarını gerektirir (Floridi ve Taddeo, 2016; Lucas, 2017:158-159).

Uluslararası güvenlik politikası ve işbirliği için sonuçlar: Siber tehditlerin değişen doğası, güçlü uluslararası güvenlik politikaları ve devletler, uluslararası kuruluşlar ve özel sektör arasındaki işbirliğinin artırılması gerekliliğini vurgular. Siber normlar konusunda fikir birliği sağlanması ve işbirlikçi siber savunma girişimlerinin teşvik edilmesi, güvenli bir siber alan için zorunludur (Nye, 2016: 44-47).

Siber tehditlerin dinamik ve karmaşık doğası, hukuki, etik ve gizlilik düşüncelerini göz önünde bulunduran, uyarlanabilir ve incelikli stratejik savunma politikalarının gerekli olduğunu ortaya koymaktadır. Dijital manzara, teknolojik ilerlemelerin etkisiyle devam ettiği sürece, uluslararası güvenlik politikaları da siber alanın sunduğu zorlukları ele almak ve fırsatları değerlendirmek için ilerlemelidir. Güçlendirilmiş uluslararası işbirliği ve ortak normlar ve prensiplerin geliştirilmesi, güvenli ve istikrarlı bir siber alanın sağlanması için kritiktir ve siber tehditlere karşı küresel topluluğun kolektif sorumluluğunu yansıtmaktadır (Segal, 2016).

8. Tartışma

Uluslararası arenadaki siber tehditlerin artışı, stratejik savunma politikalarının yeniden değerlendirilmesini gerektirmiştir ve bu, uluslararası güvenlik manzarasında kilit bir değişimi işaret eder. Bu tartışma, mevcut siber tehditlere karşı stratejik savunma politikalarının analizinden elde edilen bulguları sentezler, bunların etkinliğini ve sınırlarını değerlendirir ve bu tehditlerin uluslararası ilişkilere yönelik teorik sonuçlarını araştırır.

8.1 Analiz bulgularının bütünleştirilmesi

8.1.1. Mevcut stratejik savunma politikalarının etkinliği

Analiz, ülkelerin siber tehditleri hafifletmek için teknolojik, hukuki ve diplomatik stratejilerin bir kombinasyonunu benimseyerek çok yönlü bir yaklaşım sergilediğini ortaya koymaktadır. Bu stratejilerin etkinliği, devletlerin siber olayları tespit etme, caydırma ve yanıtlama kapasitesinde artış olarak belirgindir. Örneğin, gelişmiş siber güvenlik teknolojilerinin ve tehdit istihbaratı sistemlerinin uygulanması, devletlerin siber tehditleri proaktif bir şekilde tanımlama ve etkisiz hale getirme yeteneğini önemli ölçüde artırmıştır (Nye, 2016: 68).

Ayrıca, ulusal ve uluslararası düzeyde hukuki çerçevelerin ve politikaların geliştirilmesi, siber alandaki kabul edilebilir davranışları tanımlamada kritik bir rol oynamış ve siber savunma alanında daha organize ve işbirlikçi bir yaklaşıma katkıda bulunmuştur (Tikk vd., 2010: 104). NATO ve BM gibi organizasyonların çabalarıyla görülen uluslararası işbirliği, en iyi uygulamaların, kaynakların ve istihbaratın paylaşılmasını kolaylaştırarak siber tehditlere karşı kolektif savunma mekanizmalarını güçlendirmiştir (Valeriano ve Maness, 2018:129).

8.1.2. Mevcut stratejik savunma politikalarının sınırlılıkları

Bu ilerlemelere rağmen, birçok sınırlılık devam etmektedir. Siber tehditlerin dinamik ve değişken doğası, mevcut savunma politikaları için önemli bir zorluk oluşturmakta ve genellikle hızlı teknolojik ilerlemeler ve siber rakipler tarafından kullanılan yenilikçi taktiklerle başa çıkmada zorlanmaktadır (Lin, 2017: 520-522). Atıf sorunu, siber alanın anonimliği nedeniyle faili tanımlamayı ve sorumluları hesap vermeye zorlamayı zorlaştırarak misilleme önlemlerinin oluşturulmasını ve uygulanmasını karmaşıklaştıran kritik bir engel olarak kalır (Buchanan, 2016, 123).

Dahası, dijital altyapıya dayanma, enerji, finans ve sağlık gibi kritik sektörlerin siber saldırılarla önemli ölçüde etkilenme riski taşıyan içsel zayıflıklar yaratmaktadır. Uluslararası toplum, siber alanı yöneten normlar ve düzenlemeler konusunda fikir birliğine varmada zorluklarla karşılaşmakta olup, bu durum dijital alandaki egemenlik, özgürlük ve güvenlik konularındaki farklı ulusal çıkarları ve perspektifleri yansıtmaktadır (Klimburg, 2017: 357).

8.2. Uluslararası ilişkilerde teorik sonuçlar

Siber tehditlerin uluslararası güvenlikte merkezi bir endişe olarak ortaya çıkması, Uluslararası İlişkiler alanı için önemli teorik sonuçlar doğurmaktadır. Bir realizm perspektifinden bakıldığında, siber tehditler uluslararası sistemin anarşik doğasını vurgulamakta ve devletlerin başlıca endişesinin hayatta kalma ve güç biriktirme olduğunu göstermektedir. Siber alan, devletlerin güvenliklerini ve etkilerini artırmak amacıyla siber casusluk, sabotaj ve savaşta yer aldığı yeni bir alan haline gelmiştir (Mearsheimer, 2014: 82).

Öte yandan, liberal teoriler, siber tehditlerle başa çıkmada işbirliği ve kurum oluşturmanın potansiyelini vurgular. Siber uzayın bağlantılı doğası, karşılıklı güvenliği sağlamak için işbirliği

çabalarını gerektirir ve siber uzayda normların ve işbirliğinin geliştirilmesinde uluslararası rejimlerin, anlaşmaların ve kuruluşların önemini gösterir (Keohane ve Nye, 1998: 84-85).

Yapısalcı yaklaşımlar, normların, kimliklerin ve fikirlerin devlet davranışını siber uzayda şekillendirmedeki rolünü vurgular. Sorumlu devlet davranışı, siber caydırıcılık ve uluslararası hukukun siber uzayda uygulanabilirliği etrafında normların geliştirilmesi, siber tehditlerin ve yanıtların sosyal yapılandırmasını yansıtır ve devletlerin bu zorlukları nasıl algıladığı ve bunlarla nasıl başa çıktığı üzerinde etki yapar (Wendt, 1992: 391-395).

Siber tehditlerin yükselişi, uluslararası güvenlik ve uluslararası sistemde devlet davranışını ve etkileşimleri anlamaya çalışan teorik çerçeveler için derin sonuçlar doğurmaktadır. Mevcut stratejik savunma politikalarının belirli alanlarda etkili olduğunu göstermesine rağmen, devam eden uyum ve yenilik gerektiren önemli sınırlılıklarla karşı karşıyadır. Uluslararası ilişkilerdeki siber tehditlerin teorik sonuçları, siber uzayın çatışma ve işbirliği alanı olarak karmaşıklığını vurgular ve teknoloji, siyaset ve hukuk arasındaki etkileşimin incelikli bir anlayışını gerektirir. Siber tehditlerin ortaya çıkardığı zorlukların üstesinden gelmek, dijital alandaki etkileşimlerin kapsamlı bir anlayışıyla bilgilendirilen uluslararası toplumun birleşik çabalarını gerektirecektir.

9. Genel Değerlendirme

Siber tehditlerin ortaya çıkışı, uluslararası güvenliği çevreleyen manzarayı ve savunma politikası formülasyonunun karmaşık süreçlerini tartışmasız bir şekilde değiştirdi, böylece hem ayırt edici zorluklar hem de küresel topluluğun bir bütün olarak gezinmesi için umut verici fırsatlar sunmaktadır. Kapsamlı soruşturma, siber tehditlerin çok yönlü ve karmaşık doğasının altını çizerek, yalnızca ulusal güvenliği değil, aynı zamanda on yıllardır kurulan uluslararası güvenlik çerçevelerini de baltalama ve tehlikeye atma potansiyellerini vurgulamıştır. Siber tehditlerin doğal anonimlikleri, hızlı yürütülmeleri ve geleneksel coğrafi sınırlara açık bir şekilde göz ardı edilmesiyle karakterize edildiğini kabul etmek önemli olsa da, bu tehditlerin uzun süredir güvenilen mevcut stratejik savunma çerçevelerinin etkinliği önünde önemli engeller oluşturduğunu kabul etmek de aynı derecede önemlidir. Siber savunmaya yönelik mevcut yaklaşımların etkinliği, siber tehditlerin hızlı evrimi, saldırıların faillerine atfedilmesindeki karmaşıklıklar ve modern toplumların bağlı olduğu dijital altyapıya doğal olarak bulunan güvenlik açıkları tarafından sıklıkla engellenmektedir.

Siber tehditlerle ilgili ulaşılan bu bulguların sonuçları sadece teknik düşüncelerin çok ötesine uzanmakla birlikte, jeopolitik etkileşimleri, uluslararası yasal çerçevelerin evrimini ve karmaşık bir dünyada düzeni ve istikrarı korumayı amaçlayan küresel yönetişim yapılarını önemli ölçüde etkilemektedir. Hızla gelişen bu ortamda, siber uzay, devletlerin ulusal çıkarlarını ve hedeflerini korumaya çalışırken casusluk, sabotaj ve bilgi savaşı dahil olmak üzere çeşitli faaliyetlerde bulundukları yeni bir güç ilişkileri alanı olarak ortaya çıkmıştır. Bu gerçeklik, endişe verici bir oranda çoğalmaya devam eden siber tehditlerin dinamik ve çok yönlü doğasına etkili bir şekilde karşı koymak için tasarlanmış tutarlı ve öngörücü savunma stratejilerinin formüle edilmesi için acil gerekliliğin altını çiziyor.

Uluslararası işbirliğini teşvik etmek ve savunma çerçevelerini geliştirmek için öneriler açısından, bu yaygın siber tehditlere sağlam bir yanıt sağlamak için birkaç kritik adım atılmalıdır. İlk olarak, tehdit istihbaratının, en iyi uygulamaların ve teknolojik çözümlerin yayılmasını kolaylaştırmak ve devletler ile özel sektör arasındaki boşluğu işbirlikçi bir şekilde kapatmak için daha dayanıklı ve sofistike platformların oluşturulması zorunludur. Bu tür işbirlikçi çabalar, ilgili tüm paydaşlar arasında güven ve karşılıklılık ortamını teşvik etmek için açık protokollerin

yönetimini de denetlemesi gereken uluslararası kuruluşlar tarafından aktif olarak teşvik edilmeli ve kolaylaştırılmalıdır.

Ayrıca, siber tehditlerin yarattığı acil zorlukların üstesinden gelmek için siber uzayda devlet davranışını yöneten uluslararası normları formüle etme ve kodlama çabaları hızlandırılmalıdır. Bu çaba, mevcut uluslararası hukukun siber alan içindeki uygunluğunu netleştirmeyi ve bu alanda ortaya çıkan çatışmalarla yüzleşirken bir fikir birliği duygusunu teşvik etmeyi amaçlayan siber diplomasi alanını kapsar. Ek olarak, teknolojik açıdan az gelişmiş ülkelerin siber savunma yeteneklerini güçlendirmeyi amaçlayan girişimler gecikmeden uygulanmalıdır. Bu, dijital uçurumu kapatmaya ve tüm uluslar için daha adil bir küresel güvenlik ortamını teşvik etmeye yardımcı olmak için gerekli teknik yardım, kapsamlı eğitim ve gerekli kaynakları sağlamayı gerektirebilir.

Devlet kurumları ve özel sektör kuruluşları arasındaki ortaklıklar, özel işletmelerin siber güvenlik ortamında oynadığı kritik rolden yararlanmak için önemli ölçüde genişletilmelidir. Bu işbirlikleri stratejik olarak kritik altyapının dayanıklılığını artırmaya, siber savunma teknolojilerinde yeniliği teşvik etmeye ve ulusal ve uluslararası güvenliğe tehdit oluşturan siber olaylara hızlı ve etkili yanıtlar sağlamaya yönelik olmalıdır. Son olarak, siber güveni artırmayı amaçlayan önlemler, siber uzayda ortaya çıkabilecek tırmanma ve çatışma risklerini azaltmak için düşünceli bir şekilde tasarlanmalı ve sistematik olarak uygulanmalıdır. Bu, kriz iletişim mekanizmalarının kurulmasını, devletler arasında genellikle "yardım hatları" olarak adlandırılan doğrudan iletişim kanallarının oluşturulmasını ve giderek daha tartışmalı olan bu alanda istikrar ve barışı sağlamak için siber yeteneklerin kullanımını yöneten karşılıklı kısıtlama anlaşmalarını içerebilir.

İleriye dönük araştırma yollarıyla ilgili olarak, hızla ilerleyen siber tehditler alanı, bu çok yönlü konuların yetkin bir şekilde anlaşılmasını geliştirmek ve bunları zamanında etkin bir şekilde ele almak için gerekli olan sürekli araştırma ve incelemeyi gerektirir. Siber caydırıcılık kavramı ile ilgili olarak, siber uzay bağlamında uygulanabilen çeşitli caydırıcılık çerçevelerinin fizibilitesini ve genel etkinliğini sistematik olarak araştırmak ve aynı zamanda siber tehditlerin benzersiz özelliklerini ve ilgili zorlukları göz önünde bulundurmak, tespit edilebilirliğin inceliklerini ve kullanılabilecek misilleme mekanizmalarını belirgin bir şekilde içeren ilgili zorlukları da dikkate almak büyük önem taşıyacaktır. Ayrıca, hem siber güvenlik önlemlerini hem de uluslararası ilişkileri önemli ölçüde etkileme potansiyeline sahip yapay zeka, kuantum hesaplama ve blok zinciri gibi ileri teknolojilerin ortaya çıkmasıyla ilgili sonuçların kapsamlı bir değerlendirmesini yapmak çok önemlidir ve bu dönüştürücü teknolojilerin oluşturduğu potansiyel risklerin ve siber savunmayı proaktif bir şekilde güçlendirmek için yarattıkları fırsatların işbirlikçi bir değerlendirmesini gerektirir.

Siber normların ve yönetişimin oluşturulması söz konusu olduğunda, dijital alandaki davranışa rehberlik etmek için çok önemli olan uluslararası siber normların formülasyonu, benimsenmesi ve pratik uygulamasında yer alan süreçlere odaklanan kapsamlı araştırmalara acil bir ihtiyaç vardır. Bu araştırma hattı, bu tür normların yaratıldığı karmaşık süreçleri, çeşitli paydaşların bu standartları şekillendirmede oynadığı önemli rolü ve bu yerleşik normların giderek karmaşıklaşan siber alan arenasında devletlerin davranışı ve davranışları üzerindeki daha geniş etkilerini araştırabilir. Siber çatışma ve uluslararası hukukun kesişimi ile ilgili olarak, genellikle belirsizlik ve belirsizlik ile karakterize edilen siber çatışmaların yarattığı zorluklara uluslararası hukukun geleneksel ilkelerinin uygulanmasında ortaya çıkan sayısız karmaşıklığı ele almak zorunludur. Bu inceleme, gezinilmesi gereken zorlu eşiklerin, sürdürülmesi gereken orantılılık

ve ayrımcılık ilkelerinin ve genellikle benzersiz zorluklar ve düşünceler sunan farklı siber uzay bağlamında geleneksel insan hukukunun genel uygunluğunun kapsamlı bir incelemesini içerir.

Siber güvenliğin sosyo-politik boyutları, araştırma çerçevesinin siber güvenlikle iç içe olan sosyo-politik yönleri kapsayacak şekilde genişletilmesini ve böylece siber tehditler ile gizlilik, insan hakları ve sosyal adalet gibi kritik konular arasındaki dinamik etkileşimleri araştırmayı gerektirir. Bu, çeşitli siber operasyonların sivil nüfus üzerindeki etkilerinin kapsamlı bir analizini ve siber uzayın karmaşık ve genellikle belirsiz manzarası içindeki devlet eylemlerinin etik sonuçlarını içerir.

Siber tehditlerin artan yaygınlığı ve tırmanması, uluslararası güvenlik ve ilgili politika yanıtlarının oluşturulması için çok önemli bir kavşak anlamına gelir ve bu zorlukları titizlikle ve kararlılıkla ele almanın aciliyetini vurgulamaktadır. Bu çok yönlü tehditlerin etkili bir şekilde üstesinden gelmek, teknoloji, politika ve hukuk arasında var olan karmaşık ve karmaşık etkileşimlerin derin bir şekilde anlaşılmasına sağlam bir şekilde kök salması gereken küresel toplumun uyumlu ve birleşik bir çabasını gerektirir. Siber savunma için çok yönlü ve bütünsel bir stratejiyi benimserken, aynı anda uluslararası işbirliğini teşvik ederek ve yenilikçi araştırma alanlarını takip ederek, küresel toplumun dijital çağın yarattığı engelleri aşma şansı çok daha yüksektir. Sonuç olarak oluşturulacak kollektif çaba, gelecek nesillere miras bırakılabilecek barışçıl ve istikrarlı bir siber alan geliştirmeyi ve herkes için güvenli ve müreffeh bir dijital ortam sağlamayı amaçlamaktadır.

Kaynakça

Abbate J, 1999 Inventing the Internet (MIT Press, Cambridge, MA).

Adegbite, A.O., Akinwolemiwa, D.I., Uwaoma.P.U., Kaggwa, S.., Akindote O.J., Dawodu,S.O., (2023). Review of cybersecurity strategies in protecting national infrastructure: perspectives from the usa. Computer science ve IT research journal, V olume 4, Issue 3, 200-219.

Andrey, S. (2023). 10. Russia's participation in multistakeholder diplomacy for cybersecurity norms. Building an International Cybersecurity Regime, (Ed.)Ian Johnstone, Arun Sukumar and Joel Trachtman, Monograph Book,

Apruzzese, G., Laskov, P., Montes de Oca, E., Mallouli, W., Brdalo Rapa, L., Grammatopoulos, A. V., ve Di Franco, F. (2023). The role of machine learning in cybersecurity. *Digital Threats: Research and Practice*, *4*(1), 1-38.

Archick. K. (2005). Cybercrime: The Council of Europe Convention, Law, Political Science, Computer Science,

Brundage, M., Avin, S., Clark, J., Toner, H., Eckersley, P., Garfinkel, B., ... ve Amodei, D. (2018). The malicious use of artificial intelligence: Forecasting, prevention, and mitigation. *arXiv preprint arXiv:1802.07228*.

Buchanan, B. (2016). *The Cybersecurity Dilemma: Hacking, Trust, and Fear Between Nations*. Oxford University Press.

Buchanan, B. (2020). The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics. Harvard University Press.

Burton, J., (2015). NATO's cyber defence: strategic challenges and institutional adaptation, Defence Studies, 15/4, Routledge, 297-319.

Chen, L., Chen, L., Jordan, S., Liu, Y. K., Moody, D., Peralta, R., ... ve Smith-Tone, D. (2016). *Report on post-quantum cryptography* (Vol. 12). Gaithersburg, MD, USA: US Department of Commerce, National Institute of Standards and Technology.

Chesterman, S. (2020). Artificial intelligence and the limits of legal personality. *International ve Comparative Law Quarterly*, *69*(4), 819-844.

Clarke, R. A., ve Knake, R. K. (2010). Cyber War: The Next Threat to National Security and What to Do About It. HarperCollins.

Clarke, R. A., ve Knake, R. K. (2019). *The Fifth Domain: Defending our country, our companies, and ourselves in the age of cyber threats*. Penguin Press.

Clough, J. (2012). The Council of Europe Convention on Cybercrime: Defining `Crime' in a Digital World. *Crim Law Forum* 23, 363–391

Council of Europe. (2001). Convention on Cybercrime.

Creemers, R. (2023). 6. The Chinese Conception of Cybersecurity: A Conceptual, Institutional and Regulatory Genealogy. Journal of Contemporary China, 33(146), 173–188.

Cybersecurity Law of the People's Republic of China. (2017). National People's Congress of the People's Republic of China.

Cybersecurity, C. I. (2018). Framework for improving critical infrastructure cybersecurity. *URL: https:// nvlpubs. nist. gov/nistpubs/CSWP/NIST. CSWP*, *4162018*.

Cybersecurity, U. S. (2021). Infrastructure Security Agency (CISA). *GE Aestiva and Aespire Anesthesia (Update A). https://us-cert. cisa. gov/ics/advisories/icsma-19-190-01.*

François, Delerue. (2019). Attribution to State of Cyber Operations Conducted by Non-State Actors.

Denning, D. E. (2011). Cyber conflict as an emergent social phenomenon. In *Corporate hacking and technology-driven crime: Social dynamics and implications* (pp. 170-186). IGI Global.

European Union Agency for Cybersecurity (ENISA). (2020). ENISA Threat Landscape 2020.

Farwell, J. P., ve Rohozinski, R. (2011). Stuxnet and the future of cyber war. *Survival*, *53*(1), 23-40.

Floridi, L., ve Taddeo, M. (2016). What is data ethics?. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, *374*(2083), 20160360.

Ferenț, D.A ve Preja, C. (2023), NATO's involvement in cyber defence, *Intelligence Info*, 2:1, 189-193.

Gercke, M. (2012). Hard And Soft Law Options in Response to Cybercrime: How to weave a more effective net of global responses. *Computer law review international*, *13*(3), 78-87.

Healey, J. (2012). A Fierce Domain: Conflict in Cyberspace, 1986 to 2012. Cyber Conflict Studies Association.

Henderson, C. (2015). "The United Nations and the regulation of cyber-security," Chapters, in: Research Handbook on International Law and Cyberspace, chapter 22, 465-490.

Jason, D., Jolley., Jason, D., Jolley. (2019). Attribution, state responsibility, and the duty to prevent malicious cyber-attacks in international law.

Karnouskos, S. (2011, November). Stuxnet worm impact on industrial cyber-physical system security. In *IECON 2011-37th Annual Conference of the IEEE Industrial Electronics Society* (pp. 4490-4494). IEEE.

Kello, L. (2017). The Virtual Weapon and International Order. Yale University Press.

Keohane, R. O., ve Nye Jr, J. S. (1998). Power and interdependence in the information age. *Foreign Aff.*, *77*- 81-94.

Lin, H. (2016). Attribution of malicious cyber incidents: from soup to nuts. *Journal of International Affairs*, *70*(1), 75-137.

Lin, H. (2017). Cyber Conflict and International Humanitarian Law. *International Review of the Red Cross, 94(*886), 515-531.

Luitel, P. (2024). Role of Non-State Actors in National Security. Unity journal, Vol.5, 57-75.

Lucas, G. R. (2017). *Ethics and cyber warfare: the quest for responsible security in the age of digital warfare*. Oxford University Press.

Margulies, P. (2013). Sovereignty and cyber attacks: Technology's challenge to the law of state responsibility. Melbourne Journal of International Law, no:155, vol.14, pp.496-522.

Mearsheimer, J. J. (2014). The Tragedy of Great Power Politics. Updated Edition. W. W. Norton ve Company.

Mittelstadt, B. (2019). AI ethics – too principled to fail? SSRN Electronic Journal.

Mosca, M. (2018). Cybersecurity in an era with quantum computers: Will we be ready?. *IEEE Security ve Privacy*, *16*(5), 38-41.

Muzhanova. T., Lehominova, S., Shchavinsky, Y., Yakymenko, Y., (2024). Main approaches and directions of development of european union cyber security policy, Cybersecurity Education Science Technique, 4(24):133-149.

NATO. (2016). Warsaw Summit Communiqué. NATO Official Website

Nye, J. S. (2010). *Cyber Power* (pp. 1-24). Cambridge: Harvard Kennedy School, Belfer Center for Science and International Affairs.

Nye Jr, J. S. (2016). Deterrence and dissuasion in cyberspace. *International security*, *41*(3), 44-71.

Paris Peace Forum. (2018). Paris Call for Trust and Security in Cyberspace.

Pauletto.C. (2020). Information and telecommunications diplomacy in the context of international security at the United Nations. Transforming Government: People, Process and Policy, Vol. 14 No. 3, pp. 351-380

Proakis, J. G. (2008). *Digital Communications*. McGraw-Hill, Higher Education.

Renda, K. (2022). The development of eu cybersecurity policy: from a coordinating actor to a cyber power?. Ankara Avrupa çalışmaları dergisi, Cilt:21, No:2 (Yıl: 2022), s. 467-495.

Rid, T. (2012). Cyber War Will Not Take Place. Journal of Strategic Studies, 35(1), 5-32.

Rid, T., ve Buchanan, B. (2015). Attributing cyber attacks. *Journal of Strategic Studies*, *38*(1-2), 4-37.

Romagna, M. (2020). Hacktivism: Conceptualization, Techniques, and Historical View. In: Holt, T., Bossler, A. (eds) The Palgrave Handbook of International Cybercrime and Cyberdeviance. Palgrave Macmillan.

Satyanarayanan, M. (2017). The emergence of edge computing. *Computer*, *50*(1), 30-39.

Schmitt, M. N. (Ed.). (2013). Tallinn Manual on the International Law Applicable to Cyber Warfare. Cambridge University Press.

Segal, A. (2016). The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age. PublicAffairs.

Shemakov, R. (2019). The Morris Worm: Cyber Security, Viral Contagions, and National Sovereignty.

Singer, P. W., ve Friedman, A. (2014). Cybersecurity and Cyberwar: What Everyone Needs to Know. Oxford University Press.

Singer, P. W. (2015). Stuxnet and its hidden lessons on the ethics of cyberweapons. *Case W. Res. J. Int'l L.*, *47*, 79.

Stepanova, M.N. (2024). Information security in the legal field: strategies for legal regulation and protection of cyberspace. Law Research Journal, Vol.1, No:2, 91-101

Sujayraj, S. (2019). Classification of Cyber Attacks and its Associated Laws. Journal of emerging technologies and innovative research, 6(2), 289-298

Taddeo, M., ve Floridi, L. (2018). Regulate artificial intelligence to avert cyber arms race. *Nature*, 556, 296-298.

Taylor, L., Floridi, L., ve Van der Sloot, B. (Eds.). (2016). *Group privacy: New challenges of data technologies* (Vol. 126). Springer.

Tikk, E., Kaska, K., ve Vihul, L. (2010). "International Cyber Incidents: Legal Considerations". NATO Cooperative Cyber Defence Centre of Excellence.

United Nations General Assembly. (2015). Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security.

Valeriano, B., ve Maness, R. C. (2018). Cyber War versus Cyber Realities: Cyber Conflict in the International System. Oxford University Press.

Waqas, A. (2024). Digital Terrorism: The Emerging Threat of Behavioral Manipulation in the Digital Age. Journal of Digitainability, Realism ve Mastery,

Walker S, Tennant I. Cybercrime, the United Nations, Prospects, and Challenges for International Co-operation. In: Ishikawa T, Kryvoi Y, eds. Public and Private Governance of Cybersecurity: Challenges and Potential. Cambridge University Press; 2023:69-102.

Wendt, A. (1992). "Anarchy is What States Make of It: The Social Construction of Power Politics". International Organization, 46(2), 391-425.

Zhu, L. ve Chen, W. (2022). 5. Chinese Approach to International Law with Regard to Cyberspace Governance and Cyber Operation: From the Perspective of the Five Principles of Peaceful Co-existence. Baltic yearbook of international law,