Marmara Üniversitesi Siyasal Bilimler Dergisi • Marmara University Journal of Political Science • Cilt 9, Sayı 1, Mart 2021, ISSN 2147-6926, ss. 17-45 • DOI: 10.14782/marmarasbd.876091

**RESEARCH ARTICLE** / ARAŞTIRMA MAKALESİ

# Birleşmiş Milletler Sistemi ve Küresel Siberalan Güvenliği Regülasyonu

## The United Nations System and the Regulation of Global Cyberspace Security

**Tuba ELDEM***

**Öz**

Daha yakın zamana kadar büyük ölçüde bilgisayar sistemlerinin teknik korumasıyla ilişkilendirilen siber güvenlik, son beş yılda önemli ekonomik, insani ve ulusal güvenlik riskleri doğuran geleneksel olmayan bir güvenlik sorun olarak küresel toplumun gündemini sıklıkla meşgul etmektedir. Evrensel üyeliğe sahip ve egemen eşitlik ilkesi tarafından yönlendirilen Birleşmiş Milletler (BM), ulusal ve uluslararası siberalan güvenliği tartışmalarının yapıldığı önemli küresel hükümetlerarası örgütlerden biridir. Siber güçlerin siber normları kendi gündemleri çerçevesinde şekillendirmede etkin bir örgütsel platform ve araç olarak kullandıkları BM Genel Kurulu'nda siber güvenliğin siyasi, askeri, mali ve insani boyutlarıyla ilgili yürütülen müzakereleri ve kararları inceleyen bu makale, bir yandan siber güvenlik konusunda uluslararası toplumda oluşan fay hatlarını ortaya koymakta, diğer yandan birçok farklı hükümetlerarası organ ve örgütsel platformda ele alındığı için oldukça parçalanmış nitelikte olan BM'nin siberalan güvenliği regülasyonu hakkında tematik ve bütüncül bir analiz sunmaktadır. Makale, siber güçler arasında uluslararası siber güvenlik rejiminin niteliğine yönelik normatif çatışmayı, devletlerin siberalanda artan gücünü ve etkisini ve küresel yönetişimde Batı'dan Doğu'ya doğru bir kaymayı içeren üç ana eğilimin siberalanı şekillendirdiğini ortaya koymaktadır. Ayrıca çalışma kapsamında, devletler arasında siberalandaki faaliyetleri düzenlemek için harekete geçme iradesinde fark edilebilir bir ivme göze çarpsa da ortaya çıkan düzenleyici çerçevenin odağı ve siberalanı yönetmeye yönelik temel yaklaşımla ilgili olarak uluslararası toplumda net bir ayrımın devam ettiği ve siberalanın 21. yüzyılın merkezi bir jeopolitik rekabet alanı olarak ortaya çıktığı sonucuna varılmaktadır.

**Anahtar Kelimeler:** Uluslararası Siyaset, Uluslararası Örgütler, Birleşmiş Milletler, Uluslararası Siber Güvenlik, Uluslararası Güvenlik, Geleneksel Olmayan Güvenlik Tehditleri, Küresel Yönetişim

**Abstract**

Cybersecurity, which was until recently largely associated with the technical protection of computer systems, has in the last five years risen on the global community's agenda as an important non-traditional security issue posing significant economic, humanitarian, and national security risks. The United Nations (UN), with its universal membership and guided by the sovereign equality principle, has emerged as one of the first important global intergovernmental organizations for international

* Fenerbahçe Üniversitesi, The Center for Applied Turkey Studies (CATS) of the German Institute for International and Security Affairs (SWP), E-posta: tuba.eldem@fbu.edu.tr, Orcid: 0000-0001-6264-255X

**Makale Gönderim Tarihi / Submitted:** 07.02.2021
**Yayına Kabul Tarihi / Accepted:** 20.03.2021

cybersecurity debates. However, its regulation of cybersecurity, covering all aspects of protection from risks arising from the use of cyberspace by citizens, businesses, and governments, is highly fragmented as it is implemented by many different intergovernmental bodies and organizational platforms. In this article, I examine UN resolutions on the political, military, economic, and humanitarian aspects of cybersecurity to provide a thematic and holistic analysis of UN's activities regarding cybersecurity. I also reveal the fault lines in the international community on cybersecurity by examining debates in the UN General Assembly and other organizational platforms, which cyber powers use both as a forum and resource to shape the global cyber norms agenda. My analysis shows that three main trends shape cyberspace regulation at the UN: a normative conflict between cyber powers over the nature of the international cybersecurity regime; the increasing power and influence of states in cyberspace; and a shift from West to East in global cyberspace governance. While states are clearly willing to regulate activities in cyberspace, the article also reveals a clear divide within the international community regarding the focus of the emerging regulatory framework and the basic approach to managing cyberspace. I conclude that cyberspace is likely to remain a central area of geopolitical competition in the 21st century.
**Keywords:** International Politics, International Organizations, United Nations, International Cybersecurity, International Security, Non-Traditional Security Threats, Global Governance

## 1. Giriş

Birkaç yıl öncesine kadar uluslararası bir sorun olarak çok az ilgi gören ve büyük ölçüde bilgisayar sistemlerinin teknik korumasıyla ilişkilendirilen siber güvenlik, son yıllarda dünyanın karşılaştığı en ciddi ekonomik, insani ve ulusal güvenlik sorunlarından biri olarak ön plana çıkmaktadır. 2007'de Estonya'da, 2008 ve 2019'de Gürcistan'da, 2010'da İran'da, 2014 ve 2015'te Ukrayna'da ve 2019'da Hindistan'da devlet kuruluşlarını ve kritik altyapıları hedefleyen, kimi zaman hibrit savaş bağlamında yürütülen ve devlet destekli olduğu iddia edilen bilgisayar ağ operasyonları; 2016 ABD ve 2017 Fransa Cumhurbaşkanlığı seçimlerinde, 2016'da İngiltere'de Brexit ve 2018'de Makedonya'da referandum süreçlerinde siberalan aracılığı ile gerçekleştirilen enformasyon veya "etki" operasyonları, bir yandan siber risklerin ulusal güvenlik boyutuna işaret ederken diğer yandan 21.yüzyılın jeopolitik rekabet alanı olarak siberalanın merkezi konumunu teyit etmektedir. Hastanelerin kapanmasına, elektrik şebekelerinin devre dışı bırakılmasına, büyük şehirlerdeki hayatın durmasına ve demokratik süreçlerin bütünlüğünün bozulmasına yol açan bu siber saldırılar insan güvenliğini de gittikçe daha fazla tehdit etmektedir. Dünyanın korona virüs salgını ile mücadele ettiği 2020 yılında sağlık hizmetlerini devre dışı bırakmaya ve COVID-19 aşı araştırmalarını çalmaya yönelik siber saldırılar ve halk sağlığı tepkisini zayıflatmak ve devlet ve devlet dışı aktörlerin alternatif gündemlerini ilerletmek amacıyla yapılan dezenformasyon operasyonları siber risklerin insani maliyetlerini göstermektedir (Microsoft, 2020; WHO, 2020; Oxford University, 2020a; 2020b). Nitekim günümüzde, sağlık, bankacılık, finans, telekomünikasyon, enerji gibi kritik altyapı sektörlerinin siber-fiziksel bilgi altyapılarına yönelik gerçekleştirilen siber saldırılar ilk on küresel risk arasında kabul edilmektedir (WEF, 2020).

Siber saldırıları isnat etmede yaşanan zorluklar, düşük giriş maliyetleri ve yasal belirsizlikler siber operasyonları hem ulus devletler hem de devlet dışı aktörler için ucuz ve çekici bir araç

hâline getirmektedir. Devlet destekli siber casusluk gruplarından fidye yazılımı çetelerine kadar uzanan uluslararası siber suç ağlarının, siberalanın tanıdığı göreceli anonimlikten ve siber suçu tanımlayan uyumlu ulusal yasaların yokluğundan yararlanarak son yıllarda küresel olarak faaliyetlerini artırdıkları gözlemlenmektedir**.** Diğer yandan, siberalanın hem devlet hem de devlet dışı aktörler tarafından kötüye kullanılmasıyla birlikte insan hakları sorunları oldukça artmaktadır. Bu gelişmeler, pekişmiş liberal demokrasiler de dâhil olmak üzere bir dizi devlette kitlesel gözetleme, sansür, fikir ve ifade özgürlüğünün sınırlandırılması, hatta iç muhalefet üzerindeki baskıların meşrulaştırılması gibi insan haklarını kısıtlayıcı uygulamalara yol açarak, siberalan güvenliğinin çevrimiçi gizlilik ve insan hakları boyutlarını uluslararası toplumun gündemine taşımaktadır (Deibert ve Crete-Nishihata, 2012; Deibert, 2015).

Bulaşıcı salgın hastalıklar, doğal afetler, iklim değişikliği, çevresel bozulma, uyuşturucu, silah ve insan kaçakçılığı, terörizmin ve korsanlığın yayılması gibi siber tehditler de uluslararası ve ulusal güvenlik politikası arasındaki sınırı ortadan kaldıran ulusötesi ve geleneksel olmayan güvenlik sorunlarından biridir. Ulusötesi güvenlik tehditlerinin sınır tanımadığı gerçeği göz önüne alındığında, bunları etkili bir şekilde ele alma çabaları, devletler ve benzer şekilde ilgili devlet dışı aktörler arasında yakın alışveriş ve iş birliğini gerektirir. Bu bağlamda norm inşa etme ve güven oluşturma çabalarını içeren birçok girişim, son on yılda Afrika Birliği (2014), Güneydoğu Asya Ülkeleri Birliği (ASEAN, 2017), Avrupa Konseyi (2001), Avrupa Birliği (2019), G7 (2016), G20 (2015), Amerikan Devletleri Teşkilatı (OAS, 2004), Ekonomik İş birliği ve Kalkınma Teşkilatı (OECD, 2002; 2008; 2019), Avrupa Güvenlik ve İşbirliği Teşkilatı (OSCE, 2016a; 2016b; 2017), Şangay İşbirliği Teşkilatı (SCO, 2009) ve Kuzey Atlantik Antlaşması Örgütü (Schmitt,2017) gibi çeşitli uluslararası ve bölgesel örgütler bünyesinde süre gelmektedir. Bu girişimler, siberalan kullanımından kaynaklanan çatışma riskini azaltmayı, silahlı çatışma eşiğinin üstünde veya altında bir siber olay meydana geldiğinde tepkinin ne olması gerektiğini tanımlamayı, kritik altyapıların veya küresel finansal hizmetlerin dayanıklılığını güçlendirilmeyi, siber riskleri yönetmeyi ve internetin terörist ve suç amaçlı kullanımına yanıt vermek için iş birliğini geliştirmeyi hedeflemektedir (Kavanagh, 2017). Bunların yanı sıra son on yılda, İnternet Yönetişimi Küresel Komisyonu, Siberalan İstikrarı Küresel Komisyonu ve Carnegie'nin Siber Politika Girişimi gibi yüksek profilli uzmanlardan oluşan özel norm süreçleri, Microsoft tarafından başlatılan Cybersecurity Tech Accord ve Siemens liderliğindeki Trust Charter gibi endüstri odaklı norm süreçleri, Paris Siberalanda Güven ve Güvenlik Çağrısı, İnternet Yönetişim Forumu, Siber Uzmanlık için Küresel Forum, NETmundial Girişimi ve Christchurch Çağrısı gibi çok paydaşlı norm süreçlerinin ortaya çıktığı görülmektedir (Ruhl ve diğer., 2020). Ayrıca artan sayıda uluslararası aktör, devletlerin söz konusu norm süreçlerini ve ilgili önlemleri bölgesel ve ulusal düzeylerde uygulama çabalarını desteklemek için kapasite geliştirme desteği ve teknik yardım sağlamaktadır.

Birleşmiş Milletler (BM), uluslararası siberalan güvenliği tartışmaları için erken ve önemli küresel hükümetlerarası forumlardan biri olarak ön plana çıkmaktadır. Vatandaşları, işletmeleri ve devletleri siberalan kullanımından kaynaklanan risklerden korumanın tüm düzenleyici yönlerini kapsayan BM'nin siber güvenlik regülasyonu, birçok farklı hükümetlerarası organ ve

örgütsel platformda ele alındığı için oldukça parçalanmış niteliktedir. Bu makale, siberalana yönelik ve siberalan aracılığı ile ortaya çıkan riskleri geleneksel olmayan sınır ötesi bir güvenlik sorunu olarak ele alarak BM sisteminde devam eden siberalanı regüle etmeye yönelik kararları ve süreçleri resmî belge analizi ve süreç izleme (Collier, 2011) yöntemleri ile incelemektedir. Siberalan güvenliğine ilişkin temel kavramların tanımlanması ile başlayan makale, BM Genel Kurulu'nun çeşitli komitelerinde ve örgütsel platformlarında siber savaştan korunma, kritik altyapıların siber saldırılara karşı korunması, siber suçlarla mücadele ve çevrimiçi gizliliğin korunması konularında kabul edilen kararların incelenmesi ile devam etmektedir. Makale, bir yandan BM'nin siber güvenlik regülasyonu konusunda gelişen eko-sisteminin tematik bir analizini sunmayı diğer yandan BM Genel Kurulunu siber güçlerin çıkarlarını ilerletmek için kullandıkları bir müzakere platformu olarak ele alarak, siber güvenlik konusunda siber güçler arasındaki fay hatlarını ortaya koymayı amaçlamaktadır. Makale siberalanı düzenlenmek konusunda devletler arasında giderek artan oranda iş birliği arayışını göz önüne serse de uluslararası toplumda düzenleyici çerçevenin odağı ve siberalanı yönetmeye yönelik temel yaklaşımla ilgili olarak net bir ayrımın devam ettiği ve siberalanın 21. yüzyılın merkezi bir etki ve güç alanı olarak ortaya çıktığı sonucuna varmaktadır.

## 2. Küresel Siberalan Güvenliği

Siber güvenlik açısından en temel kavram olan siberalan, gündelik hayatta internet ile eşanlamlı olarak kullanılansa da aslında sadece internet ve internete bağlı cihazları değil, telekomünikasyon ağları, bilgisayar sistemleri, gömülü işlemciler ve kontrolörler dâhil olmak üzere tüm bilgi altyapılarını, fikir ve sanal gerçekleri de içinde barındıran sanal dünyanın toplamını ifade etmektedir. Literatür siberalanı; fiziksel ağ, mantıksal ağ ve siber-persona olmak üzere birbiriyle etkileşim halinde olan üç katmandan oluşan bir yapı olarak tanımlamaktadır (ABD Ordusu Ortak Yayını JP 3-12, 2018; Schmitt, 2017, s.12; Deibert ve diğer., 2012, s.5-6). Siberalanın temel katmanı; mekanik ve elektriksel, manyetik ve optik iletişim hatlarını oluşturan bilgisayarlar, yönlendiriciler, kablolar, sunucular, cep telefonu kuleleri, uydular gibi makineleri ifade eden fiziksel altyapıdır. Fiziksel katman, verinin iletildiği kara ve deniz altı kabloları gibi kablolu ve radyo, röle-radyo, hücresel, uydu gibi kablosuz iletim araçlarını içermektedir. Siberalanın mantıksal veya "kod" katmanı; alan isimlendirme sistemi (DNS) ve internet servis sağlayıcıları (ISP) gibi iletişim trafiğini çalıştıran mantıksal talimatlar ve yazılımları ifade etmekte ve fiziksel katmanda veri alışverişine izin veren uygulamalar, veriler ve protokoller dâhil ağ cihazları arasında var olan bağlantılardan oluşmaktadır. Bireyler de dâhil olmak üzere ağ üzerinde yer alan bütün aktörleri ifade eden siber-persona katmanı kimi zaman "sosyal" (Schmitt, 2017, s.12) veya "düşünsel" (Deibert ve diğer., 2012, s.6) katman olarak da tanımlanmaktadır. Videoların, görüntülerin, seslerin ve metinlerin dolaştığı bu katmanı hedef alan siber operasyonlar askeri alanda 'enformasyon operasyonları' olarak adlandırılmaktadır (Deibert ve diğer., 2012, s.6).

Siberalan güvenliği hem bu yeni alanın yarattığı güvensizlikle hem de onu daha güvenli hâle getirecek süreçler, politikalar, prosedürler, düzenlemeler, standartlar, yazılımlar ve donanımlarla

ilgilidir. Dar anlamda, "siberalandaki bilgilerin gizliliğinin, bütünlüğünün ve kullanılabilirliğinin korunması" (ISO/IEC 27032, 2012) olarak tanımlanan siber güvenlik kavramı, yıllar içinde genişleyerek hem donanım, yazılım ve ilgili altyapıda dâhil olmak üzere bilgi ve iletişim teknolojilerine bağlı sistemleri hem de içindeki bilgileri yetkisiz erişime veya erişim teşebbüslerine karşı korumayı amaçlayan bir dizi faaliyet ve önlemle ilişkilendirilmektedir (Finnemore ve Hollis, 2016, s. 431). Örneğin, BM uzman kuruluşu olan Uluslararası Telekomünikasyon Birliği (ITU, 2008), siber güvenliği "siber ortam ve organizasyon ve kullanıcının varlıkları korumak için kullanılabilecek araçlar, politikalar, güvenlik kavramları, güvenlik önlemleri, yönergeler, risk yönetimi yaklaşımları, eylemler, eğitim, en iyi uygulamalar, güvence ve teknolojilerin toplamı" olarak tanımlamaktadır (s.2). Uluslararası ilişkiler uzmanları ise siber güvenliği ulusal güvenliğin temel bir boyutu olarak değerlendirerek "devletin kendisini ve kurumlarını casusluk, sabotaj, suç ve dolandırıcılık, hırsızlık ve yıkıcı çevrimiçi etkileşimler ve çevrimiçi işlemleri içeren siberalandaki tehditlere karşı koruma yeteneği" olarak tanımlamaktadır (Chouchri, 2012, s.39).

Her ne kadar siber güvenliğin üzerinde mutabık kalınan ve tek tip bir tanımın yapılması zor olsa da uluslararası ilişkiler alanında siberalan güvenliği kavramı, siberalana yönelik ve siberalan vasıtasıyla ortaya çıkan risklerin minimize edilmesi olarak kavramsallaştırılmaktadır (Deibert ve Rohozinski, 2010). Siberalana yönelik riskler, bilgisayar ve iletişim teknolojilerinin fiziksel altyapısına yönelik riskleri işaret ederken siberalan vasıtasıyla ortaya çıkan riskler, siberalanda siber teknolojilerle gerçekleştirilen ancak kendi başlarına doğrudan kritik bilgi altyapılarını hedef almayan riskleri ifade etmektedir. Siberalan aracılığı ile ortaya çıkan riskler, Deibert ve Rohozinski'nin (2010) karanlık ağlar ve sivil direniş ağları olarak ifade ettikleri iki tur ağdan gelen riskleri içermektedir. Karanlık ağlar; çok çeşitli militan gruplar, radikal hareketler ve terör örgütlerini içinde barındıran uluslararası suç ve terör ağlarını kapsamaktadır. Son yirmi yılda siberalanın gelişmesi, bu karanlık ağlara operasyonlarını tamamen yerelden ulusal ve küresel boyuta taşımalarını kolaylaştıran önemli avantajlar sağlamıştır. Dolayısı ile ağ güvenliğinin ihlalleri, bilgisayar sistemlerine veya verilerine yasa dışı erişim veya müdahale, bilgisayarla ilgili dolandırıcılık, sahtecilik ve telif hakkı suçları, yasadışı mal satışı, çocuk pornografisinin çevrimiçi dağıtımı gibi suçlar büyük mali ve insani maliyetler doğurur hale gelmiştir. Ekonomik açıdan 2021 yılında siber suçların maliyetinin dakikada 11,4 milyon dolar olacağı (RiskIQ, 2020) ve siber suçların toplam maliyetinin 2021'de 6 trilyon ABD dolarına ulaşarak dünyanın en büyük üçüncü ekonomisinin gayri safi milli hasılasına eşdeğer olacağı öngörülmektedir (Cybersecurity Ventures, 2020). Dünya Ekonomik Forumu tarafından belirlenen uzun vadeli küresel on risk listesinde yer alan veri dolandırıcılığı veya hırsızlığı da önemli ölçüde artmaktadır (WEF, 2020). Nitekim sadece 2020'nin ilk dokuz ayında toplam 36 milyar kayıt çalınarak bu alanda dünya rekoru kırılmıştır (Risk Based Security, 2020). Bazı devletlerin siber saldırıları gerçekleştirmek için bilgisayar korsanları ve diğer uluslararası suç ağlarını vekil olarak kullanması, siber suç ile siber savaş arasındaki sınırı bulanıklaştırmakta ve uluslararası toplumdaki karşılıklı güveni zayıflatmaktadır (Kavanagh, 2017, s.44; Detsch, 2018).

Sivil direniş ağları siyasal otoriteye meydan okuyan halk hareketlerini ifade etmektedir. Tıpkı çok çeşitli suç ve silahlı örgütleri kapsayan karanlık ağlar gibi sivil direniş ağları da internet ve

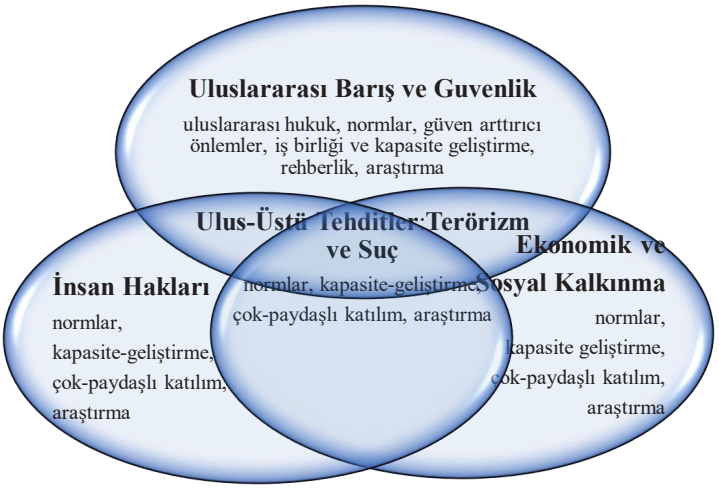
sosyal medya gibi siberalanın sağladığı imkânları kullanarak oldukça etkili protesto hareketlerine yönelmektedir. Bu sivil direniş hareketleri özellikle de otoriter rejime sahip olan devletler başta olmak üzere ulusal siyasal otoriteler için yeni, dinamik ve zorlu bir güvenlik riski meydana getirmektedir. Bu riskleri azaltmak için Rusya, Çin ve İran başta olmak üzere birçok devlet, stratejik ve politik amaçları doğrultusunda bilgi ve iletişimi engelleyen, işleyen ve şekillendirmeyi amaçlayan bir dizi düzenleyici önlem, yasa, politika ve taktikleri içeren enformasyon kontrol araçları kullanmaktadır (Deibert ve Crete-Nishihata, 2012; Deibert, 2015). Bu kontrol araçlarının kullanımı siberalanda içerik kontrolü, çevrimiçi gizlilik ve insan hakları gibi birçok konuyu uluslararası toplumun gündemine getirmektedir.

Her ne kadar çoğunlukla karıştırılsa da uluslararası düzeyde iş birliği ve devlet politikaları açısından iki risk türü farklılaşmaktadır. Siberalana yönelik risklerle ilgili olarak, kritik enformasyon altyapısı ve ağlarını ekonomi, hükümet, toplum ve kültür için yaşamsal olarak gören bir uluslararası anlayış ortaya çıkmaktadır. Bu nedenle ulusal ve uluslararası politikalar; ticaretin gelişebileceği, verilerin yolsuzluk olmadan iletilebileceği, finans ve bankacılık, enerji, ulaşım ve iletişim gibi kritik altyapı sektörlerinin önemli bir aksaklık veya kesinti olmadan çalışacağı bir küresel enformasyon ağının korunmasını esas almaktadır. Siber suçlar, kitlesel gözetim, içerik kontrolü gibi siberalan aracılığı ile oluşan riskler söz konusu olduğunda ise devletler arasında algılanan çıkarların önemli ölçüde farklılaştığı için daha zayıf uluslararası fikir birliği ve iş birliği sağlandığı görülmektedir (Deibert ve Rohozinski, 2010; Nye, 2014).

Siber güvenlik regülasyonu kavramı, bu risklerin gelecekteki gelişimi ve evrimini ele almak ve yönlendirmek için küresel düzeyde yürütülen tüm düzenleyici çabaların toplamını ifade etmektedir (Feick ve Werle, 2010, s. 525). Siberalan regülasyonu ile ilişkili konular ise spektrum tahsisi ve DNS standartları gibi İnternet yönetişimi ile ilgili konuların yanı sıra, telif hakkı ve fikri mülkiyet koruması, içerik düzenlemesi, çevrimiçi gizlilik, siber suç, siber casusluk, siber terörizm ve siber savaş gibi geniş bir alanı kapsamaktadır (Mueller, 2010, s. 79, Nye, 2014, s. 9-11; Finnemore ve Hollis, 2016). Bu sorun alanları üzerine çalışan pek çok bölgesel ve uluslararası örgüt ve İnternet Tahsisli Sayılar ve İsimler Kurumu (ICANN) gibi kâr amacı gütmeyen özel kuruluşlar vardır. Dolayısı ile siberalanı düzenlemeye yönelik tek bir forum veya uluslararası örgütten bahsedemeyecek olsak da gerçek anlamda tek küresel hükümetlerarası örgüt olan BM, uluslararası siber güvenlik normlarının ortaya çıkmasında önemli bir küresel müzakere forumu görevini ifâ etmektedir. Şimdiye kadar Güvenlik Konseyi, siber güvenlik konusunda kritik altyapının terör saldırılarına karşı korunmasına ilişkin bilgi işlem teknolojilerinin (BİT) güvenliğini önemli bir koruma unsuru olarak tanıyan 2341 (2017) sayılı kararı dışında siber güvenlik konusunda herhangi bir karar almamıştır. Fakat, siberalanın farklı yönlerini düzenlemeye ilişkin taslak kararlar; BM Genel Kurulu'nun Silahsızlanma ve Uluslararası Güvenlik Komitesi (Birinci Komite), Ekonomik ve Mali Komite (İkinci Komite) ve Sosyal, İnsani ve Kültürel Komite (Üçüncü Komite) olmak üzere BM'nin altı ana komitesinin üçü tarafından BM Genel Kurulu'na sunulmuş ve kabul edilmiştir. Aşağıdaki bölümler bu komitelerde sürdürülen tartışma ve kabul edilen kararları inceleyerek BM'nin oldukça dağınık olan siber güvenlik regülasyonunun tematik ve bütüncül analizini sunmakta ve uluslararası toplumda siber güvenlik ile ilgili uluslararası iş

birliği ve çatışmanın dinamiklerine, devletlerin siberalanın kontrolü için izlediği stratejilerine ve bu devletlerin siberalandaki çıkarlarını nasıl savunduklarına ışık tutmaktadır.

*Figür 1: Siberalan Regülasyonu Konusunda BM Çalışmalarının Arasındaki Bağlantılar*




**Kaynak:** Kavanagh, 2017, s.37'den yazar tarafından uyarlanmıştır.

### 3. Uluslararası Barış ve Güvenliğin Korunması için Siberalanda Sorumlu Devlet Davranışı Normları

BM'nin silahsızlanma ve uluslararası güvenlik konuları ile ilgilenen Birinci Komitesi, (Silahsızlanma ve Uluslararası Güvenlik Komitesi) Rusya'nın uluslararası güvenlik bağlamında bilgi ve telekomünikasyon alanındaki gelişmeler üzerine 1998 yılında sunduğu önergeden beri uluslararası siber güvenlik konusunda norm geliştirme sürecinde merkezi bir rol oynamıştır. BM Genel Kurulu, Rusya'nın önergesini kabul ederek enformasyon güvenliğinde bilimsel ve teknolojik gelişmelerin olduğunu, ancak potansiyel kötü amaçlı kullanımının da olabileceğinin altını çizmiş ve üye devletlerin enformasyon güvenliği konusunda görüşlerini isteyen yıllık önergeleri kabul etmeye başlamıştır (UNGA 53/70, 1999). Rusya'nın 2001 yılında sunduğu önergesinde bilgi güvenliği alanındaki mevcut ve potansiyel tehditleri ve olası iş birliği tedbirlerini değerlendirmek üzere, coğrafi dağılım temelinde seçilen 15 devlet uzmanından oluşan bir hükümet uzmanları grubu (Group of Governmental Experts, HUG) kurulmasını istemiştir (UNGA 56/19, 2001). Bu öneri kabul edilerek 2004–2005, 2009–2010, 2012–2013, 2014–2015 ve 2016–2017 yıllarında uluslararası güvenlik bağlamında siberalan kullanımının oluşturduğu tehditleri ve bu tehditlerin nasıl ele alınması gerektiğini inceleyen ve üçü uzlaşı raporu üreten beş BM Hükümetlerarası Uzman Grubu (HUG) oluşturulmuştur.

Son yirmi yıl içinde elliden fazla devletin Birinci Komite ve BM HUG bünyesinde katkıda bulunduğu uluslararası siber güvenlik veya enformasyon güvenliği tartışmaları, ABD ve Rusya'nın başını çektiği iki grubun çekişmesine sahne olmuştur. Sınır ötesi enformasyon içeriğini bir ulusal güvenlik meselesi olarak ele alan Rusya enformasyon içeriğinin gözetimini de kapsayan daha geniş ve bütünleşik bir "enformasyon güvenliği" stratejisi izlemektedir (Budnitsky ve Jia, 2018; Nocetti, 2015; Pallin, 2017). Enformasyon güvenliğini "enformasyon alanında ulusal çıkarların korunması" olarak tanımlayan Rusya'nın enformasyon güvenliği doktrini, devletlerin "enformasyon alanlarını" koruma hakkını vurgulamaktadır (Rusya Federasyonu, 2000). Bu hem enformasyon ve iletişim altyapısına hem de enformasyonun kendisine yönelik tehditlerin ortadan kaldırılmasını içermektedir. Sivil ve askeri enformasyon teknolojilerinin dünya çapındaki gelişiminin uluslararası yasal düzenlemelere ihtiyaç duyduğunu vurgulayan Rusya, enformasyon güvenliğine yönelik yeni bir uluslararası rejimin kurulması gerektiğini savunmaktadır (Tikk-Ringas, 2012, p. *7)*. Nitekim Rusya'nın siber güvenliğe ilişkin öncelikli dış politikası, devletlerin tehlikeli enformasyon silahları geliştirmesini ve siberalan aracılığı ile diğer devletlerin içişlerine karışmasını yasaklayacak çok taraflı bir enformasyon silahları kontrol antlaşmasının benimsenmesi yönünde olmuştur (UNGA, 1999). Rusya, enformasyon güvenliği normlarını, Şangay İş birliği Örgütü (The *Shanghai Cooperation Organisation – ŞİÖ*) çerçevesinde ve Çin'in desteğiyle bölgesel düzeyde desteklemektedir. ŞİÖ'nün altı üyesinden dördü 2011 yılında BM Genel Kurulu'na "Uluslararası Bilgi Güvenliği Davranış Kuralları" adlı bir sözleşme sunmuştur (UNGA Letter 66/359, 2011). Uluslararası insan hakları hukuku kapsamında ele alınan çevrimiçi gizlilik ve serbest bilgi akışı gibi ilkeleri ihlal ettiği için sivil toplum ve Batılı devletlerin eleştirilerine maruz kalan sözleşme kısıtlı olarak revize edilerek, ŞİÖ'nün'nun altı üye devleti tarafından 2015 yılında tekrar BM Genel Kurulu'na sunulmuştur (UNGA Letter 69/273, 2015). Rusya, BM bünyesindeki tartışmalarda ayrıca İran, Suriye, Mısır ve Suudi Arabistan gibi siber egemenler olarak adlandırılabilecek siberalanda sınırsız devlet egemenliğini savunan demokratik olmayan bir grup ülke tarafından desteklenmektedir (Kerr, 2018; Maréchal, 2017; McKune ve Ahmed, 2018; Safshekan, 2017).

ABD ve Avrupa ülkelerinin başını çektiği, çok paydaşlılar olarak adlandırılabilecek olan devlet grubu, serbest bilgi akışı ve kullanıcıların etkinliği üzerinde asgari devlet kontrollerinin olduğu, kamu ve özel sektör arasında dağıtılmış bir güvenlik ağı tarafından çok paydaşlı olarak yönetilen açık ve özgür bir siberalanı savunmaktadır. Bilginin içeriğini de tehdit olarak içermesi yüzünden bilgi güvenliği kavramına karşı çıkan bu devletler, siber-fiziksel altyapı ve siber ağların güvenliğine odaklanan siber güvenlik kavramını tercih etmektedir. ABD ve müttefikleri uluslararası hukukun siberalanda geçerli olduğunu savunmakta ve BM Şartı, mevcut silahlı çatışma yasası ve insanilik, gereklilik, orantılılık, ayrım gözetmeme gibi uluslararası insancıl hukukun yerleşik ilkelerinin siber teknolojilerin askeri uygulamalarına da uygulanabileceğini öne sürmektedir. ABD'nin başını çektiği bu devletler siber güvenliğin kapsamı ve odağı hakkında uluslararası ortak bir anlayış olmadığını belirtmektedir. Ayrıca siber teknolojiler çok hızlı geliştiği için birtakım sivil ve /veya askeri teknolojilerin geliştirilmesini veya bunların kullanılmasını kısıtlayacak bağlayıcı yasal bir düzenlemeden önce siberalan kullanımına ilişkin kapsayıcı ilkelerin tüm yönleriyle

oluşturulması gerektiğini savunmaktadır (Grigsby, 2017; Tikk-Ringas, 2012; Maurer, 2011; 2019; Ruhl ve diğer., 2020).

Bu görüş ayrılıklarından ve ABD'nin tek başına Rusya tarafından verilen önergeleri reddetmesinden dolayı 2009 yılına kadar BM Genel Kurulu ve BM HUG'larda pek ilerleme kaydedilmemiştir. 2009 yılında Obama'nın Başkan seçilmesiyle uluslararası iş birliğine daha fazla önem veren ABD yönetimi, bundan sonra Rusya'nın bilgi güvenliği alanında yasal olarak bağlayıcı bir silah kontrolü antlaşması için sunduğu öneriye karşı aktif bir şekilde barış zamanında siberalanda devlet davranışını düzenleyecek uluslararası normların geliştirilmesi konusunda liderliği üstlenmiştir (Maurer, 2019). ABD'nin Rusya tarafından verilen önergeye ortak sponsor olmayı kabul etmesi ile BM HUG siberalandaki mevcut ve potansiyel tehditlerin 21. yüzyılın en ciddi zorlukları arasında olduğuna dikkat çeken 2010 yılındaki ilk uzlaşı raporunu yayımlamıştır (UNGA 65/201, 2010).

Bunu takip eden 2013 uzlaşı raporu, uluslararası hukukun ve özellikle BM Şartının siberalan için geçerli olduğunu kabul etmiş (UNGA 68/98, 2013), 2015'teki uzlaşı raporu ise herkes için açık, güvenli, istikrarlı, erişilebilir ve barışçıl bir siberalan sağlayabilmek için siberalanda uygun devlet davranışına rehberlik edecek 11 norm ortaya koymuştur (UNGA 70/174, 2015). Bu normlar devletlerin kendi topraklarındaki siber teknolojilerin uluslararası haksız eylemler için kullanılmasını (Madde 13/c); kritik altyapıya kasıtlı olarak zarar veren veya işletilmesini engelleyen siber faaliyetler içerisine girmesini veya desteklemesini (Madde 13f) ve başka bir devletin acil müdahale ekiplerinin enformasyon sistemlerine zarar verecek faaliyetleri yürütmesini veya desteklemesini (Madde 13/k) sınırlandırmaktadır. Bu normlar devletleri hem kritik altyapısı kötü niyetli siber eylemlere maruz kalan başka bir devletin yardım taleplerine hem de kendi topraklarından başka bir devletin kritik altyapısını hedef alan kötü niyetli siber faaliyetleri azaltmaya yönelik yapılan taleplere cevap vermekle yükümlü kılmaktadır (Madde 13h). Ayrıca, devletleri küresel siber güvenlik kültürünün oluşturulması ve kritik enformasyon altyapılarının korunması hakkında 2003 yılında kabul edilen 58/199 sayılı BM Genel Kurul kararını dikkate alarak kritik altyapılarını siber tehditlerden korumak için uygun önlemler almaya çağırmaktadır (Madde 13/g). Öte yandan, söz konusu normlar devletleri, siberalanın güvenli bir şekilde kullanılmasını sağlarken, ifade özgürlüğü hakkı da dâhil olmak üzere insan haklarına tam saygı gösterilmesini sağlamak için internette insan haklarının geliştirilmesi, korunması ve kullanılmasına ilişkin İnsan Hakları Konseyi'nin 20/8 ve 26/13 sayılı kararlarına ve dijital çağda gizlilik hakkını tanıyan 68/167 ve 69/166 sayılı Genel Kurul kararlarına uymaya çağırmaktadır (Madde 13/e). Bu normlar, ayrıca devletleri uluslararası barış ve güvenliğe tehdit oluşturabilecek siber uygulamaları önlemek (Madde 13/a); siberalanın terörizm ve suç amaçlı kullanımını kovuşturma ve bu tür diğer tehditleri ele almak (Madde 13/d); ve siber teknolojiye bağımlı altyapıya yönelik potansiyel tehditleri sınırlamak ve ortadan kaldırmak için (Madde 13/j) iş birliğine davet etmekte ve siber olaylarda, devletleri olayın daha geniş bağlamı, siberalanda isnat etme zorlukları ve sonuçların niteliği ve kapsamı da dâhil olmak üzere tüm ilgili bilgileri dikkate almaya (Madde 13/b) çağırmaktadır.

BM HUG'un "herkes için açık, güvenli, istikrarlı, erişilebilir ve barışçıl bir siberalan" sağlayabilmek için tavsiye ettiği bu normlar G7 (2016), G20 (2015), OSCE (2016), ve ASEAN (2017) gibi uluslararası örgütler ve Siberalanda Güven ve Güvenlik üzerine Paris Çağrısı (2018) ve Siberalanın İstikrarına İlişkin Küresel Komisyon (GCSC, 2018, 2019) gibi çok taraflı ve çok paydaşlı platformlar tarafından desteklenmiştir. Bu gelişmeler uluslararası ortamda artan iş birliği arayışının işaretleri olarak görülebilse de söz konusu normları spesifikleştirmeyi amaçlayan beşinci BM HUG, üye devletler arasında süregelen uluslararası hukukun siberalana nasıl uygulanacağı, özellikle meşru savunma hakkı ve uluslararası insancıl hukukun siber çatışmalara uygulanabilirliği ve siber egemenliğin kapsamı konularındaki anlaşmazlık nedeniyle 2017 yılında bir uzlaşı raporu kabul edememiştir (UNGA 72/327, 2017). Siber güvenlik normlarının hayat döngüsündeki bu duraksama, BM Genel Kurulu'nun 2018'de Rusya ve ABD'nin başını çektiği iki rakip önergeyi onaylaması ile kısmen aşılmış ve siber güvenliğin uluslararası güvenlik bağlamında ele alınacağı ikili bir sürecin önü açılmıştır. ABD ve müttefiklerinin sunduğu önerinin kabulü ile altıncı bir HUG (UNGA Resolution 73/266, 2018) ve Rusya ve müttefiklerinin sunduğu önerge ile Açık Uçlu Çalışma Grubu (Open-Ended Working Group, AUÇG) 2019 yılında kurulmuştur (UNGA Resolution 73/27, 2018). 25 temsilci ile sınırlı olan BM HUG'un aksine tüm devletlerin ve devlet dışı paydaşların katılımına izin veren AUÇG, siberalanda sorumlu devlet davranışı normlarının uygulamada ne ifade ettiğini ve nasıl uygulanabileceği konusunda somut tavsiyeler üreterek, bu normların daha geniş kitlelere yayılmasında kritik bir rol oynama potansiyeline sahiptir. Nitekim Aralık 2019'da siberalan yönetişimi ile ilgili BM müzakereleri, ilk kez çok paydaşlı bir formatta yapılmış ve bu sayede düşünce kuruluşları, insan hakları grupları, epistemik topluluklar, siber güvenlik kuruluşları ve çok uluslu şirketler dâhil olmak üzere yüzden fazla sivil toplum kuruluşu siberalanda sorumlu davranış için normlar, kurallar ve ilkeler hakkında fikir alışverişinde bulunmak için BM himayesinde bir araya gelmiştir. Diğer yandan AUÇG, BM HUG'dan farklı olarak ayrıca BM himayesi altında düzenli kurumsal diyalog kurma olasılığını incelemek üzerine görevlendirilmesi Rusya'nın küresel bir enformasyon güvenliği rejiminin kurulmasına yönelik hedefine yaklaştırdığına işaret etmektedir.

### 4. Sürdürülebilir Kalkınmanın Korunması için Kritik Bilgi Altyapılarının Siber Saldırılara Karşı Korunması

BM Genel Kurulu'nun ekonomik ve mali konularla ilgilenen ve çok taraflı küresel bir forum niteliğini haiz olan İkinci Komitesi, kritik enformasyon altyapılarının siber saldırılara karşı korunması için ortak bir siber güvenlik kültürünün inşa edilmesinde önemli bir rol oynamıştır. Siber-fiziksel bilgi altyapılarının giderek bankacılık, finans, sağlık, telekomünikasyon, enerji gibi kritik sektörlerin önemli bir parçasını oluşturduğunu gözlemleyen ABD, Fransa, Almanya, İtalya, Japonya, Birleşik Krallık, Kanada ve Rusya'dan oluşan G8'in kritik bilgi altyapılarının korunması için bir dizi ilke ve norm önermesinden sonra (G8, 2003), ABD'nin liderliğinde bu devletler, siber-fiziksel bilgi altyapılarının korunmasını öngören yeni bir "güvenlik kültürünün" gerekliliğini BM Genel Kuruluna taşımıştır. BM Genel Kurulu'nun İkinci Komitesi, küresel bir siber güvenlik yaratılması konusunda 2002, 2003 ve 2009'da aldığı üç karar ile uluslararası

siber güvenlik kültürünün ana unsuru olarak kritik bilgi altyapılarının siber saldırılara karşı korunmasının ortaya çıkmasında küresel bir forum olarak önemli rol oynamıştır. Bu yanı ile Tim Maurer'in (2011) de ifade ettiği gibi Birinci Komite'de siber savaşa yönelik siyasi-askeri akımı ve Üçüncü Komite'de siber suç odaklı ekonomik akımı büyük ölçüde birleştirmiştir (s.43).

Siber güvenliğin küresel ekonomi ve sürdürülebilir kalkınma bağlamında ele alındığı bu kararlardan ilki "küresel bir siber güvenlik kültürünün yaratılması" adlı BM Genel Kurul'unun 20 Aralık 2002'de kabul ettiği karardır (UNGA 57/239, 2002). ABD'nin liderlik ettiği tasarıya Rusya'nın dâhil olduğu toplam 36 üye ülke ortak sponsor olmuş, Çin ise katılmamıştır (UNGA Report 57/529/Add. 3, 2002). Küresel bir siber güvenlik kültürünün yaratılması için farkındalık, sorumluluk, yanıt verme, etik, demokrasi, risk değerlendirmesi, güvenlik tasarımı ve uygulaması, güvenlik yönetimi ve yeniden değerlendirme olmak üzere 9 tamamlayıcı unsurun altını çizen karar, ortaya çıkan dijital uçurumun üstesinden gelmek için teknoloji transferleri ve kapasite geliştirme çabalarını artırma çağrısında bulunmuştur (UNGA Resolution 57/239, 2002). Ayrıca nihai karar, üye devletleri 2005 yılında Tunus'ta düzenlenecek olan Dünya Bilgi Toplumu Zirvesi'ne bu kararı dikkate alarak katılmaları için davet etmiştir.

ABD'nin önderlik ettiği ancak Rusya tarafından desteklenmeyen küresel bir siber güvenlik kültürünün yaratılması ve kritik bilgi altyapılarının korunması adlı ikinci karara, Çin'in de dâhil olduğu toplam 69 ülke ortak sponsor olmuştur (UNGA Report 58/481/Add.2, 2003). Kritik bilgi altyapılarını korumaya yönelik unsurlar ekini içeren ve 2003 yılında kabul edilen bu karar, etkili siber güvenlik için gerekli temel unsurları vurgulamış, kritik altyapıları korumak için belirli adımlar önermiş ve özel sektörün rolünü vurgulamıştır. Karar ayrıca küresel bir siber güvenlik kültürünün yaratılmasına ilişkin unsurlar arasında siber güvenlik açıkları, tehditler ve olaylarla ilgili acil durum ağlarına sahip olma, bilgi altyapılarını ve bunlar arasındaki karşılıklı bağımlılıkları inceleme, kamu ve özel sektör paydaşları arasında bilgi paylaşımı da dâhil olmak üzere ortaklıkları teşvik etme, yeterli maddi ve usul kanunlarına ve saldırılara karşı etkili soruşturma ve kovuşturma yürütebilecek eğitimli personele sahip olma ve kritik bilgi altyapılarını güvence altına almak için uluslararası iş birliğine girme gibi eylemleri kapsamaktadır (UNGA Resolution 58/199, 2003).

Küresel bir siber güvenlik kültürünün oluşturulması ve kritik bilgi altyapılarının korunması için ulusal çabaların envanterinin çıkarılmasına yönelik diğer 39 ülke adına ABD tarafından sunulan Rusya ve Çin'in ise katılmadığı üçüncü önerge, İkinci Komite tarafından 15 Aralık 2009'da benimsenerek Genel Kurul'a sunulmuştur (UNGA Report 64/422/Add.3, 2009). BM Genel Kurulu tarafından 21 Aralık 2009'da kabul edilen önerge, üye devletlere kritik bilgi altyapılarını koruma ve siber güvenliklerini güçlendirme çabalarına yardımcı olmak için gönüllü ve yararlı bir öz değerlendirme aracı önermiştir (UNGA Resolution 64/211, 2009). Bugün ulusal siber güvenlik stratejilerini geliştirmeye çalışan devletler için bir temel oluşturan bu kılavuz, devletleri siber güvenlik ihtiyaçları ve stratejileri, paydaş rolleri ve sorumlulukları, politika süreçleri ve katılım, kamu-özel iş birliği, olay yönetimi ve kurtarma, yasal çerçeveler ve küresel bir siber güvenlik kültürü geliştirme yolları olmak üzere toplam yedi konu üzerinde çalışmaya davet etmiştir. He

ne kadar bu karar Rusya ve Çin'in desteğini alamamış olsa da her iki devletin de dâhil olduğu BM HUG'un 2015 Raporu, devletlerin iş birliğini geliştirme ve kapasite oluşturma çabalarının bu kararın hükümlerinden kaynaklanması gerektiğini tavsiye etmiştir (UNGA 70/174, 2015, Madde 21). Ayrıca devletler, küresel siber güvenlik kültürünün oluşturulması ve kritik bilgi altyapılarının korunması ilgili kararlar hakkında 2013 yılında kabul edilen 58/199 sayılı Genel Kurul kararını dikkate alarak kritik altyapılarını siber tehditlerden korumak için uygun önlemleri almaya çağırmıştır (Madde 13/g).Siber güvenlik kültürünü oluşturan unsurların bu şekilde genişletilmesi ve kritik altyapı sektörlerinin korunması ve siber güvenlik arasında ortaya çıkan bu bağlantı, Maurer (2011, s.44) ve Henderson'ın da (2015) işaret ettiği gibi uluslararası düzeyde kabul görmüş çeşitli unsurların ve ilkelerin ortaya çıkışını veya bir başka ifade ile kritik bilgi altyapılarının korunması üzerine inşa edilen düzenleyici uluslararası siber güvenlik rejiminin oluşumuna işaret etmektedir (s.471-72).

Üye ülkeler arasında güvenlik ve barışı korumak için bağlayıcı karar alma yetkisine sahip BM'nin en güçlü hükümetlerarası organı olan Güvenlik Konseyi'nin gündemine uluslararası siber güvenlik, siber terörizm ve hibrit savaşlar bağlamında son beş yılda giderek artan şekilde siber-fiziksel bilgi altyapılarının korunmasının sıklıkla gelmesi, bu alanda ortaya çıkmaya başlayan normun ilk işaretlerini vermektedir. Örneğin, 2015'te elektrik şebekelerini hedef alan devlet destekli siber saldırılara maruz kalan Ukrayna, 21 Kasım 2016'da düzenlediği bir Arria Formula toplantısı aracılığı ile BM Güvenlik Konseyi üyelerini terörist saldırılara karşı kritik bilgi altyapılarının korunması konusunda ilk kez bilgilendirilmiştir (SCR, 2016a). Bunu takip eden 28 Kasım 2016'daki İspanya ve Senegal tarafından organize edilen ikinci bir Arria Formula toplantısında siyasi veya askeri gerilimleri tırmandırmada devletlerin siberalan kullanım potansiyeli ve siberalanın fiziksel altyapısına bağlı kritik sektörlerdeki bilgi altyapısının korunması üzerinde durulmuştur *(*SCR, 2016b*).* Bir sonraki yıl, BM Güvenlik Konseyi, siber güvenliği önemli bir koruma unsuru olarak kabul eden kritik altyapıların terör saldırılarına karşı korunmasına ilişkin 2341 sayılı kararı kabul etmiştir (UNSC Resolution 2341, 2017). Kritik altyapıya veya temel hizmetlere yönelik siber saldırılara özel olarak atıfta bulunmayan karar, kritik sektörlerdeki bilgi altyapılarının ortaya çıkardığı yeni güvenlik endişelerinin oluşturduğu tehditlere ve güvenlik açıklarına atıfta bulunarak, kritik altyapıyı korumak için gerekli önlemler arasında siber güvenlikten bahsetmiştir. 2018'de, BM Güvenlik Konseyi Terörle Mücadele Komitesi Yürütme Direktörlüğü (UN CTED), INTERPOL ve BM Terörle Mücadele Ofisi ile iş birliği içinde, kritik altyapıyı terör saldırılarına karşı koruma, kapasite geliştirme ve en iyi uygulamaların teşviki için kritik altyapıların terör saldırılarına karşı korunması üzerine bir çalışma yayımlamıştır (UN CTED ve UN OCT, 2018). Kritik altyapının siber saldırılara karşı savunmasızlığı konusunda farkındalık yaratmak ve kritik altyapıyı bu tehdide karşı koruma ihtiyacı konusunda tartışmaları ilerletmek için 26 Ağustos 2020'de Estonya ve Endonezya tarafından düzenlenen son Arria Formula toplantısında siberalandaki sorumlu devlet davranışı normlarının, kritik altyapıyı nasıl koruduğu ve uluslararası barış ve güvenliğin korunmasına nasıl katkıda bulunduğu ve Güvenlik Konseyi'nin, bu sorunun ele alınmasında nasıl daha önemli bir rol oynayabileceği tartışılmıştır (SCR, 2020). Tüm bu gelişmeler, bir yandan kritik bilgi altyapılarının korunmasının uluslararası

barış ve güvenlik için giderek artan öneminin altını çizerken diğer yandan siberalanın devletler tarafından kullanımına ilişkin daha resmi bir tartışmanın gelecekte Güvenlik Konseyi gündeminde ortaya çıkmasının muhtemel olduğuna işaret etmektedir.

## 5. Ulusötesi Bir Tehdit Olarak Siber Suçlarla Mücadele

Siber suç, çevrimiçi olarak gerçekleşen veya siber teknolojinin saldırı için bir araç ve / veya hedef olduğu birçok farklı suç türünü ifade eden "şemsiye" bir terimdir ve siber bağımlı ve siber etkin suçlar olmak üzere ikiye ayrılır. Siber bağımlı suçlar, dijital bir sistemin hem hedef hem de saldırı araçları olduğu siberalanın fiziksel altyapısını bozmak için bilgisayar sistemlerine yapılan saldırıları veya kötü amaçlı yazılım kullanarak bir ağ üzerinden veri çalınması gibi suçları kapsamaktadır. Siber etkin suçlar ise siberalan kullanımıyla ölçek veya biçim olarak dönüştürülmüş çevrimdışında da işlenebilen uyuşturucu ticareti, insan kaçakçılığı ve çocuk pornografisi gibi geleneksel suçları ifade etmektedir. Bu kapsamda siberalanın kriminal kullanımı, özellikle de siber suçlara yanıt verecek normatif bir temel oluşturmaya yönelik çalışmalar, 2000'li yılların başından bu yana BM'nin Üçüncü Komitesi'nde, 2010 yılından itibaren BM Ekonomik ve Sosyal Konseyi'nde ve 2011 yılından itibaren Konsey'in işlevsel komisyonu olan Suç Önleme ve Ceza Adaleti Komisyonu'nda sürmektedir. Bu platformlarda siber suçlara ilişkin sürdürülen tartışmalar, uluslararası toplumda 2000'lerin başında görülen kısa süreli uzlaşının ileriki yıllarda yerini parçalanmaya bıraktığını ve uluslararası siber güvenlik bağlamında ortaya çıkan fay hatlarına benzer ayrılıkların siber suçlar konusunda da ortaya çıktığını gözler önüne sermektedir. Nitekim bilgi teknolojilerinin suiistimaline karşı mücadele konusunda Üçüncü Komite'de 2000 yılında kabul edilen karar, ABD tarafından diğer 38 devlet adına sunulmuş ve Rusya söz konusu karara ortak sponsor olmuştur (UNGA Report 55/593, 2000). Rusya ve ABD arasındaki 2000'lerin başında gözlemlenen kısa süreli iş birliğine işaret eden bu karara dokuz üye devlet daha sonra ortak sponsor olmuş, Çin ise katılmamıştır (UNGA Resolution 55/63, 2001). Bilgi teknolojilerinin kriminal kullanımıyla mücadele için yasal bir temel oluşturmayı amaçlayan karar, teknolojik gelişmelerin kriminal faaliyetler, özellikle bilgi teknolojilerinin suistimali için yeni olanaklar yarattığını vurgulayarak, bu sorunla mücadelede devletler ve özel sektör arasında iş birliği ihtiyacının altını çizmiş ve bilgi teknolojilerinin suistimaliyle mücadele etmek için bir dizi önlem sıralamıştır. Bu önlemler; bilgi teknolojilerini kriminal olarak kötüye kullananlar için güvenli sığınakların ortadan kaldırılması; devletler arasında kolluk kuvvetleri arasında iş birliği; bilgi paylaşımı; kolluk kuvvetleri personelinin uygun eğitimi; verilerin ve bilgisayar sistemlerinin gizliliğinin, bütünlüğünün ve kullanılabilirliğinin korunması ve kriminal kullanımın cezalandırılması; belirli kriminal soruşturmalarla ilgili elektronik verilerin korunması ve bunlara hızlı erişim; kanıtların zamanında incelenmesi ve bilgi teknolojilerinin kriminal kullanımına yönelik kanıtların değiş tokuşu; bu alanda suçluluğu önleme ve bunlarla mücadele etme ihtiyacı konusunda halkın farkındalığının artırılması; suçluların kötüye kullanımını tespit etmek ve önlemek, suçluları izlemek ve kanıt toplamak için bilgi teknolojilerinin tasarlanması ve bilgi teknolojilerinin suç olarak kötüye kullanımına karşı mücadelede hem bireysel özgürlüklerin ve

gizliliğin korunması hem de hükümetlerin bu tür suçlularla savaşma kapasitesinin korunmasını içermektedir (Madde 1, a-j).

Bunu takip eden bilgi teknolojilerinin suistimalini gözetlemeye ilişkin 2001'de kabul edilen Genel Kurul Kararı, ABD ve aralarında Rusya Federasyonu, Fransa, İsrail, Kore Cumhuriyeti ve Birleşik Krallık'ın da bulunduğu 73 diğer üye devlet tarafından Üçüncü Komite'ye sunulmuştur (UNGA Resolution 56/121, 2002). Sekiz üye devletin daha sonra sponsor olduğu Çin'in ise katılmadığı karar, BM Ekonomik ve Sosyal Konseyi'nin işlevsel komisyonu olan Suç Önleme ve Ceza Adaleti Komisyonu'nun yüksek teknoloji ve bilgisayarla ilgili suçlara karşı eylem planında öngörülen çalışmayı beklediğini ifade ederek, siber suçlarla mücadele konusunda BM'nin Üçüncü Komitesi'nden BM Ekonomik ve Sosyal Konseyi'ne ve Suç Önleme ve Ceza Adaleti Komisyonu'na büyük oranda kaymıştır.

Rusya, siber suçla mücadelede bilgi ve istihbarat alışverişi dâhil olmak üzere önemli ölçüde sınır ötesi iş birliğini mümkün kılacak küresel bir siber suç sözleşmesi konusunu 2010 yılında 12. BM Suç Önleme ve Ceza Adaleti Kongresi'nde gündeme getirmiş ancak kongreye katılan 45 ülke arasında ulusal egemenlik ve çevrimiçi hakların korunması konularına ilişkin yapılan müzakerelerde bir fikir birliği sağlanamadığı için ilerleme kaydedilememiştir. Bunun üzerine Suç Önleme ve Ceza Adaleti Komisyonu'nun himayesinde siber suç sorununa ilişkin kapsamlı bir çalışma yürütmek için açık uçlu bir hükümetlerarası uzman grubu kurulmuş ve aynı zamanda ABD, Avustralya, Kanada, Japonya, Norveç, Birleşik Krallık tarafından finanse edilen BM Uyuşturucu ve Suç Ofisi (UNODC) bünyesinde Siber Suçlar Küresel Programı faaliyete geçmiştir (UNGA Resolution 65/230, 2010). Bu, üye devletler tarafından bir referans belge olarak kullanılan Siber Suçlar Üzerine Kapsamlı Araştırma ile sonuçlanmıştır (UNODC, 2013). Siber suçlar ve devletler, uluslararası toplum ve özel sektör tarafından verilen yanıtlar üzerine çok paydaşlı bir çalışma yürütmek için 2011'de çalışmaya başlayan Siber Suçlar Uzman Grubu bugüne kadar toplam beş kere toplanmıştır.

Uzman grupta sürdürülen tartışmalara siber egemenler ve çok paydaşlılar diye tanımlayabileceğimiz iki devlet grubu arasındaki yeni bir küresel siber suç sözleşmesine gerek olup olmadığı konusundaki görüş farklılıkları damgasını vurmuştur. Çok paydaşlılar, Avrupa Konseyi'nin 2001 yılında kabul edilen ve 2004 yılında yürürlüğe giren ve siberalanı düzenleyen ilk yasal bağlayıcı antlaşma olan Budapeşte Siber Suç Sözleşmesini küresel iş birliği için sağlam bir başlangıç noktası olarak görmektedir. Toplam 65 devletin kabul ettiği sözleşme; Rusya, İrlanda, İsveç ve San Marino hariç olmak üzere neredeyse tüm Avrupa Konseyi Üye Devletleri tarafından onaylamış ayrıca ABD, Kanada, Avusturalya ve Japonya gibi Konsey üyesi olmayan devletler de kabul etmiştir. İlgili ülkelerin ulusal yasalarını uyumlu hâle getirerek ve soruşturma tekniklerini geliştirerek siberalandaki suçları ele almayı amaçlayan bu sözleşmenin 15. maddesi, sözleşmede ele alınan yetki ve usullerin uygulanmasının 1950 Avrupa Konseyi İnsan Hakları ve Temel Özgürlüklerin Korunması Sözleşmesi ve 1966 Sivil ve Siyasal Haklar Uluslararası Sözleşmesi'nde belirtilen yükümlülüklere uygun olduğunu özellikle belirtmektedir (Avrupa Konseyi, 2001).

Verilere sınır ötesi erişimi ulusal egemenliklerinin ihlali ve içerik gözetimini ulusal egemenliklerinin bir tezahürü olarak gören Çin ve Rusya'nın başını çektiği siber egemenler olarak adlandırdığımız devlet grubu, Budapeşte Siber Suç Sözleşmesi'nin devlet egemenliği ve müdahale etmeme ilkelerini ihlal ettiğini öne sürmektedir. Söz konusu devletler, özellikle Sözleşme'nin devletlerin verilere yasal sahibi izin verdiği takdirde hükümet onayına gerek kalmadan başka bir ülkede bilgi edinmesine izin veren 32 (b) maddesine ulusal egemenliklerinin ihlali olarak değerlendirerek karşı çıkmaktadır. Bu devletler ayrıca, hazırlanma sürecine dâhil olmadıkları bu Sözleşme'nin küreselden ziyade bölgesel nitelikte bir antlaşma olduğunu iddia ederek siber suçları düzenlemeye yönelik yeni bir küresel siber suç anlaşmasının kabul edilmesi için çalışmaktadır (Hakman, 2017; Walker, 2019). Söz konusu devletler, bu taleplerini Ekim 2016'da Birleşmiş Milletler Ulusaşırı Organize Suçla Mücadele Sözleşmesi Taraflar Konferansı'nda dile getirmiştir. BRICS devletleri, ayrıca 2017 Xiamen Bildirisi ile BM himayesi altında BİT'lerin cezai kullanımıyla mücadele konusunda evrensel düzenleyici ve bağlayıcı bir antlaşma yapılması gerekliliğini yinelemiştir (BRICS, 2017, para 56).

Siber suçlar konusunda çok taraflı bir anlaşma için BM'ye uzun süredir baskı yapan Rusya, Ekim 2017'de siber suçlarla mücadelede iş birliğine ilişkin yeni bir BM Konvansiyonu taslağını genel sekretere sunmuştur (UNGA A/C.3/72/12, 2017). Üye devletlerden gerekli desteği alamayan Rusya, bir sonraki yıl BM Genel Sekreterini suç amaçlı BİT kullanımına karşı koymanın zorlukları hakkında bir rapor hazırlaması için görevlendiren önergeyi Üçüncü Komite'ye iletmiştir (UNGA Resolution A/C.3/73/L.9/Rev.1, 2018). BİT'lerin suç amaçlı kullanımına karşı mücadele adlı Rusya, Çin, İran, Suriye, Azerbaycan gibi siber egemenler ve Hindistan ve Güney Afrika gibi iki devlet grubu arasında kalan devletlerin de sponsor olduğu önerge 94 ülke lehine, 59 aleyhte ve 33 çekimser oyla Genel Kurul'da kabul edilmiştir (UNGA 73/187, 2018). Bu kararın kabulü, BM Genel Kurulu'nun gelecek toplantılarına yönelik bir gündem maddesi oluşturarak yeni bir siber suç antlaşması için gerekli adımların atılmasını sağlamıştır.

Nitekim 5 Kasım 2019'da Üçüncü Komite, siber egemenler olarak adlandırılan aralarında Rusya, Çin, Küba, İran, Suriye ve Mısır gibi toplam 27 devletin ortak sponsor olduğu "BİT'lerin Kriminal Amaçlarla Kullanımına Karşı" başlıklı kararı kabul ederek, Genel Kurul'a yollamıştır (UNGA Resolution A/C.3/74/L.11/Rev.1, 2019). Genel Kurul'un 33 çekimser, 60 aleythe ve 79 lehte kabul ettiği önerge, BİT'lerin kriminal amaçlarla kullanımına karşı kapsamlı bir uluslararası sözleşme hazırlamak için tüm üye devlet temsilcilerinin katılacağı bir başka açık uçlu bir hükümetlerarası uzmanlar komitesinin kurulmasını içermektedir (UNGA Resolution 74/247, 2019). Siber egemenler dışında Hindistan, Endonezya, Malezya, Pakistan, Singapur, Güney Afrika, Tayland gibi iki devlet grubu arasında kalan bazı devletler tasarıya olumlu oy kullanırken; Brezilya, Türkiye, Meksika, Tunus gibi diğer arada kalan devletler ise çekimser oy kullanmıştır. Karara muhalefet esas olarak çok paydaşlılar olarak adlandırdığımız Avustralya, Kanada, Avrupa Birliği ve ABD'nin başını çektiği devletler grubundan gelmiştir. Karar, BİT'lerin kriminal amaçlarla kullanılması ile ne kastedildiğini net bir şekilde tanımlanmaması, siber bağımlı ve siber etkin suçlar arasında ayrım yapmaması, insan haklarına atıfta bulunulmaması, Suç Önleme ve Ceza Adaleti Komisyonu'nda devam eden çalışmaları dikkate almaması ve Avrupa Konseyi Siber

Suç Sözleşmesi'ne alternatif olarak siber suçlarla ilgili yeni bir küresel anlaşma yaratma girişimi olması açılarından eleştiriye maruz kalmıştır (Brown, 2019). Bu devletler grubu, ilgili kararın siber suçlarla mücadelede gelişmiş koordinasyonun gerekli olduğu bir zamanda uluslararası iş birliğini baltalayacağını savunurken insan hakları örgütleri ise otoriter ülkelere internet kesintileri ve sansür için yasal koruma sağlamayı, ifade özgürlüğünü suç sayma potansiyelini ve otoriter ülkelerin siyasi muhalefeti bastırmak için iş birliği yapmalarını kolaylaştıracak hükümler içermesi riskinden endişe duyduklarını ifade etmiştir (APC, 2019).

Açık uçlu hükümetlerarası uzmanlar komitesi, 60'ın üzerinde üye devletin yanıtlarını yansıtan "Bilgi ve İletişim Teknolojilerinin Kriminal Amaçlarla Kullanımına Karşı Çıkılması" başlıklı Genel Sekreter Raporu'nun yayınlanmasıyla çalışmalarına başlamıştır (UNGA Report 74/130, 2019). Bu bağlamda Ağustos 2020'de tartışmaya açılan rapor, Haziran 2024'te tamamlanana kadar uzmanlar komitesinin çalışmaları için bir çerçeve sağlayacaktır.

### 6. Çevrimiçi Gizliliğin ve Dijital Hakların Korunması

Dijital haklar; bireylerin dijital medya erişimine, kullanımına, oluşturmasına ve yayınlamasına veya bilgisayarlara, diğer elektronik cihazlara ve telekomünikasyon ağlarına erişmesine ve bunları kullanmasına izin veren insan hakları ve yasal hakları kapsamaktadır. Kavram, özellikle internet başta olmak üzere dijital teknolojiler bağlamında gizlilik hakkı ve ifade özgürlüğü gibi mevcut hakların korunması ve gerçekleştirilmesi ile ilgilidir. BM içinde bu konular Genel Kurul'un Üçüncü Komitesi ve Genel Kurul'un yan organı olan İnsan Hakları Konseyi'nde ele alınmıştır.[1] 2011'de dijital haklar konusunun İnsan Hakları Konseyine gelmesinden beri ABD bu konuda liderlik rolü üstelenerek Konsey'in internette insan haklarının geliştirilmesi, korunması ve kullanılmasını desteklemek için bir dizi karar almasında önemli rol oynamıştır. Başta ifade özgürlüğü olmak üzere kişilerin çevrimdışında sahip olduğu hakların çevrimiçi olarak da korunması gerektiğini benimseyen 20/8 sayılı İnsan Hakları Konseyi kararı, dijital haklara ilişkin ilk BM kararı olma özelliğini taşımaktadır (UN HRC 20/8, 2012). Karar, dijital haklara yönelik yeni tehditleri ele almak ve bu alandaki normları geliştirmek için iki yılda bir güncellenmiştir (UN HRC 26/13, 2014; UN HRC 32/13, 2016; UN HRC 38/7, 2018).

ABD'nin açık ve özgür internet söylemi üzerine kurulan dijital hakları destekleme çabaları, 2013 yılında Edward Snowden'in ABD'nin kitlesel gözetleme uygulamalarını ortaya çıkaran ifşaatları ile meşruiyet kaybına uğramış ve bu uygulamaların ana mağdurları olan Brezilya ve Almanya gibi ABD'nin geleneksel müttefiklerinin tepkilerini doğurarak BM'de gizlilik söyleminin başlamasına neden olmuştur (Deibert, 2015). Bu noktada Brezilya ve Almanya'nın ortak sponsor olduğu ve

1 İnsan Hakları Konseyi özel raportörleri internette insan haklarına yönelik olarak şu raporları hazırlamıştır: Çevrimiçi nefret söylemi (A / 74/486), yapay zekâ (A / 73/348), gözetim (A /HRC/41/35), çevrimiçi içerik düzenlemesi (A / HRC / 38/35), internet ve telekomünikasyon erişiminin sağlanmasında görev alan özel aktörlerin rolleri (A / HRC / 35/22), bilgi ve iletişim teknolojisi sektörünün ifade özgürlüğü ile ilişkili yönlerinin haritasını çıkarmak (A / HRC / 32/38), şifreleme ve anonimlik araçları (A / HRC / 29/32), gizlilik hakkı (A / 73/45712) ve dijital gözetimin terörle mücadele amaçları için kullanımı (A / HRC / 34/61).

BM'nin gizlilik ve gözetim hakkına ilişkin ilk büyük bildirisi olan 68/167 sayılı "Dijital Çağda Gizlilik Hakkı" (2013) kararı; iletişimlerin sınır ötesi gözetiminin, bunların dinlenmesinin ve kişisel verilerin yasadışı olarak toplanmasının, gizlilik hakkını ve ifade özgürlüğünü ihlal eden ve demokratik bir toplumun temellerini tehdit eden son derece müdahaleci bir eylem teşkil ettiğini vurgulayarak, devletlerin terörizme karşı aldığı tedbirlerin uluslararası hukuka uygun olmasını sağlama yükümlülüğünü ve Uluslararası Sivil ve Siyasi Haklar Sözleşmesi'nin 17. maddesi ile İnsan Hakları Evrensel Beyannamesi'nin 12. maddesinde yer alan gizlilik hakkı hükümlerini hatırlatmaktadır (UNGA Resolution 68/167 2013, Preamble). Karar, devletleri bu hakların ihlaline son vermek için tedbirler almaya ve iletişimlerin gözetimi ve dinlenmesinde ve kişisel verilerin toplanmasında şeffaflık ve hesap verebilirliği sağlayacak bağımsız ulusal gözetim mekanizmaları kurmaya çağırmaktadır. Karar, ayrıca BM İnsan Hakları Yüksek Komiserliği'nden ülke içi ve sınır ötesi gözetim ve/veya dijital iletişimin engellenmesi bağlamında gizlilik hakkının korunması ve geliştirilmesi hakkında bir rapor sunmasını talep etmiştir. BM İnsan Hakları Yüksek Komiserliği'nin toplu ölçekte dâhil olmak üzere kişisel verilerin toplanmasında gizlilik hakkının korunmasına ilişkin 27/37 sayılı raporu doğrultusunda (UNGA Report 27/37, 2014) devletlere verilerin toplanması ve ele geçirilmesinde "gizlilik hakkına saygı duyma ve koruma" çağrısında bulunan Genel Kurul tarafından kabul edilen ikinci karara, Rusya'nın içinde olduğu 66 devlet ortak sponsor olmuş, Çin ve Beş Göz devletleri olarak anılan ABD, Birleşik Krallık, Kanada, Avustralya, Yeni Zelanda ise katılmamıştır (UNGA Resolution 69/166, 2014). Söz konusu karar, kişisel bilgileri açığa çıkarma potansiyeline sahip üst verilere ve dijital iletişim gözetiminin yasal bir çerçeve temelinde yürütülmesi gerektiğine atıf yaparak, gizlilik hakkı ihlal edilen bireyler için etkili hukuk yollarına erişim çağrısında bulunmuş ve İnsan Hakları Konseyini gizlilik hakkının geliştirilmesi ve korunmasına ilişkin ilkeleri, standartları ve en iyi uygulamaları belirlemek ve açıklığa kavuşturmak için "özel bir prosedür" oluşturmaya davet etmiştir. Ayrıca ilgili karar, İnsan Hakları Konseyi'nin özel hayatın gizlilik hakkı konusunda üç yıl süre ile çalışacak bir Özel Raportör atamasını istemiştir (UN HRC Resolution 28/16, 2015).

Özel Raportör'ün 2018 yılında raporunu sunması ardından (UNGA Report 39/29, 2018), Genel Kurul 17 Aralık 2018'daki 73. oturumunda "Dijital Çağda Gizlilik Hakkı"na ilişkin yeni bir kararı konsensüs ile kabul etmiştir. Söz konusu karar, devletlerin bilgi ve istihbarat paylaşım anlaşmaları yoluyla toplanan verileri paylaşmaları veya başka bir şekilde bunlara erişim sağlamaları da dâhil olmak üzere gizlilik hakkıyla ilgili uluslararası insan hakları yükümlülüklerine saygı duymaları gerektiğini vurgulayarak, vatandaşların gizlilik hakkına yönelik herhangi bir müdahalenin yasallık, gereklilik ve orantılılık ilkeleriyle tutarlı olması gerektiğinin altını çizmektedir. Karar ayrıca yapay zekânın tasarımında, geliştirilmesinde, konuşlandırılmasında, kullanımında ve biyometrik bilgilerin toplanması, işlenmesi, paylaşılması ve saklanması sırasında gizlilik ve diğer insan haklarının dikkate alınması gerektiğini vurgulamaktadır (UNGA Resolution 73/179, 2018). Bu kararlar, genel olarak bağlayıcı olmamakla birlikte, dijital alanda uluslararası insan haklarına saygı göstermenin öneminin giderek daha fazla kabul edildiğini yansıtmakta ve devletlerin siberalandaki insan haklarına yönelik tehdit ve zorlukları ele alma istekliliğini göstermektedir

## 7. Sonuç

Soğuk Savaş sonrasında askeri kaynaklı tehditlerin giderek azalmasına karşın küreselleşme süreci ile birlikte bulaşıcı salgın hastalıklar, doğal afetler, iklim değişikliği, düzensiz göç hareketleri, küresel ekonomik krizler, uyuşturucu, silah ve insan kaçakçılığı gibi askeri olmayan tehditler artmıştır. Birey, toplum ve devletlerin refahını ve güvenliğini tehdit eden bu yeni sınır ötesi risklerin artması askeri savunma odaklı geleneksel güvenlik anlayışının genişlemesine ve derinleşmesine yol açarak yeni güvenlik yaklaşımlarının ortaya çıkmasına neden olmuştur. Söz konusu yeni güvenlik yaklaşımları, küreselleşen dünyanın bir yan ürünü olarak ortaya çıkan bu sınır ötesi risklerle etkin bir mücadelenin ancak devlet ve devlet-dışı aktörler arasında yakın alışveriş ve iş birliği ile mümkün olduğu üzerinde durmuş ve siber güvenlik konusunu bu kapsamda değerlendirmeye başlamıştır.

Bu bağlamda bu makale de siberalana yönelik ve siberalan aracılığı ile ortaya çıkan riskleri sınır tanımayan ulusötesi ve geleneksel olmayan güvenlik sorunlarından biri olarak ele almıştır. Her ne kadar geleneksel güvenlik sorunlarının aksine, birçok ulusötesi güvenlik tehdidiyle mücadele aynı derecede uyumlu uluslararası çabaları henüz ortaya çıkarmamış olsa da bu makale uluslararası siber güvenlik alanında gittikçe artan oranda uluslararası iş birliği arayışının ortaya çıktığını göstermiştir. BM Genel Kurulu'nun çeşitli komitelerinde yirmi yılı aşkın bir süredir devam eden tartışmalar, konu hakkında sayıları giderek artan Genel Kurul kararları ve bu kararların gittikçe yüksek oranla kabulü, siber suçlar ve siber savaş konularında oluşturulan uzman çalışma grupları, uluslararası şirketler ve sivil toplum gibi devlet dışı aktörlerin bu çalışmalara entegre edilmesi ve BM'nin en güçlü hükümetlerarası organı olan Güvenlik Konseyi'nin konuyu gündemine almaya başlaması, uluslararası toplumdaki iş birliği arayışına işaret etmektedir.

Bu makale, son yirmi yıldan beri BM'de süregelen siberalanı düzenlemeye yönelik faaliyetleri dört tematik başlık altında inceleyerek, BM'nin birçok farklı komitesinin ve departmanının siber risklerle başa çıkmak için geniş bir normatif çerçeve çizdiğini vurgulamıştır. Yeni ortaya çıkmakta olan bu norm, ilke ve standartların, uluslararası barışı ve sürdürülebilir kalkınmayı sağlamayı, siber suçlar gibi ulusötesi tehditlerle etkili bir şekilde mücadele etmeyi ve çevrimiçi gizlilik ve insan haklarını korumayı hedeflediği üzerinde durmuştur. Genel Kurulun Birinci Komitesi, BM HUG'lar ve 2019'da kurulan AUÇG, siber savaş riskini minimize etmek için devletlerin siberalan kullanımında bağlayıcı ve bağlayıcı olmayan normlarının uygulanması üzerine tartışmalar için merkezi bir platform görevi görmüştür. BM Genel Kurulu'nun tüm üyeleri 2010, 2013 ve 2015 yıllarında birbirini izleyen üç BM HUG raporunda siberalan kullanımından kaynaklanan çatışma risklerini azaltmak için uluslararası hukukun siberalana uygulanması, siberalan kullanımında devlet davranışına rehberlik edecek normların ve güven artırıcı önlemlerin geliştirilmesi ve devletlerin kendilerini yıkıcı veya dengesizleştirici siber faaliyetlerden daha iyi korunabilmelerini sağlamak için kapasite geliştirilmesi olmak üzere dört sütun üzerine kurulan çerçeveyi defalarca teyit etmiştir. Ayrıca kritik altyapı koruması konusunda BM HUG'lar tarafından referans noktası olarak görülen, küresel bir siber güvenlik kültürünün teşviki ve kritik altyapının korunmasına ilişkin Genel Kurul kararlarının

çerçevelenmesi için İkinci Komite önemli bir rol oynamıştır. Siberalanın kriminal kullanımı, özellikle de siber suçlara yanıt verecek normatif bir temel oluşturmaya yönelik çalışmalar, BM'nin Üçüncü Komitesi'nde, BM Ekonomik ve Sosyal Konseyi'nde ve Konsey'in işlevsel komisyonu olan Suç Önleme ve Ceza Adaleti Komisyonu'nda ele alınmaktadır. Bu platformlarda siber suçlara ilişkin devam eden tartışmaların Birinci Komite'deki uluslararası siber güvenlik tartışmalarında ortaya çıkan fay hatlarına benzer ayrılıkları doğurduğu gözlemlenmiştir. Siberalanın devlet kullanımlarından kaynaklanan insan hakları sorunlarının Üçüncü Komite ve BM Genel Kurulu'nun yan organı olan İnsan Hakları Konseyi'nde tartışılmıştır. 2013, 2014, 2015 ve 2018'de çevrimiçi gizlilik konusunda kabul edilen üç ayrı karar, kamu güvenliği ve ulusal güvenliği garanti etme amacına yönelik kısıtlamaların; meşru amaç, gereklilik ve orantılılık gibi mevcut uluslararası normların yanı sıra şeffaflık ve hesap verebilirlik gibi devlet sorumluluğu ilkeleri tarafından yönlendirilmesi gerektiğini vurgulamıştır.

Devletler arasında siberalandaki faaliyetleri düzenleme konusunda fark edilebilir bir ivme göze çarpsa da ortaya çıkan düzenleyici çerçevenin odağı ve siberalanı yönetmeye yönelik temel yaklaşımla ilgili olarak uluslararası toplumda net bir ayrım devam etmektedir. Nitekim uluslararası sistem açısından bakıldığında, siber normlar konusunda devletler arasında BM Genel Kurulu'nda süren müzakereler, küresel bir teknoloji devrimi karşısında 21. yüzyılın başlarında dünya siyasetinde meydana gelen daha geniş değişikliklerin bir izdüşümünü gözler önüne sermektedir. Soğuk savaştan sonra tartışmasız dünya hegemonu olarak ortaya çıkan ABD tarafından şekillendirilen küresel yönetişimdeki egemen konumunu koruma kararlılığı, Rusya'nın küresel aktör olma girişimleri ve Çin'in yeni dünya düzenini şekillendirme arzusu BM bünyesinde uluslararası siber savaş ve siber suç üzerine sürdürülen tartışmalarda net bir şekilde görülmektedir. BM HUG'da kabul edilen siberalanda sorumlu devlet davranışı normları ve kritik bilgi altyapılarının siber saldırılara karsı korunması üzerine inşa edilen ve İkinci Komite'de kabul edilen küresel bir siber güvenlik kültürü yaratmaya ilişkin kararlar, ABD'nin siberalandaki egemen konumunu koruma girişiminin bir aracı olarak görülebilse de BM Genel Kurulu'nun Birinci ve Üçüncü Komitesinde son birkaç yılda yaşanan gelişmeler Rusya ve Çin gibi yükselen güçlerin gündemlerini ilerletmek için prosedürel kuralları ve uygulamaları kullanma konusunda çok daha yetenekli hâle geldiklerini gözler önüne sermektedir. Hem siber suç hem de siberalan güvenliği hakkında Rusya'nın önerisi doğrultusunda açık uçlu hükümet uzman kuruluşlarının kurulmasıyla başlayan iki yeni süreç, siberalanın geleceği için birbiriyle yarışan vizyonları yansıtan bir forum işlevi görmesinin yanı sıra Rusya ve müttefiklerini yeni bir enformasyon güvenlik rejimi yaratma hedefine doğru yaklaştırmaktadır. ABD'nin siberalan üzerindeki hâkimiyetinin azalmasını ve gelecekteki parçalanmaya işaret eden bu geçişin, Çin'in bu tartışmada daha aktif bir rol üstlenip üstlenmeyeceği ve gelecekte siber normları nasıl şekillendireceği sorusunu da gündeme getirmektedir. Bu bağlamda, devletlerin diğer operasyonel alanlarda ve güç araçları arasında avantajlar yaratmak ve olayları etkilemek için siberalanı giderek daha fazla kullanacakları ve siberalanın 21. yüzyılın merkezi bir jeopolitik mücadele ve rekabet alanı olarak konumunu koruyacağı öngörüsünde bulunulabilir.

**Kaynakça**

ABD Ordusu Ortak Yayını JP 3-12 (2018). US Army Joint Publication JP 3-12 Cyberspace Operations, (CreateSpace Independent Publishing Platform, June 2018) https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf > (Erişim Tarihi: 10 Ocak 2021)

Afrika Birliği (2014). African Union Convention on Cyber Security and Personal Data Protection, June 27, 2014, https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection (Erişim Tarihi: 10 Ocak 2021)

ASEAN (2017). Preserving and Enhancing International Cyber Stability: Regional Realities and Approaches in ASEAN Report of the 2nd International Security Cyber Workshop Series, September 20-21, 2017, https://unidir.org/files/publications/pdfs/preserving-and-enhancing-international-cyber-stability-regional-realities-and-approaches-in-asean-en-778.pdf (Erişim Tarihi: 9 Ocak 2020)

Association for Progressive Communications (APC) (2019). Open Letter to UN General Assembly: Proposed International Convention on Cybercrime Poses a Threat to Human Rights Online, November 6, 2019, https://www.apc.org/en/pubs/open-letter-un-general-assembly-proposed-international-convention-cybercrime-poses-threat-human (Erişim Tarihi: 1 Şubat 2021)

Avrupa Birliği (2019). Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on Information and Communications Technology Cybersecurity Certification and Repealing Regulation (EU) No 526/2013 (Cybersecurity Act) PE/86/2018/REV/1, https://eur-lex.europa.eu/eli/reg/2019/881/oj (Erişim Tarihi: 1 Şubat 2021)

Avrupa Konseyi (2001). Convention on Cybercrime, 23 November 2001, https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185 (Erişim Tarihi 7 Temmuz 2020)

BRICS (2017). BRICS Leaders Xiamen Declaration, 5 September 2017, http://www.bricschn.org/English/2017-09/05/c_136583711_2.htm (Erişim Tarihi: 1 Şubat 2021)

Brown D. (2019). UN General Assembly Adopts Record Number of Resolutions on Internet Governance And Policy: Mixed Outcomes For Human Rights Online, APC, (10 January) https://www.apc.org/en/news/un-general-assembly-adopts-record-number-resolutions-internet-governance-and-policy-mixed (Erişim Tarihi: 9 Eylül 2020)

Budnitsky, S. ve Jia, L. (2018). Branding Internet Sovereignty: Digital Media and the Chinese–Russian Cyber Alliance, European Journal of Cultural Studies, 21(5), 594– 613. DOI: https://doi.org/10.1177/136.754.9417751151

Center for Strategic and International Studies (CSIS) (2018). Economic Impact of Cybercrime: No Slowing Down, https://csis-prod.s3.amazonaws.com/s3fs-public/publication/economic-impact-cybercrime.pdf (Erişim Tarihi: 9 Ağustos 2020)

Choucri N. (2012). Cyberpolitics in International Relations, The MIT Press.

Collier, David (2011). Understanding Process Tracing. PS: Political Science and Politics, 44 (4), 823-830, DOI: https://doi.org/10.1017/S104.909.6511001429

Cybersecurity Ventures (2020). Official Annual Cybercrime Report, https://cybersecurityventures.com/annual-cybercrime-report-2020/

Deibert R. J. ve Rohozinski R. (2010). Risking Security: Policies and Paradoxes of Cyberspace Security, International Political Sociology 4 (1) 15–32, DOI: https://doi.org/10.1111/j.1749-5687.2009.00088.x

Deibert, R. J., Rohozinski R. ve Crete-Nishihata M. (2012). Cyclones in Cyberspace: Information Shaping and Denial in the 2008 Russia–Georgia War, Security Dialogue 43 (1) 3–24,DOI: https://doi.org/10.1177/096.701.0611431079

Deibert R. J. ve Crete-Nishihata M. (2012). Global Governance and the Spread of Cyberspace Controls, Global Governance 18, 339-361, DOI: https://doi.org/10.1163/19426.720.01803006

Deibert R. (2015). The Geopolitics of Cyberspace after Snowden, Current History 114 (768) 9-15, DOI: https://doi.org/10.1525/curh.2015.114.768.9

Detsch, J. (2018). How Russia and Others Use Cybercriminals as Proxies, The Christian Science Monitor, (28 June), https://www.csmonitor.com/USA/2017/0628/How-Russia-and-others-use-cybercriminals-as-proxies

Feick, J. ve Werle, R. (2010). Regulation of Cyberspace. In R. Baldwin, M. Cave, & M. Lodge (Eds.), The Oxford Handbook of Regulation (Oxford: Oxford University Press) 523-547, DOI: doi.org/10.1093/ oxfordhb/978.019.9560219.003. 0021

Finnemore M. ve Hollis D B. (2016). Constructing Norms for Global Cybersecurity, The American Journal of International Law 110 (3) 425 – 479, DOI:https://doi.org/10.1017/S000.293.0000016894

G20 (2015). 'Leaders' Communiqué Antalya Summit' (2015) November 15-16 http://www.g20.utoronto.ca/2015/151116-communique.html > (Erişim Tarihi: 8 Eylül 2020)

G7 (2016). Principles and Actions on Cyber' (2016) https://www.mofa.go.jp/files/000160279.pdf > (Erişim Tarihi: 8 Eylül 2020)

G8 (2003). Principles for Protecting Critical Information Infrastructures, http://www.cybersecuritycooperation.org/documents/G8_CIIP_Principles.pd (Erişim Tarihi: 1 Şubat 2021)

GCSC (The Global Commission on the Stability of Cyberspace) (2018). 'Norm Package Singapore', (2018) Kasım https://cyberstability.org/wp-content/uploads/2018/11/GCSC-Singapore-Norm-Package-3MB.pdf > (Erişim Tarihi: 5 Ocak 2020)

GCSC (The Global Commission on the Stability of Cyberspace) (2019). 'Advancing Cyberstability Final Report' (2019) Kasım https://cyberstability.org/report/#6-norms > (Erişim Tarihi: 10 Ocak 2020)

Grigsby, A. (2017). The End of Cyber Norms, Survival 59 (6) 109-122, DOI: 10.1080/00396.338.2017.1399730

Hakman, J. (2017). Building a Stronger İnternational Legal Framework on Cybercrime, Chatham House, 6 June 2017, https://www.chathamhouse.org/expert/comment/building-stronger-international-legal-framework-cybercrime (Erişim Tarihi: 10 Ocak 2021)

Henderson C. (2015). The United Nations and the Regulation of Cybersecurity, Içinde Nicholas Tsagourias ve Russell Buchan, (der.), International Law and Cyberspace. Research Handbooks in International Law, (Edward Elgar) 465-490.

ISO/IEC 27032:2012 (2012). Information Technology — Security Techniques — Guidelines for Cybersecurity https://www.iso.org/standard/44375.html (Erişim Tarihi: 7 Şubat 2021)

ITU (2008). X.1205: Overview of Cybersecurity, https://www.itu.int/rec/T-REC-X.1205-200804-I (Erişim Tarihi: 5 Ocak 2021)

Kavanagh C. (2017). The United Nations, Cyberspace and International Peace and Security: Responding to Complexity in the 21st Century, UNIDIR, https://www.unidir.org/files/publications/pdfs/the-united-nations-cyberspace-and-international-peace-and-security-en-691.pdf (Erişim Tarihi: 1 Eylül 2020)

Kerr, J. A. (2018). Information, Security, and Authoritarian Stability: Internet Policy Diffusion and Coordination in the Former Soviet Region, International Journal of Communication 12, 3814–3834, DOI: 1932–8036/20180005

Maréchal, N. (2017). Networked Authoritarianism and the Geopolitics of Information: Understanding Russian Internet Policy, Media and Communication, 5 (1): 29–41 DOI: 10.17645/mac.v5i1.808

Maurer T. (2011). Cyber Norm Emergence at the United Nations, – An Analysis of the UN's Activities Regarding Cyber-security (2011), Belfer Center Discussion Paper #2011-11, https://www.belfercenter.org/sites/default/files/files/publication/maurer-cyber-norm-dp-2011-11-final.pdf > (Erişim Tarihi :8 Ağustos 2020).

Maurer T. (2019). A Dose of Realism: The Contestation and Politics of Cyber Norms, Hague Journal on the Rule of Law 1-23, DOI: 10.1007/s40803.019.00129-8

McKune, S. ve Ahmed, S. (2018). The Contestation and Shaping of Cyber Norms through China's Internet Sovereignty Agenda, International Journal of Communication 12, 3835–3855.

Microsoft (2020). Cyberattacks Targeting Health Care Must Stop, Nov 13, https://blogs.microsoft.com/on-the-issues/2020/11/13/health-care-cyberattacks-covid-19-paris-peace-forum/ (Erişim Tarihi: 10 Ocak 2021)

Mueller M. L. (2010). Networks and States: The Global Politics of Internet Governance, MIT Press.

Nocetti, J. (2015). Contest and Conquest: Russia and Global İnternet Governance. International Affairs, 91: 111-130, DOI:10.1111/1468-2346.12189

Nye, J. S. (2014). The Regime Complex for Managing Global Cyber Activities. Global Commission on Internet Governance Paper Series, https://www.cigionline.org/publications/regime-complex-managing-global-cyber-activities

OAS (2004). Resolution AG / RES. 2004 (XXXIV-O/04), titled "The Inter-American Integral Strategy to Combat Threats to Cyber Security," https://www.oas.org/juridico/english/cyb_pry_strategy.pdf (Erişim Tarihi: 10 Haziran 2020)

OECD (2002). Guidelines for the Security of Information Systems and Networks Towards a Culture of Security, http://www.oecd.org/sti/ieconomy/15582260.pdf (Erişim Tarihi: 10 Kasım 2020)

OECD (2008). Recommendation of the Council on the Protection of Critical Information Infrastructures (C(2008)35) [OECD/LEGAL/0361], http://www.oecd.org/sti/40825404.pdf (Erişim Tarihi: 10 Kasım 2020)

OECD (2019). Recommendation of the Council on Digital Security of Critical Activities, OECD/LEGAL/0456, https://www.oecd.org/sti/ieconomy/recommendation-on-digital-security-of-critical-activities.htm (Erişim Tarihi: 10 Kasım 2020)

OSCE (2016a). Permanent Council Decision No. 1202, OSCE Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the use of Information and Communication Technologies, https://www.osce.org/pc/227281?download=true (Erişim Tarihi: 11 Kasım 2020)

OSCE (2016b). Ministerial Council Decision No.5/16 – OSCE Efforts Related to Reducing the Risks of Conflict Stemming from the Use of Information and Communication Technologies. https://www.osce.org/files/f/documents/2/8/288086.pdf (Erişim Tarihi: 11 Kasım 2020)

OSCE (2017). Cyber Security for Critical Infrastructure: Strengthening Confidence Building in the OSCE – Conference of the Austrian OSCE Chairmanship 15 February 2017, Vienna, https://www2.osce.org/files/f/documents/5/1/298281.pdf (Erişim Tarihi: 11 Kasım 2020)

Oxford University (2020a). Oxford Statement on the International Law Protections against Cyber Operations Targeting the Health Care Sector, 21 May 2020, https://www.elac.ox.ac.uk/the-oxford-statement-on-the-international-law-protections-against-cyber-operations-targeting-the-hea (Erişim Tarihi: 11 Ocak 2021)

Oxford University (2020b). Second Oxford Statement on International Law Protections of the Healthcare Sector During Covid-19: Safeguarding Vaccine, 7 August 2020, https://www.elac.ox.ac.uk/article/the-second-oxford-statement (Erişim Tarihi: 11 Ocak 2021)

Pallin, C.V. (2017). Internet Control through Ownership: The Case of Russia, Post – Soviet Affairs, 33 (1):16-33,DOI: https://doi.org/10.1080/1060586X.2015.112.1712

Paris Call for Trust and Security in Cyberspace (2018, 12 November). https://www.diplomatie. gouv.fr/IMG/pdf/paris_call_text_-_en_cle06f918.pdf > (Erişim Tarihi: 9 Ocak 2020)

Risk Based Security (2020). Data Breach 2020 Q3 Report, https://pages.riskbasedsecurity.com/hubfs/Reports/2020/2020%20Q3%20Data%20Breach%20QuickView%20Report.pdf (Erişim Tarihi: 11 Ocak 2021)

RiskIQ (2020). The 2020 Evil Internet Minute, https://www.riskiq.com/resources/infographic/evil-internet-minute-2020/ (Erişim Tarihi: 11 Ocak 2021)

Ruhl, C., Hollis, D., Hoffman, W. ve Maurer T. (2020). Cyberspace and Geopolitics: Assessing Global Cybersecurity Norm Processes at a Crossroads. Carnegie Endowment for International Peace, https://carnegieendowment.org/files/Cyberspace_and_Geopolitics.pdf (Erişim Tarihi: 9 Ocak 2021)

Rusya Federasyonu (2000). Information Security Doctrine of the Russian Federation https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/Russia_2000.pdf > (Erişim Tarihi: 20 Kasım 2019)

Safshekan, O. (2017). Iran and the Global Politics of Internet Governance, Journal of Cyber Policy, 2 (2), 266-284, DOI: 10.1080/23738.871.2017.1360375

Schmitt M. (2017). Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, 2nd Ed., Cambridge University Press.

SCO (Shanghai Cooperation Organization) (2009). Agreement on Cooperation in the Field of International Information Security, (16 June) https://ccdcoe-admin.aku.co/wp-content/uploads/2018/11/SCO-090616-IISAgreement.pdf > (Erişim Tarihi: 15 Ocak 2020)

Security Council Report (SCR) (2016a). Open Arria-Formula Meeting on Counter-Terrorism , (21 November), https://www.securitycouncilreport.org/whatsinblue/2016/11/open-arria-formula-meeting-on-counter-terrorism.php (Erişim Tarihi: 20 Eylül 2020)

Security Council Report (SCR) (2016b). Open Arria-Formula Meeting on Cyber Security, (28 November), https://www.securitycouncilreport.org/whatsinblue/2016/11/open-arria-formula-meeting-on-cybersecurity.php (Erişim Tarihi: 20 Eylül 2020)

Security Council Report (SCR) (2020). Arria-formula Meeting on Cyber-Attacks Against Critical Infrastructure (26 August), https://www.securitycouncilreport.org/whatsinblue/2020/08/arria formula-meeting-on-cyber-attacks-against-critical-infrastructure.php (Erişim Tarihi: 20 Ocak 2021)

Tikk-Ringas, E. (2012). Developments in the Field of Information and Telecommunication in the Context of International Security: Work of the UN First Committee 1998-2012, ICT4Peace Publishing, https://citizenlab.ca/wp-content/uploads/2012/08/UN-GGE-Brief-2012.pdf (Erişim Tarihi: 7 Temmuz 2020)

UN CTED ve UN OCT (2018). The Protection of Critical Infrastructures Against Terrorist Attacks: Compendium Of Good Practices, https://www.un.org/sc/ctc/wp-content/uploads/2018/06/Compendium-CIP-final-version-120618_new_fonts_18_june_2018_optimized.pdf (Erişim Tarihi: 12 Ekim 2020).

UN Human Rights Council (HRC) Resolution 20/8 (2012). The Promotion, Protection and Enjoyment of Human Rights on the Internet, (16 July 2012), A/HRC/RES/20/8, https://undocs.org/A/HRC/RES/20/8

UN Human Rights Council (HRC) Resolution 26/13 (2014). The Promotion, Protection and Enjoyment of Human Rights on the Internet (26 July 2014), A/HRC/RES/26/13 https://daccess-ods.un.org/TMP/4319.375.15735626.html

UN Human Rights Council (HCR) Resolution 28/16 (2015). The right to privacy in the digital age (26 March 2015) A/HRC/RES/28/16, https://documents-dds-ny.un.org/doc/UNDOC/GEN/G15/068/78/PDF/G1506878.pdf?OpenElement

UN Human Rights Council (HRC) Resolution 32/13 (2016). The Promotion, Protection and Enjoyment of Human Rights on the Internet (1 July 2016), A/HRC/RES/32/13, https://daccess-ods.un.org/TMP/3695.021.56972885.html

UN Human Rights Council (HRC) Resolution 38/7 (2018). The Promotion, Protection and Enjoyment of Human Rights on the Internet, (5 July 2018), A/HRC/RES/38/7, https://undocs.org/A/HRC/RES/38/7

UN Office on Drugs and Crime (UNODC) (2013). Comprehensive Study on Cybercrime, New York. https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf

UNGA 65/201 (2010). Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, Note by the Secretary-General (30 July 2010), A/65/201 https://www.unidir.org/files/medias/pdfs/information-security-2010-doc-2-a-65-201-eng-0-582.pdf >

UNGA 66/359 (2011). Letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General, A/66/359, https://digitallibrary.un.org/record/710973>

UNGA 68/98 (2013). Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, Note by the Secretary-General (24 June 2013), A/68/98, https://www.unidir.org/files/medias/pdfs/developments-in-the-field-of-information-and-telecommunications-in-the-context-of-international-security-2012-2013-a-68-98-eng-0-518.pdf >

UNGA 69/273 (2015). Letter dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General, U.N. Doc. A/69/273, http://www.un.org/Docs/journal/asp/ws.asp?m=A/69/723 >

UNGA 70/174 (2015). Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, Note by the Secretary-General (22 July 2015), A/70/174, https://undocs.org/A/70/174 >

UNGA 72/327 (2017). Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, Report of the Secretary-General (14 August 2017), A/72/327 https://documents-dds-ny.un.org/doc/UNDOC/GEN/N17/257/46/PDF/N1725746.pdf?OpenElement >

UNGA A/C.3/72/12 (2017). Letter dated 11 October 2017 from the Permanent Representative of the Russian Federation to the United Nations addressed to the Secretary-General , https://undocs.org/A/C.3/72/12

UNGA Report 54/213 (1999). Report of the Secretary-General Developments in the Field of Information and Telecommunications in the Context of International Security (10 August 1999), A/54/213 https://undocs.org/A/54/213 >

UNGA Report 55/593 (2000). Report of the Third Committee 55/593, Crime prevention and criminal justice, (16 November 2000), A/55/593, https://undocs.org/A/55/593

UNGA Report 57/529/Add. 3 (2002). Report of the Second Committee 57/529/Add. 3, Macroeconomic policy questions: science and technology for development, (21 December 2002), A/57/529/Add. 3, https://undocs.org/A/57/529/Add.3

UNGA Report 58/481/Add.2 (2003). Report of the Second Committee 58/481/Add.2, Macroeconomic policy questions: science and technology for development, (15 December 2003), A/58/481/Add.2, https://undocs.org/A/58/481/Add.2

UNGA Report 64/422/Add.3 (2009). Report of the Second Committee 64/422/Add.3, Globalization and interdependence: science and technology for development, (15 December 2009) A/64/422/Add.3, https://undocs.org/pdf?symbol=en/A/64/422/Add.3

UNGA Report 27/37 (2014). Report of the Office of the United Nations High Commissioner for Human Rights, The Right to Privacy in the Digital Age, (30 June 2014), A/HRC/27/37 https://undocs.org/A/HRC/27/37

UNGA Report 39/29 (2018). Report of the United Nations High Commissioner for Human Rights 39/29, The right to privacy in the digital age, (3 August 2018), A/HRC/39/29, https://undocs.org/A/HRC/39/29

UNGA Report 74/130 (2019). Report of the Secretary-General 74/130, Countering the use of information and communications technologies for criminal purposes, (30 July 2019) A/74/130. https://undocs.org/A/74/130

UNGA Resolution 53/70 (1999). Developments in the Field of Information and Telecommunications in the Context of International Security, (4 Ocak 1999). A/RES/53/70, https://undocs.org/pdf?symbol=en/a/res/53/70 >

UNGA Resolution 55/63 (2001). [on the report of the Third Committee (A/55/593)], Combating the criminal misuse of information technologies, (22 January 2001) A/RES/55/63. https://undocs.org/en/A/RES/55/63

UNGA Resolution 56/121 (2002). [on the report of the Third Committee (A/56/574)] Combating the criminal misuse of information technologies, (23 January 2002), A/RES/56/121, https://undocs.org/en/A/RES/56/121

UNGA Resolution 56/19 (2001). [on the report of the First Committee (A/56/533)] , Developments in the Field of Information and Telecommunications in the Context of International Security, (7 January 2002 ), A/RES/56/19, https://undocs.org/A/RES/56/19 >

UNGA Resolution 57/239 (2002). [on the report of the Second Committee (A/57/529/Add.3)] Creation of a global culture of cybersecurity, (20 December 2002) A/RES/57/239 https://undocs.org/en/A/RES/57/239

UNGA Resolution 58/199 (2003). [on the report of the Second Committee (A/58/481/Add.2)]. Creation of a global culture of cybersecurity and the protection of critical information infrastructures, (23 December 2003), A/RES/58/199, https://undocs.org/en/A/RES/58/199

UNGA Resolution 64/211 (2009). [on the report of the Second Committee (A/64/422/Add.3)] Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures, (21 December 2009), A/RES/64/211, https://undocs.org/A/RES/64/211

UNGA Resolution 65/230 (2010). [on the report of the Third Committee (A/65/457)] Twelfth United Nations Congress on Crime Prevention and Criminal Justice (21 December 2010), A/RES/65/230, https://undocs.org/A/Res/65/230

UNGA Resolution 68/167 (2013). [on the report of the Third Committee (A/68/456/Add.2)]. The right to privacy in the digital age, (18 December 2013), A/RES/68/167, https://undocs.org/A/RES/68/167

UNGA Resolution 69/166 (2014). [on the report of the Third Committee (A/69/488/Add.2 and Corr.1)], The right to privacy in the digital age (18 December 2014) A/RES/69/166. https://documents-dds-ny.un.org/doc/UNDOC/GEN/N14/707/03/PDF/N1470703.pdf?OpenElement

UNGA Resolution A/C.3/73/L.9/Rev.1 (2018). Countering the use of information and communications technologies for criminal purposes, (2 November 2018), https://undocs.org/A/C.3/73/L.9/Rev.1

UNGA Resolution 73/179 (2018). [on the report of the Third Committee (A/73/589/Add.2)] The right to privacy in the digital age, (17 December 2018), A / RES / 73/179, https://undocs.org/en/A/RES/73/179

UNGA Resolution 73/187 (2018). [on the report of the Third Committee (A/73/590)] Countering the use of information and communications technologies for criminal purposes, (17 December 2018), A/RES/73/187, https://undocs.org/en/A/RES/73/187

UNGA Resolution 73/266 (2018). [on the report of the First Committee (A/73/505)] Advancing responsible State Behavior in Cyberspace in the Context of International Security, A/RES/73/266, https://undocs.org/A/RES/73/266 >

UNGA Resolution 73/27 (2018). [on the Report of the First Committee (A/73/505)] Developments in the Field of Information And Telecommunications In The Context Of International Security, (11 December 2018), A/RES/73/27 , https://undocs.org/A/RES/73/27 >

UNGA resolution 74/173 (2019). [on the report of the Third Committee (A/74/400)] Promoting technical assistance and capacity-building to strengthen national measures and international cooperation to combat cybercrime, including information-sharing (18 December 2019) A/RES/74/173 , https://undocs.org/pdf?symbol=en/A/RES/74/173

UNGA Resolution 74/247 (2019). [on the report of the Third Committee (A/74/401)] Countering the use of information and communications technologies for criminal purposes, ( 27 December 2019), A/RES/74/247 https://documents-dds-ny.un.org/doc/UNDOC/GEN/N19/440/28/PDF/N1944028.pdf?OpenElement

UNGA Resolution A/C.3/74/L.11/Rev.1 (2019). Countering the use of information and communications technologies for criminal purposes (5 November 2019) https://undocs.org/A/C.3/74/L.11/Rev.1

UN Security Council (UNSC) Resolution 2341 (2017) [on threats to international peace and security caused by terrorist acts], (13 February 2017), S/RES/2341 (2017), https://undocs.org/S/RES/2341(2017)

Walker, S. (2019). Cyber-Insecurities? A Guide to the UN Cybercrime Debate, Global Initiative Against Transnational Organized Crime, Geneva. https://globalinitiative.net/wp-content/uploads/2019/03/TGIATOC-Report-Cybercrime-in-the-UN-01Mar1510-Web.pdf (Erişim Tarihi: 15 Kasım 2020).

WHO (2020). WHO Reports Fivefold İncrease in Cyber Attacks, Urges Vigilance (23 April), https://www.who.int/news/item/23-04-2020-who-reports-fivefold-increase-in-cyber-attacks-urges-vigilance (Erişim Tarihi: 12 Ocak 2021).

World Economic Forum (WEF) (2020). The Global Risks Report 2020, Geneva, 2020 http://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf (Erişim Tarihi: 1 Ağustos 2020)

# The United Nations System and the Regulation of Global Cyberspace Security

**Tuba ELDEM***

Cybersecurity is a fairly new international issue. Two decades ago, it received little attention as an international problem and largely associated with the technical protection of computer systems. Over the last few years it has, however, risen on the global community's agenda as an important cross-border transnational issue posing significant economic, humanitarian, and national security risks. Like many other transnational and cross-border security challenges, cybersecurity risks, such as cyberattacks on critical infrastructure, cybercrime and cyberespionage, require significant collaboration and cooperation among different actors at different levels and across borders. Unlike traditional security challenges, many transnational non-traditional security threats have not yet produced the requisite coherent international efforts to tackle them, although – as this article shows – an emerging cooperative mitigating framework has emerged among states within the United Nations (UN).

Cybersecurity discussions in the UN started in 1998 with Russia's draft resolution on "Developments in the Field of Information and Telecommunications in the Context of International Security". However, cybersecurity gained significantly greater prominence on the UN's agenda over the last decade along with growing numbers of sophisticated computer network operations and cyber-enabled information operations carried out in or through cyberspace by both state-sponsored and non-state actors. Edward Snowden's revelations regarding the US-led Five Eyes spying alliance's use of cyberspace for espionage and mass surveillance in 2013, alongside the mounting economic cost and social damage of cybercrime, and the growing importance of cyber technologies for sustainable development further raised the issue of cybersecurity in the UN.

In this article, I examine the decisions and processes to regulate cyberspace in the UN system by addressing cybersecurity risks as a cross-border non-traditional security issue arising as a by-product of the globalizing world. I analyze ongoing norm-setting work within the three main Committees of the UN General Assembly (UNGA) to provide a thematic and holistic evaluation of the UN's highly fragmented cybersecurity regulatory activities. I also aim to identify emerging

* Fenerbahçe University, the Center for Applied Turkey Studies (CATS) of the German Institute for International and Security Affairs (SWP), E-mail: tuba.eldem@fbu.edu.tr

fault lines in international society concerning the regulation of global cyberspace by locating the challenges and sources of disagreement.

My analysis of the twenty-year-old negotiations among states about cyber norms reveals that the UN's efforts to regulate cybersecurity cover many issues, such as establishing formal and informal norms of behavior for state and non-state actors in cyberspace, protecting critical information infrastructures against cyber-attacks for sustainable development, creating legal mechanisms to address cross-border cybercrime, and securing privacy and human rights online. Several UN organs have been involved in cyber norm building processes. In particular, the UNGA's First Committee has been a central forum for key cyber powers, such as the U.S., China, and Russia, to discuss the information security threats. The adoption of three consensus reports by the UN Groups of Governmental Experts (GGEs) in 2010, 2013, and 2015 created a global cyber stability and resilience framework. This has four key pillars: the application of international law to cyberspace, the adoption of the norms of responsible state behavior in times of peace; the development of confidence-building measures to reduce cyber conflict; and capacity-building to enable states to better protect themselves from destructive or unbalancing cyberactivity. The Second Committee played an important role in framing resolutions on the promotion of a global culture of cybersecurity and the protection of critical information infrastructures within the context of sustainable development. This was later used as a reference point by the UN GGEs. The Third Committee, together with the Economic and Social Council, focused on strengthening the normative base for responding to transnational threats from the criminal use of the Internet and information and communication technologies. The Third Committee and Human Rights Council also addressed the right to online privacy, particularly human rights issues resulting from state (ab)uses of cyberspace and accepted a series of resolutions on the right to privacy in 2013, 2014, 2015 and 2018. These endorsed that restrictions for ensuring public safety and national security should be guided and limited by principles of state responsibility, such as transparency and accountability, as well as the norms and core principles of international law, such as legitimate aim, necessity, and proportionality.

While states have demonstrated increasing willingness to regulate cyberspace activities, I show that the international community remains clearly divided regarding the focus of the emerging regulatory framework and the basic approach to managing cyberspace. In particular, three main trends have shaped cyberspace regulation at the UN: a normative conflict between cyber powers over the nature of the international cybersecurity regime; the increasing power and influence of States in cyberspace; and a power shift from West to East in global cyberspace governance. Indeed, from the perspective of the international system, the ongoing inter-state negotiations on cyber norms at the UNGA reveal wider changes in world politics due to the global technology revolution. On the one hand, the resolution adopted in the Second Committee on creating a global cybersecurity culture and the norms adopted in the UN GEE consensus reports regarding responsible state behavior in cyberspace reflect US efforts to preserve its dominant position in global cyberspace governance; on the other hand, the recent developments in the First and Third

Committees reveal that rising powers like Russia and China have become much more capable of using procedural rules and multilateral diplomacy to advance their own agendas.

The establishment of open-ended expert groups on both cybercrime and cyberwar not only reflects competing visions for the future of cyberspace but also advances Russia's long-standing aim of creating a new information security regime based on multi-lateral treaties. This transition, which marks the decline of US hegemony, not only implies that global cyberspace governance will fragment further but also raises the questions of whether China will play a more active role in this debate and how its behavior will shape cyber norms in the future. I predict that cyberspace will maintain its central position as a new geopolitical competition area of the twenty-first century as states continue to use it to gain advantages and influence events in other operational areas and across the instruments of power.