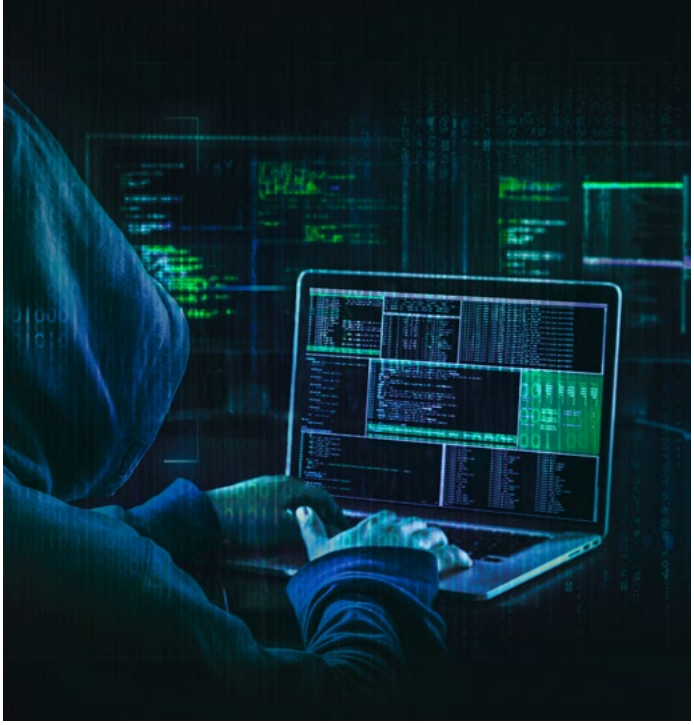
thinktech
STM Teknolojik Düşünce Merkezi

Rusya'nın Ukrayna İşgali Kapsamında Siber Savaşın Geleceği



İnsanlık tarihi çok çeşitli konularda savaşlara tanıklık etti. Ülkeler toprak ele geçirmek için, komutanlar kendilerini kanıtlamak için, liderler halklarını savunmak için savaşlarda kayıplar verdi. Tüm zamanlarda konvansiyonel savaşlar fiziksel hasarlara yol açarken günümüz teknoloji dünyasında gündemde olan yeni savaş türü ise sanal ortamda yarattığı etkiyle dikkatleri üzerine çekiyor. Siber savaş ülkeler üzerinde fiziksel kayıpların çok ötesinde bir etki yaratıyor.

İlk çağlarda basit silahlarla icra edilen savaşlar, gelişen silah teknolojisi doğrultusunda kapsamlı bir biçimde değişti. Bu değişim bir anda meydana gelmedi, yüzlerce yıllık bir sürecin sonucu olarak ortaya çıktı. Günümüzde pek çok ülkenin gündemini meşgul eden "siber savaş" bu sürecin son halkalarından birisi olarak dikkat çekiyor[1].

Siber Savaş ve Konvansiyonel Savaş Arasındaki Sınır

Günümüz teknolojileri bilgiye her yerden erişime imkân verirken siber riskleri de beraberinde getiriyor. Bu riskler bireysel olduğu kadar ülkelerin ulusal güvenliğini de tehdit edebiliyor. Geçmişte bir saldırıya verilen fiziksel karşı saldırılar yerine artık siber âlemde yapılan saldırılar daha güçlü sonuçlar doğurabiliyor. 2019 yılında İran'ın bir ABD keşif drone'unu yerden havaya füze sistemiyle düşürmesine ABD tarafından siber saldırıyla verilen cevap bu durumun en iyi örneklerinden biri olarak görülüyor. 131 milyon dolar değerinde bir drone'un kaybına karşılık ABD Siber Komutanlığı, İran'ın hava ve füze savunma sistemlerini kontrol eden bilgisayar sistemini siber saldırıyla etkisiz hâle getirerek İran'ı hava saldırılarına karşı tamamen savunmasız kıldı. Konvansiyonel bir saldırıya karşılık düzenlenen bu siber saldırı iki savaş âleminin sınırının giderek ortadan kalktığının işaretlerinden biriydi[2].

Konvansiyonel savaşlarda öncelik fiziksel hasarla karşıt güçlerin zayıflatılması veya etkisiz hâle getirilmesidir. Konvansiyonel harekâtların hemen öncesinde hedef ülkelerin; saldıran tarafından hava, kara ve deniz ateş destek unsurlarıyla baskı altına alınması bilinen bir savaş stratejisidir. Karşı tarafa baskı uygulanması ve önceden belirlenen kritik önemi olan hedeflerin etkisiz hâle getirilmesi saldıran taraf için büyük bir avantaj sağlarken savunma tarafında ise yıkıcı sonuçlar doğurabiliyor.

Konvansiyonel savaşlar sivil ve askeri can kayıplarıyla da sonuçlanıyor. Siber savaş ise temelde elektronik sistemlerin ve altyapıların etkisizleştirilmesiyle gücünü gösteriyor. Bu şekilde karşıt güçlerde can kaybı

1 https://dergipark.org.tr/en/download/article-file/1114311
2 https://www.secureworld.io/industry-news/cyber-war-vs-traditional-war

yaşanmadan da zayıflatıcı bir etki yaratılabiliyor. Konvansiyonel ve siber saldırıların bir arada kullanıldığı savaşlar ise hibrid savaşlar olarak adlandırılıyor.

Rusya'nın Ukrayna'ya yönelik işgal harekâtıyla birlikte "siber saldırıların" hibrid savaşın önemli bir unsuru olarak muharebe sahasının şekillendirilmesi faaliyetleri kapsamında kullanıldığı bir kez daha ortaya çıkıyor[3].

Bazı araştırmacılar siber savaşın gelecekte konvansiyonel savaşların yerine geçeceğini düşünüyor. Siber saldırı ekipmanlarının konvansiyonel araçlara oranla çok daha ekonomik olması, uzaktan kontrol edilmesi, etkili sonuçlar gösterirken can kayıplarının çok düşük tutulmasına sağladığı faydalar bu yeni savaş tekniğinin tercih edilmesinin öncelikli sebepleri arasında yer alıyor. Ülkelerin siber güçleri saldırılara karşı önemli bir caydırıcı etki de yaratıyor. Siber gücü yüksek ülkeler güçlü savunma teknikleriyle karşıt güçlerin saldırı teşebbüslerini hızla püskürterek, aldıkları önlemlerle yeni bir saldırı tehdidini de ortadan kaldırıyor.

Ancak siber savaş yönteminin yakın gelecekte konvansiyonel savaşın yerini alamayacağı düşüncesi daha ağır basan bir görüş olarak öne çıkıyor. Özellikle konvansiyonel savaşların sonucunda bir kazanan taraf olması ve kaybeden tarafın aldığı kalıcı hasarlar neticesinde yerine konulamaz insan ve ekipman kaybı ortaya çıkması savaşın sonlanmasında önemli bir etken olarak ortaya çıkıyor. Siber savaşta ise, karşı taraf aldığı hasarları teknolojik altyapı kapasitesi çerçevesinde belirli bir sürede onarabilirken bu savaş yöntemi genelde oyalayıcı veya erteleyici bir yöntem olarak görülüyor[4].

Aslında siber saldırılar hibrid savaş ortamında konvansiyonel savaşların daha hızlı sonuçlanmasına destek sağlayabiliyor. Teknoloji geliştikçe ve teknolojiye olan bağımlılık arttıkça siber savaşların kalıcı etkileri gelecekte artarak bu savaş tekniğinin güçlenmesini sağlayabilir. Ancak günümüzde konvansiyonel savaş aşamasına geçilmeden yapılan siber saldırılar karşılıklı cevaplarla uzun süre devam edebiliyor. Teknolojik gücü üstün olan taraf daha uzun süren etkili saldırılarla savaş sürecinde etkili olabiliyor. Siber savaşın konvansiyonel savaşa bir zemin hazırlamak için kullanımına gösterilebilecek en önemli örneklerden biri olarak Rusya ve Ukrayna arasında gerçekleşen karşılıklı siber saldırılar öne çıkıyor.

Rusya-Ukrayna Arasında Siber Savaş

Rusya'nın Ukrayna'ya karşı başlattığı siber savaş Kiev ile Moskova yönetimlerinin arası açılır açılmaz yoğunlaşmıştı. 2014-2018 yılları arasında stratejik devlet kurumlarının ve özel şirketlerin bilişim sistemleri Rus istihbarat servislerinin koordinasyonuyla bilgisayar korsanları tarafından hedef alındı[5].

Son altı yıldır Rusya'nın Ukrayna'ya yoğun siber saldırılar gerçekleştirdiği ve hatta siber silah cephaneliği için Ukrayna'yı test sahası olarak kullandığı biliniyor. Rusya'nın 2014'de Kırım'ı egemenliği altına almasının ardından Ukrayna'ya yönelik siber saldırılarında ciddi artış söz konusu oldu. 2015-2016 yıllarında Ukrayna'daki ana dağıtıcı elektrik santraline düzenlenen bir dizi siber saldırıda neredeyse çeyrek milyon Ukraynalı elektriksiz kaldı[6].

Rusya'nın bu yıl gerçekleştirdiği Ukrayna işgaliyle birlikte siber saldırılar daha da güçlendi. Bu süreçte Rusya'nın Ukrayna'ya uyguladığı tespit edilen 150 siber saldırının büyük çoğunluğu psikolojik etkileme hedefiyle gerçekleştirildi. Bu saldırılarda, Ukrayna Hükümeti ile vatandaşlarını yıldırmak ve direnişi kırmak amaçlanıyordu. Siber saldırıları izleyen uzmanlar savaş başladığından bu yana kritik altyapılara veya elektrik sistemlerine zarar verecek bir saldırı gerçekleşmediğini düşünüyor[7].

3 https://www.pugat.org/siber-guvenlik/2022/03/02/ukraynada-rus-isgali-ve-yaklasan-kuresel-siber-savas-riski/
4 https://www.cfc.forces.gc.ca/259/290/317/305/stimpson.pdf
5 https://setav.org/assets/uploads/2020/02/R152.pdf
6 https://www.aa.com.tr/tr/analiz/rusya-ukrayna-savasinin-siber-boyutu/2522079
7 https://www.dw.com/en/ukraine-cyberwar-creates-chaos-it-wont-win-the-war/a-60999197

STM ThinkTech'in yayınladığı "Siber Tehdit Durum Raporu Ocak Mart 2022"ye göre, Check Point Research rakamları, Rusya'nın 24 Şubat'ta Ukrayna'da başlattığı işgalin ilk günlerinde Ukrayna askeri ve devlet kurumlarına yönelik çevrimiçi saldırılarını yüzde 196 artırdığını ortaya koyuyor. Buna karşılık olarak Ukrayna, uluslararası duyarlılığı harekete geçirmeye ve Rusya'daki askeri ve kritik altyapı hedeflerine saldırmak için bir siber güvenlik uzmanları ordusu oluşturmaya çalışarak siber uzayda benzersiz bir strateji izledi[8].

Diğer taraftan Rusya'nın siber saldırılarına kayıtsız kalmayan Avrupa ülkelerinin, 2020 yılından itibaren Ukrayna'ya siber güvenlik gücünü artırması amacıyla yatırım yaptığı biliniyor. ABD Uluslararası Kalkınma Ajansı da yaptığı 38 milyon dolarlık yatırımla bu çalışmaları destekliyor.

Ukrayna işgal sonrasında siber saldırı ve savunma hatlarını ayırarak gönüllülük esasıyla vatandaşların da katılacağı bir oluşum başlattı. Ukrayna, siber saldırıları etkisizleştirmek için SpaceX'in kurucusu Elon Musk'tan gelişmiş uydu iletişim sistemi olan Starlink konusunda istediği desteğin olumlu karşılanmasıyla siber saldırılara karşı daha dirençli hâle gelmeye başladı[6].

Karşı saldırı olarak Anonymous ve Cyber Partizans gibi güçlü hacker grupları da Ukrayna'ya dışardan destek verdiler. Rus hükümet siteleri, devlet televizyonu ve askeri nakil hattı olarak kullanılan Belarus Demiryolu Ağı'na yapılan 1.500'ün üzerinde siber saldırı Ukrayna direnişini desteklemeyi amaçlıyor. Twitter sosyal medya ağında 7,4 milyon takipçiye sahip olan Anonymous'un yaptığı çağrıyla Ukrayna için ciddi bir siber karşılık fırsatı yarattığı biliniyor[9].

Ülkeler açık bir şekilde Rusya ile bir siber çatışmaya girmese de alternatif yöntemlerle Rusya ve Ukrayna arasında devam eden siber savaşa Ukrayna tarafında destek vermeye devam ediyor. Küresel bir siber savaşın başlamaması için hassas dengelerle yönetilen siber savaş ortamı gelecekte daha da genişleyecek gibi görünüyor.

Siber Savaşta Yeni Yöntemler

Siber saldırılar modern savaş teknolojisinin bir parçası hâline geldi. Bunlar bir yandan psikolojik etkilerle moral bozma ve dezenformasyon amacı taşırken, diğer yandan askeri girişimlerde etkili sonuçlar alınmasını sağlıyor. Öncelikle yapılan siber saldırılar karşıt güçlerin direncini ciddi oranda zayıflatarak konvansiyonel bir saldırıya gerek kalmadan teslim olunmasını sağlayabilirken, olası bir çatışmada ise psikolojik olarak yıpratılan tarafın direnci daha hızlı kırılabiliyor[10].

Rusya-Ukrayna savaşında Rusya'nın gerçekleştirdiği tespit edilen siber saldırılar arasında çeşitli siber savaş yöntemleri dikkat çekiyor. Wipers adı verilen ve hedef sistemdeki bütün veriyi yok eden silici saldırı yöntemi, web sitelerini kullanışsız hâle getiren DDoS saldırı yöntemi ve Yanıltma/Sahte Haber Yayma yöntemi tespit edilen yöntemler arasında bulunuyor[7].

Ülkeler karşıt güçlerin siber kabiliyetlerini yakından izliyor. Siber aktiviteleri izlemek için kurulan organizasyonlar ise çeşitli risk değerlendirmeleriyle gelecek siber saldırılara karşı hazırlık yapmayı hedefliyor. ABD'nin Ulusal İstihbarat Topluluğu Tehlike Analiz Raporu'na göre, Rusya siber savaş unsurları da oldukça yüksek riskli bir konumda tutuluyor. Raporda özellikle Rusya gibi ülkelerin kendini küçük gören veya ciddiye almayan ülkelere karşı aktif siber operasyonlar düzenlediği, gazetecilerin hack'lenmesi, bilgi sızdırılması ve çeşitli organizasyonlardan bilgi çalınması için girişimlerde bulunduğu belirtiliyor. Rapordan anlaşıldığı üzere, siber savaş yöntemleri arasında aktif savaş operasyonlarından farklı olarak, istihbarat, casusluk veya gündem yaratma/değiştirme faaliyetleri de bulunuyor[11].

8 https://thinktech.stm.com.tr/tr/siber-tehdit-durum-raporu-ocak-mart-2022
9 https://www.cnbc.com/2022/03/01/how-is-anonymous-attacking-russia-disabling-and-hacking-websites-.html
10 https://www.dw.com/tr/rusyan%C4%B1n-ukraynaya-kar%C5%9F%C4%B1-siber-sava%C5%9F%C4%B1/a-60946766
11 https://www.dni.gov/files/ODNI/documents/assessments/ATA-2022-Unclassified-Report.pdf

Ülkelerin siber savaş unsurlarına karşı ortaklaşa hareket planları da bulunuyor. NATO siber âlemi bir savaş alanı olarak tanıyor. Siber Bilgi ve İstihbarat Paylaşım Girişimi, ortakları arasında bir otomasyon platformu üzerinden bilgi paylaşımına imkân verirken, Siber Savunma İttifakı Asya finansal pazarları ve İngiltere güvenlik kuvvetleriyle kâr amacı gütmeyen ortaklaşa bir siber platform üzerinde çalışıyor[12].

Konvansiyonel savaşlara karşı kurulan ittifakların siber savaşa karşı da oluşması, siber âlemde yaşanacak çatışmaların gelecekte artma potansiyelinin ne kadar ciddiye alındığına bir işaret olabilir.

Siber savaşta saldırı yöntemleri ve amaçlarının yanında savunma amaçlı uygulamalar da önem kazanıyor. Sıfır güven politikasıyla bağlanan her cihaz ve yazılıma kuşkuyla bakılması ve güvenlik istisnası sunulmaması savunma hattının ilk basamağını oluşturuyor. Mobil cihazların hızla arttığı günümüzde uzaktan bağlantıların yarattığı riskle düşman veya dost bağlantıların ayırt edilme zorluğu sıfır güven politikasını güçlendiriyor[13].

Rusya-Ukrayna Savaşı Siber Savaşların Geleceğini Nasıl Etkiliyor?

Tüm dünyanın yakından takip ettiği Rusya-Ukrayna savaşı, insan hayatını birçok alanda olumsuz etkiliyor. Kurumlar ve ülkeler savaşa ambargolarla tepki gösterirken, siber dünyadaki dijital varlıkların da risk oluşturan yeni gelişmelere karşı hazırlıklı olması gerekiyor. Rusya gösterilen tepkilere cevap olarak Avrupa'daki varlıklarını ve yatırımlarını geri çekerken, bir siber saldırıyla özellikle tepki gösteren ülke ekonomilerinde zarara neden olacak karşılıklar verebilir. Bu olasılıktan yola çıkarak oluşturulan siber güvenlik platformunda 1.500'den fazla bağımsız siber güvenlik uzmanı şirketlerin ve ülkelerin sistemlerini 7/24 denetleyerek, bulunan yeni güvenlik açıklarını kısa sürede kapatmayı öneriyor[14].

Rusya savaşta siber saldırı tekniklerini şimdilik en düşük seviyede uygulamayı tercih ediyor. Bunun nedeninin hem kabiliyetlerini test etmek istemesi hem de diğer ülkelerin Ukrayna siber savunmasına destek vermesi nedeniyle daha güçlü bir siber savaş alanının ortaya çıkması durumunda gerçek gücünü göstermek istemesi olduğu düşünülüyor. Siber saldırıların sonuçları fiziksel hasarlara da yol açabiliyor. Mevcut savaşta şimdilik böyle bir saldırı şekli görülmemiş olsa da küresel bir siber savaşın tetiklenmemesi için bütün taraflar uluslararası kanunlarca belirlenmiş savaş sınırlarını ihlal etmemeye özen gösteriyor. Kuzey Atlantik Antlaşması Örgütü (NATO) Antlaşması'nın 5. maddesine göre, herhangi bir üyeye yapılacak bir saldırı bütün üyelere yapılmış sayılıyor. Siber güvenlik uzmanlarına göre ise Rusya'nın siber savaş kabiliyetleri ABD, Çin ve İngiltere'nin gerisinde kalıyor. Bu nedenle uluslararası antlaşma ve kanunların ihlali, Rusya'yı altından kalkamayacağı bir cepheye sürükleme potansiyeli taşıyor[15].

Bu durum siber savaşın ortaya çıkması için kanunların, ittifakların ve kabiliyetlerin çok iyi analiz edilmesi gerekliliğini ortaya koyuyor. Herhangi bir ülke veya organizasyonun bir siber operasyon için gelecek adımlarını da öngörerek bir savaş planı oluşturması gerekiyor. Teknoloji ve altyapı yeterli olsa bile kaynakların yetersizleşmesi ve küresel ittifakların oluşturulması siber savaşın seyrini saniyeler içinde değiştirme olasılığı yaratıyor. Siber savaşın geleceğinde teknolojik altyapının yanı sıra, normalde konvansiyonel savaşlarda daha yoğun olarak görülen stratejik planlama ve operasyon yönetimi de önem kazanıyor. Rusya-Ukrayna savaşı bu görüşlerin benimsenmesi ve test edilmesi için iyi bir örnek oluşturuyor.

Siber savaşlar, doğrudan ve doğrudan olmayan saldırı yöntemleriyle uygulanabiliyor. Doğrudan olmayan saldırı yöntemlerinde bilgisayarlar ve kişiler yerine enerji nakil hatları, su şebekeleri, iletişim ve ulaştırma sistemleri hedef alınabiliyor. Bu şekilde ciddi bir kaynak sıkıntısı ortaya çıkıyor. Doğrudan olmayan saldırı yöntemlerine

12 https://www.forbes.com/sites/forbestechcouncil/2022/02/24/its-2022-is-the-global-cyberwar-finally-inspiring-a-collective-response/?sh=48fca70e1047
13 https://www.forbes.com/sites/louiscolumbus/2020/03/28/cyber-warfare--truth-tactics-and-strategies-is-a-good-read/?sh=be61adc1d3fe
14 https://www.globaltechmagazine.com/2022/03/22/rusya-ve-ukrayna-arasindaki-siber-savas-dunyayi-etkiliyor/
15 https://www.nature.com/articles/d41586-022-00753-9

karşı güçlü güvenlik duvarlarının yanı sıra bağımsız internet altyapılı yedek sistemler etkili olabiliyor. Ayrıca etkilenecek sistemlerde hizmetin devam ettirilmesi için yedek hatlar veya kaynaklar kurgulanması da önemli bir savunma aracı olarak değerlendiriliyor.

Doğrudan yapılan siber saldırılar kişilerin veya kurumların gizli veya kritik altyapı bilgilerinin çalınması, silinmesi veya değiştirilmesi şeklinde uygulanabiliyor. Bu saldırı yöntemi ciddi psikolojik baskı kurmak veya şantaj amaçlı kullanılabiliyor. Doğrudan yapılacak saldırılara karşı güçlü şifreleme sistemleri, sıfır güven politikası gibi hep şüpheyle yaklaşılan siber güvenlik uygulamaları, güncel yazılım kullanımı, çalışanların ve toplumun teknoloji risklerine karşı eğitilmesi gibi önlemler faydalı olabiliyor[16].

Siber savaşlar belirli sınırları olan savaş alanlarına benzemediğinden siber âlemde sınırların iyi bir şekilde belirlenmesi de gerekiyor. Ülkeler ve hacker'lar siber âlemi kullanmak için dünyanın çeşitli yerlerinden farklı sunucuları kullanarak siber saldırılar gerçekleştirebiliyor. Bazen bu durum sunucuların topraklarında konuşlandırıldığı ülkelerin kanunlarına aykırı olabileceği gibi bu ülkeleri siber savaşın içine çekme riski de yaratıyor.

Çin bu gibi durumlarla sıklıkla karşılaşan bir ülke olarak biliniyor. Çin Dışişleri Bakanı tarafından yakın zamanda yapılan bir açıklamada, özellikle ABD'nin hacker'ları tarafından Çin'de bulunan bilgisayarların hack'lenerek bu sistemlerden Rusya'ya siber saldırılar gerçekleştirildiği belirtiliyor. Benzer şekilde Almanya ve Hollanda'nın da Çin sunucularını hack'lediği ve bu sunucuların yüzde 87'sinin Rusya'ya siber saldırı gerçekleştirmek amacıyla kullanıldığı bildiriliyor. Çin özellikle siber operasyonlarda aracı olarak kullanılmaktan duyduğu rahatsızlığı dile getirirken, bu durumun devamı hâlinde küresel ölçekte başka sorunların ortaya çıkabileceğinin işaretini veriyor[17].

Siber savaş hassas dengelerle yönetilmesi gereken bir cephe olarak her geçen gün daha fazla önem kazanıyor. Siber âlem sınırsız bir alan sunarken, bu alanda yapılacak faaliyetlerin sonuçları ve kimler üzerinden gerçekleştirileceği siber savaşın geleceği için önemli bir unsur olarak ortaya çıkıyor. Yapılacak basit hataların veya iyi planlanmayan bir siber saldırının karşılığı çok ağır olabileceği gibi küresel ölçekte bir prestij ve güven kaybına da neden olabilir. Geleceğin siber savaşlarının bu ve benzeri birçok kriterin titizlikle düşünülerek yönetilmesi gerekiyor.

Siber yeteneklerin geleceğin harp ortamında ciddi sonuçlar yaratacağı kesin görünse de henüz silahlı çatışma hukuku kapsamında tam anlamıyla karşılanabilecek bir siber savaş eşiğinin geçildiğini söylemek mümkün görünmüyor. Aynı şekilde, ofansif siber yeteneklere ilişkin düzenleyici bir uluslararası mekanizmanın kurulması ve bir onaylama rejimi oluşturulması hususlarında da ülkelerin kurduğu ittifaklar ve çalışmalar umut vadediyor. Ülkeler henüz kendi iletişim ve bilgisayar altyapısını uluslararası kontrole açmak konusunda istekli görünmüyor. Ek olarak, başta ABD olmak üzere, teknolojik yetenekler konusunda önemli üstünlükler yakalamış ülkelerin imkân ve kabiliyetlerini dış kullanıma açık olacak şekilde bir uluslararası pazarlık konusu yapmaları beklenmiyor[18].

Siber savaşların yaşanmaması, siber silahsızlanma, bireysel ve kamu güvenliğinin siber âlemde sağlanması ve kritik altyapıların korunması için hızlı bir şekilde güç sahibi ülkelerin bir araya gelerek ittifaklar oluşturması ve yasal düzenlemeler ile küresel bir antlaşmaya imza atması önem kazanıyor. Teknoloji geliştikçe bireysel olarak veya ülkelerin kontrolünde gerçekleşen siber saldırıların devam etmesi muhtemel görünüyor.

16 https://hbr.org/2022/03/what-russias-ongoing-cyberattacks-in-ukraine-suggest-about-the-future-of-cyber-warfare?utm_medium=email&utm_source=newsletter_monthly&utm_campaign=strategy_not_activesubs&deliveryName=DM180552
17 https://theparadise.ng/china-warns-us-over-cyber-attacks-targeting-russia/
18 https://edam.org.tr/siber-savas-gelecegin-askeri-gercekligi-ve-gunumuzun-bilimkurgusu-arasinda/