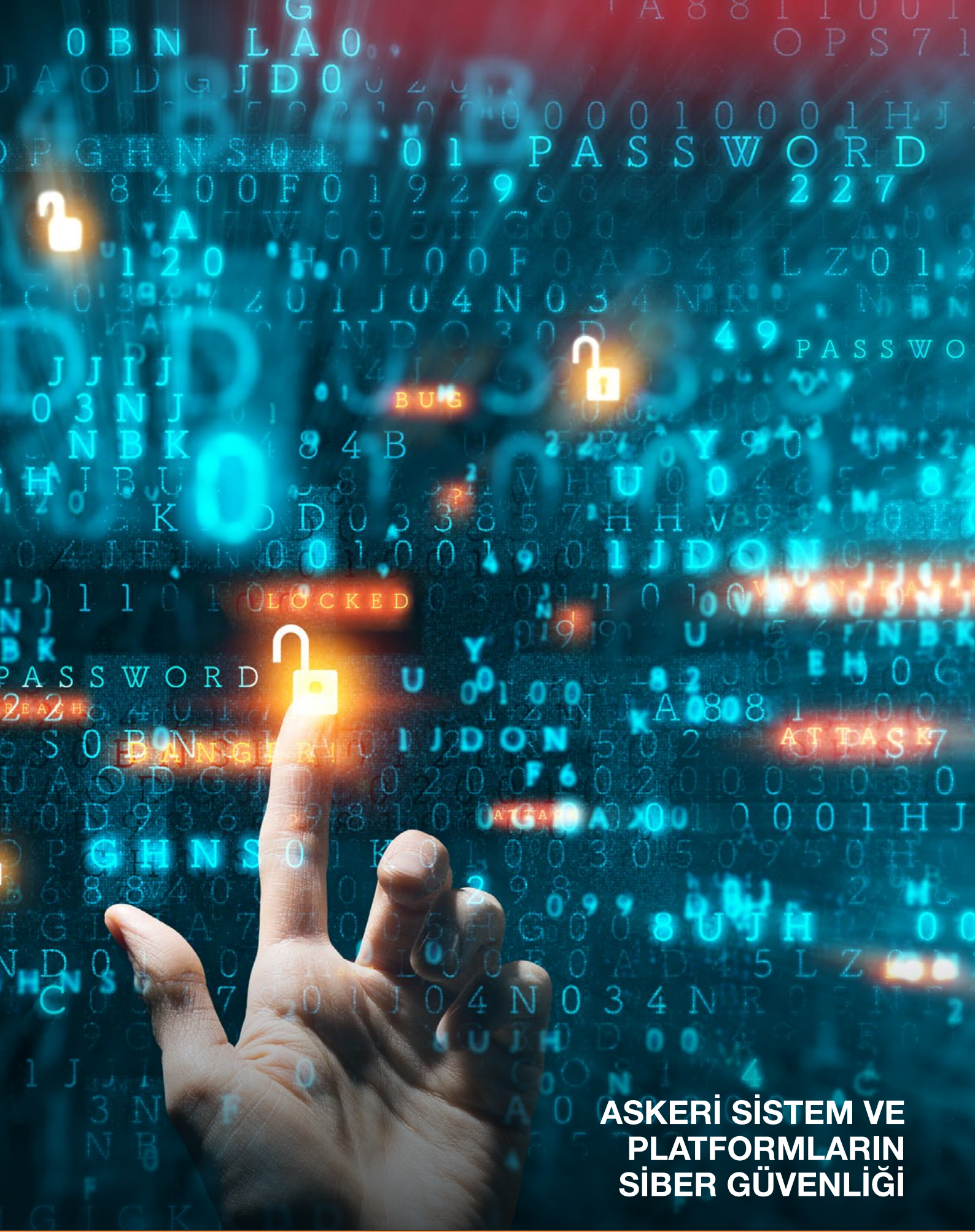
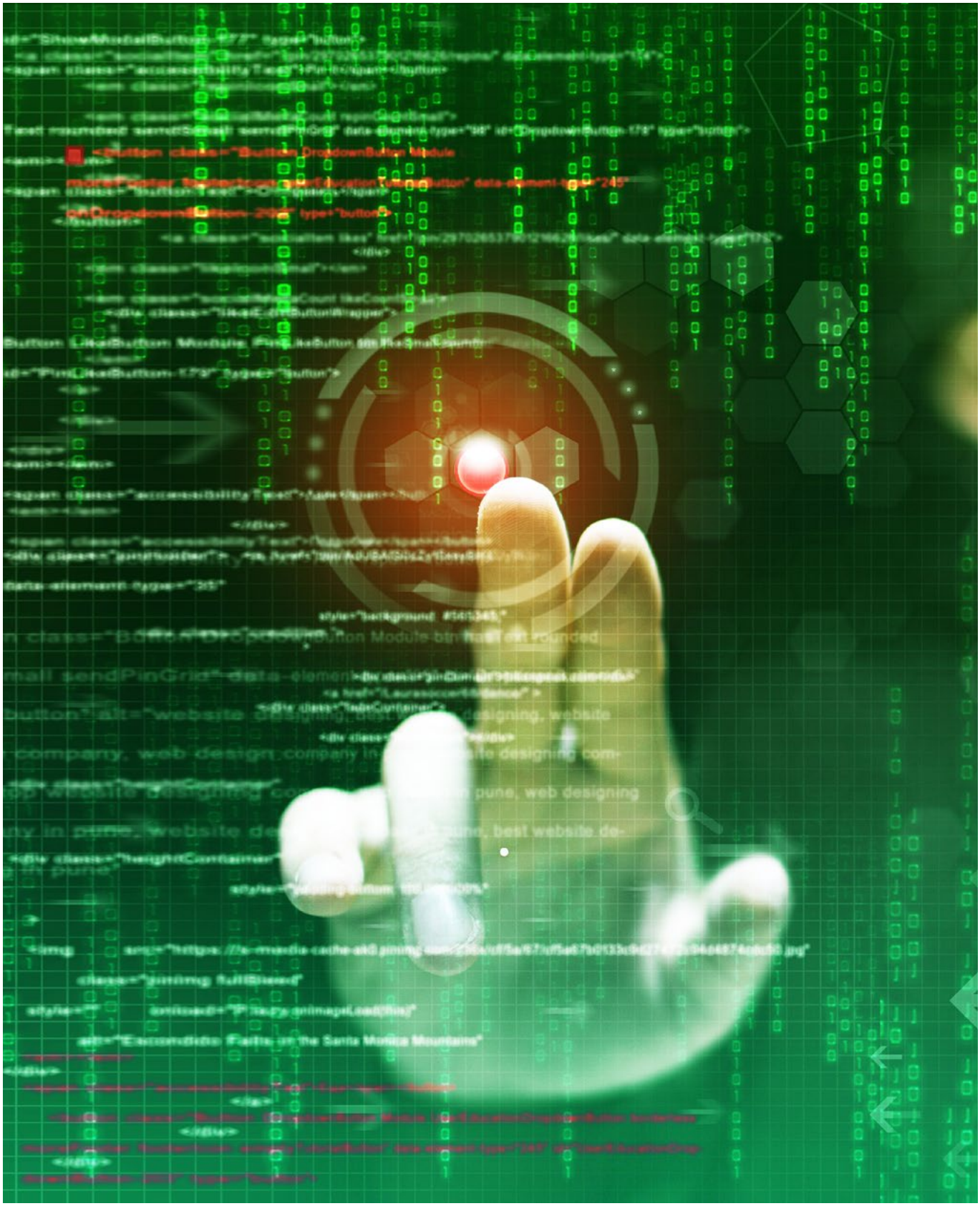


ASKERİ SİSTEM VE PLATFORMLARIN SİBER GÜVENLİĞİ

TREND ANALİZİ MART 2021

thinktech
STM Teknolojik Düşünce Merkezi



STM ThinkTech

1. GİRİŞ

Hayatın hemen her alanında merkezi bir rol edinmiş olan bilgi ve iletişim teknolojileri sağladığı geniş imkânlar yanında güvenlik risklerini de beraberinde getirmektedir.

1990'lardan itibaren devletler beşinci boyut olarak değerlendirilen siber uzayın sağladığı imkânları askeri kapasitelerini geliştirmede yeni bir fırsat olarak görmüştür. Bu doğrultuda uluslararası sistemde küresel ve bölgesel güç konumunda olan birçok devlet, hatta uluslararası örgütler, kendi siber savunma ve saldırı yeteneklerini artırmak amacıyla siber güvenlik stratejileri ortaya koymaya başlamıştır.

Bugün siber güvenlik, farklı kurumların sorumluluklarıyla kesişen çok boyutlu ve stratejik olarak ele alınması gereken bir konu hâline gelmiştir. Ancak her şeyden önce bir güvenlik meselesi olması nedeniyle askeri boyutu önemini korumaktadır.

Analizimizde öncelikle siber güvenlik kavramı ve olgusu değerlendirilerek, askeri sistem ve platformların karşı karşıya kalabileceği siber tehditler ile bu alanda öne çıkan yeni teknolojilere değinilecek, ayrıca güncel siber güvenlik stratejileri gözden geçirilecektir.

2. SİBER GÜVENLİK NEDİR?

Siber güvenlik, sistemlerin, ağların, programların, cihazların ve verilerin çeşitli teknolojiler, uygulamalar ve kontrol yöntemleriyle siber saldırılara karşı korunmasıdır. Siber güvenliğin hedefi sistemlerin, ağların ve teknolojilerin izinsiz etkenlere karşı zaaflardan korunmasını sağlamak ve siber saldırı risklerini azaltmak olmalıdır[1].

Siber güvenlik aynı zamanda bilgi teknolojilerinin güvenliği olarak da düşünülmektedir. Siber güvenlik ile ilgili çalışmalar yapılırken ağ, uygulama, veri, bulut güvenliği ile birlikte mobil cihazların güvenliği, kimlik yönetimi ve uzaktan erişim sistemlerinin güvenliği bir bütün olarak düşünülmelidir[2].

Siber güvenlik ağırlıklı olarak sivil uygulamalarda değerlendirilse de bütün vatandaşların ve ülkenin genel güvenliğinden sorumlu silahlı kuvvetlerin de siber uzayda varlığını güçlendirmesi önemlidir. Gelecekte meydana gelecek savaşların dijital platformlarla desteklenerek devam edeceği düşünüldüğünden askeri uygulamalar siber uzayın güvenliğinde çok önemli bir rol oynamaktadır[3].

3. SİBER SALDIRI YÖNTEMLERİ

Dijital teknolojilerin evrilmesiyle siber tehditlerde de ciddi artışlar yaşanmıştır. Siber suçlular karmaşık, savunması güç ve güçlü saldırılarla şehirlerin elektrik enerjilerini kesmek, askeri teçhizatlara zarar vermek ve ulusal güvenlik sırlarına sızmak gibi birçok saldırı yöntemi uygulamaktadır.

Siber savaş, bir devletin altyapısını istikrarsızlaştırmak için mütevazı araçlar kullanarak stratejik zafer elde etmeye yönelik askeri bir girişimdir. Çoğunlukla fiziksel bir zarar vermese bile askeri sistemlerin operatörleri için kafa karıştırıcı hatta yanıltıcı etkileri olabilmektedir[4].

Son yıllarda gerçekleşen birçok farklı siber saldırı yöntemi bulunmaktadır. Bu saldırıların hedefleri politik, ideolojik, ekonomik veya askeri olabilmektedir. Her savaşta olduğu gibi siber savaşta da saldırı amacıyla çeşitli silahlar kullanılmaktadır. Konvansiyonel silahların aksine siber silahlar çok farklılık göstermektedir. Bilinen en yaygın siber saldırı silahları arasında virüsler, solucanlar,

truva atları, komut dosyası saldırıları, haydut internet kodları ve servis reddi (Distributed Denial of Service -DDoS) bulunmaktadır. Bu saldırı yöntemlerinin birçoğu kilobayt boyutlarına varan küçüklükte olsa da verdikleri hasar çok büyük olabilmektedir. Bir virüsle örneklemek gerekirse "Ateş ve Öğrenci (Flame and Student)" saldırısı geçmişte İran'ın nükleer silah geliştirme kabiliyetine büyük bir darbe vurmuştur[5].

4. ASKERİ SİSTEM VE PLATFORMLARIN KARŞI KARŞIYA KALDIĞI SİBER TEHDİTLER

Enerji hatları, su arıtma ve dağıtma tesisleri, hastaneler, trafik kontrolü, havacılık, demiryolları, deniz ulaşımı, uzay tabanlı iletişim sistemleri, konumlama, zaman ve navigasyon uygulamalarının tamamı siber uzayın ve askeri güçlerin bir parçasıdır. Ülkelerin savunma yeteneklerinin zayıflatılması için de sıklıkla siber saldırılar düzenlenmektedir[6].

Askeri casusluk ve bilgilerin çalınması gibi siber saldırı yöntemleri devletlerin askeri güçleri için büyük tehdit oluşturmaktadır. Askeri stratejiler, askerlerin dağıtım bilgileri, silah tasarımları ve füze konumları bu yöntemlerle sıklıkla tehlikeye düşebilmektedir. Birbirleriyle bağlantılı üsler, sistemler ve araçların ele geçirilme veya iletişimlerinin kesilmesi olasılığı ise bir başka tehdit unsuru yaratmaktadır.

Örneğin, savaş gemileri görev ve sorumluluklarını yerine getirmek için bilgi teknolojilerine ihtiyaç duymaktadır. Geminin hareket etmesi için gerekli olan makinelerin kontrolünden güvenli bir şekilde yolunu bulması için gerekli olan navigasyon sistemlerine, gemide kullanılan ateş gücünün doğru bir şekilde komuta edilmesinden gemi ile genel komuta merkezi arasındaki iletişimin güvenli bir şekilde sağlanmasına kadar çok geniş bir alanda bilgi teknolojilerine ihtiyaç duyulmaktadır. Savaş gemilerinde temel olarak üç ana sistem bulunmaktadır. Bunlar endüstriyel kontrol sistemleri, navigasyon sistemleri ve muharebe yönetim sistemleridir. Bu sistemler doğrudan internete bağlı olmasalar da tedarik zincirinin herhangi bir noktasında yüklenen zararlı yazılım, sistemleri doğrudan etkileyecektir. Sosyal mühendislik saldırısı sonucu bir USB ile zararlı yazılım gemi bilişim sistemlerine bulaşabilir ve DOS saldırısı ya da bilgi sızdırma gerçekleşebilir. Bu şekilde füzenin ateşlenmesi, radar sistemlerinin kapatılması veya daha kötüsü dost unsurların düşman gibi gösterilerek dost ateşi ile imha edilmesi sağlanabilir.

Savaş gemilerinde bulunan sistemlerin her birinin farklı siber güvenlik gereksinimleri bulunmaktadır. Bu sistemlerin geliştirilmesinde güvenli sistem geliştirme süreçlerinin takibi, sistemlerin güvenliğinin sağlanması için düzenli olarak sistemler üzerinde ne tür zaafiyetlerin olduğuna bakılması ve bu sistemlerin savunulması noktasında gerekli kaynakların ayrılması son derece önemlidir. Bu nedenlerden dolayı askeri otoriteler savaş gemilerinde siber güvenliği bütüncül bir yaklaşım ile ele almalı ve yeni stratejiler geliştirmelidir.

Askeri otoriteler; uçakları, platformları ve donanmaları izledikleri gibi üst düzey komutan ve yöneticileri de GPS ve benzeri sistemlerle izleyebilmektedir. İstihbarat servislerince bu izleme sistemlerine sızılması ile ülkelerin hayatta kalması ve savunması için önemi olan kişiler açısından ölümcül sonuçlar ortaya çıkabilmektedir[5].

Çoğu zaman kullanıcıların bilgisi dahi olmadan başkalarınca ele geçirilmiş bilgisayarlar olan "botnet"lerle yapılan DDoS saldırıları da bilgi işlem altyapılarının çalışamamasına neden olabilmektedir. Sistemlerin cevaplayabileceğinden çok daha fazla çoklu isteğin iletilmesiyle çalışan DDoS, veri akışının kilitlenmesine ve sistemin kullanılmaz hâle gelmesine neden olmaktadır. Akıllı bombalar adı verilen siber saldırı yöntemleri ise yazılım ve cihazların kullanılmadan önce içerisine sızdırılarak kullanıma başlaması sonrası faaliyete geçip çeşitli arızalara neden olabilmekte ve hatta yazılım ve sistemi tamamen yok edebilmektedir. Bunlarla beraber yazılım ve araçlara yüklenebilen arka kapılarla (backdoor) istenmeyen kişilere uzaktan bağlantı imkânı da yaratılabilmektedir[7].

Son yıllarda meydana gelen siber saldırılar incelenecek olursa savunma yapılarının da kamu kurumları kadar hedef alındığı görülmektedir[8]:

- Mayıs 2020'de ABD Ulusal Güvenlik Ajansı, Rusya Askeri İstihbarat Teşkilatı (Glavnoye Razvedyvatel'noye Upravleniye -GRU) ile bağlantılı bir grup Rus hacker'ın ABD sunucularının kontrolünü uzaktan ele geçirdiğini bildirmiştir.
- Haziran 2020'de şüpheli Kuzey Koreli hacker'lar Orta Avrupa'da en az iki güvenlik firmasını hack'leyerek kendilerini ABD savunma üreticileri olarak tanıtıp sahte siparişler vermişlerdir.
- Temmuz 2020'de eski ABD Başkanı Donald Trump, Rus İnternet Araştırmaları Ajansının sistemlerinin kapatılması için 2019 yılında ABD Siber Komutanlığına talimat verdiğini açıklamıştır.
- Ekim 2020'de ABD Ulusal Güvenlik Ajansı, Çin hükümet hacker'larının ABD Savunma Endüstri üssünü hedef alan casusluk saldırılarını bildirmiştir.

ABD'nin Hava Kuvvetlerinin kullandığı teknolojilerin gelişmesi de siber saldırı endişelerinin artmasına neden olmaktadır. RAND Corporation'ın "ABD Hava Kuvvetleri Askeri Sistemlerinin Siber Güvenliğini Yaşam Döngüleri Boyunca İyileştirmek" isimli raporunda[9] ABD Hava Kuvvetlerinin ne gibi siber zafiyetleri olduğu ve bunların nasıl giderilebileceği incelenmiştir.

Rapora göre; sürekli değişken yapıda olan siber uzay, öngörülmesi güç zorluklar ortaya çıkarmaktadır. Ancak ülkelerin genel siber güvenlik politikaları stabil, basit ve tahmin edilebilir yaklaşımlar üzerinden ilerlemektedir. Bu durum askeri alanda siber güvenlik yönetimleri için önemli boşluklara neden olmaktadır.

Eksikliklerin giderilmesi için öncelikle askeri sistemler ve hava kuvvetleri açısından siber güvenlik hedefleri

belirlenmelidir. Siber güvenlik risk yönetimi sorumlulukları gözden geçirilmeli ve dengeli bir yaklaşım belirlenmelidir. Yetkilendirilen sorumluların hangi sistemlere nasıl yetki vereceği sürekli izlenir bir şekilde kurgulanmalıdır. En önemlisi ise siber güvenlik karışıklığını azaltmak için ara bağlantıların azaltılarak sistemlerin belirli bir düzenle bağlantılı olmasının sağlanmasıdır.

İngiliz şirketi BAE Systems gibi bazı özel kuruluşlar da birçok ülkede faaliyet gösteren askeri yapılara siber güvenlik hizmetleri sunmaktadır. BAE Systems'in temel hedefi hizmet verdikleri tarafların araçlarını ve sistemlerini siber saldırılardan korumaktır. Tilki Kalkanı (Fox Shield) adını verdikleri paket program ile kara, hava ve uzay platformlarında siber saldırılara karşı güçlü bir savunma ve erken tespit imkânı hedeflenmektedir[10].

ABD Savunma Bakanlığı ile birlikte çalışmalar yapan Mission Secure (MSI) firması da insansız hava araçlarının siber saldırılara karşı korunması için araştırmalar yapmaktadır. Güvenli Nöbetçi Platformu (Secure Sentinel Platform) adı verilen sistemler ile GPS verilerine, güzergâh ara nokta manipülasyonlarına, gözlem ve mühimmat kullanımıyla ilgili sistemlere karşı yapılacak siber saldırıların engellenmesini hedeflemektedir[11].

4.1 İstihbarat, Bilgi ve Siber Savaş

Siber savaş birden fazla şekilde tanımlanabilmektedir. Bunların en önemlilerinden bazıları iletişim ile verilerin savunması ve saldırılar, iletişimi sağlayan sistemlerin işlem yapma kapasitelerinin engellenmesi ve manipüle edilmesi gibi alanlardan oluşmaktadır.

Teknoloji çağında askeri güçlerin elinde bulunan en önemli silahlardan biri de bilgi teknolojileridir. İletişimin hayati önem taşıdığı operasyon ve sistemlere sızılması veya bu sistemlerin engellenmesi çok ciddi sorunlar doğurabilmektedir. Ayrıca bilgiye herkesten önce ulaşılması ve iletişimin güçlü kılınması taktiksel avantajlar da sunmaktadır[12].

Siber savaş sadece bilgisayarlar veya veriler arasında süren bir savaş gibi düşünülmemelidir. Aslında bu savaş şekli siber uzay veya dijital düzlemde rakibine saldırmak olarak da tanımlanabilir. Bu saldırılar devlet destekli sızmalar ile iletişim sistemlerinin etkilenmesinden, hacker'ların başkalarını etkilemek için bireysel politik görüşlerini sunduğu uygulamalara kadar farklılık göstermektedir.

Siber savaşın en zorlu koşullarından biri saldırıyı gerçekleştireni tanımlamaktır. Saldırılar bir topluluk ile birlikte veya bir kişinin komutasındaki onlarca bilgisayar ile gerçekleşebilmektedir. Ayrıca siber savaş sonuçları çok hassas bir keskinlikte olmadığından sonrasında etkilenenlerin sayısı hedeflenenin çok üzerinde de olabilmektedir[13].

4.2 Siber Güvenlikte Kuantum Bilişim, Yapay Zekâ ve Bulut Bilişim

Siber savaş için kuantum bilişim uygulamaları sınırsızdır. Kuantum bilgisayarları günümüz geleneksel bilgisayarlarının 10.000 yılda yapabileceği bir işlemi 200 saniye gibi kısa bir sürede gerçekleştirebilmektedir[14].

Kuantum teknolojileri ve bilgisayarlarda yaşanan gelişmeler ülkeleri teknoloji ve askeri anlamda çok ilerilere taşıyabilmektedir. Bilgiişlem teknolojisinin önemli bir kısmını oluşturan siber dünyada meydana gelen siber savaşlar da kuantum bilgisayarlarından etkilenerek yeni olasılıklar ve riskler yaratmaktadır[15].

Günümüzde sistemlerin korunmasında etkin olarak kullanılan gelişmiş algoritmaların geleceğin kuantum bilgisayarlarına karşı çok şansı olmadığı düşünülmektedir. Şifreli verileri çözebilecek kuantum bilgisayarlara sahip olmayan taraflar ise ele geçirilen bilgileri depolayarak ileride teknolojik anlamda yeterli hâle gelince açmak üzere yüksek miktarda veri saklamaktadır.

Ancak günümüz kuantum bilgisayarları mevcut gelişmiş algoritmaları çözümleyemediğinden kuantum bilgisayarlar ile ilgili birçok siber savaş yaklaşımı teoride kalmaktadır. Pek çok bilim insanı ise kuantum bilgisayarların gelecekte kırabilecekleri şifreleme yöntemlerini güçlendirmek için çalışmalar yapmaktadır. Bu çalışmaların en çok gözlemlendiği yerlerden biri ABD Ulusal Standartlar ve Teknolojiler Enstitüsüdür. Enstitü araştırmacıları, "Kuantum Sonrası Kriptolama" adı verilen 69 potansiyel metot için 2024 yılına kadar taslak çalışmaları tamamlamayı hedeflemektedir. Bir diğer alternatif kriptolama yöntemi ise "kuantum anahtar dağıtımı" adı verilen bir uygulamadır. Bu yöntemde alıcı ve verici arasında kuantum iletişiminde simetrik bir anahtarla güvenlik sağlanabilmektedir. Ancak bu yöntem özel teçhizatlar gerektirmektedir.

Kriptolama güvenliğin tamamen sağlandığı anlamına gelmediğinden son kullanıcı tarafından her zaman dikkatli olunması gerekmektedir. Günümüz iletişim teknolojilerinin giderek kamuya daha açık hâle geldiği dünyamızda askeri uygulamaların güvenliği için kuantum iletişimi, kriptolama, yapay zekâ destekli güvenli bulut ve iletişim yazılımları gibi birçok farklı yöntem bir arada kullanılabilir[15].

Siber savaşlarda avantaj sağlayan bir diğer teknoloji de yapay zekâdır. Otonom sistemlerin temel bileşeni haline gelen yapay zekâ kendi kendini yönetme ve durumlara adapte olabilme özelliği ile siber saldırılara karşı savunmada avantaj sağlarken, rakibin savunmasını aşma konusunda da güçlü bir saldırı aracı olabilmektedir. Her türlü durumda yapay zekânın da hack'lenebilmesi ve düşman kontrolüne geçme olasılığı siber dünyanın getirdiği risklerden biridir. Her ne kadar ABD gibi süper güçler, nükleer silahlar gibi kitle imha silahlarının kontrolünü hiçbir zaman bir yapay zekâ uygulamasına devretmeyeceğini bildirse de bu uygulamaların dolaylı yoldan risk yaratma olasılığı hâlen korkutucu bir gerçektir[14].

Yapay zekânın askeri siber güvenlikte uygulanabildiği üç önemli alan bulunmaktadır.

- Otonomi ve makine öğrenmesi ile gelişen sistemler, siber saldırılara karşı da daha açık hâle gelmektedir. Deepfake gibi yeni yaklaşımların ortaya çıkmasını sağlayan yapay zekâ, askeri haber alma sistemleri ve diğer bütün mekanizmalar için hesaplama, öngörü ve karşılık verme yeteneklerini etkileyebilmektedir.

- Siber saldırılara maruz kalan yapay zekâ sistemlerinin çalışmaları boyunca kaydettikleri makine öğrenmesi verilerinin de saldırganların eline geçmesi bir risk yaratmaktadır. Yüz tanıma, analiz sistemleri ve istihbarat verilerinin ele geçirilme riski istihbarat desteği, izleme ve keşif kabiliyetlerini etkileyebilmektedir.
- Son olarak yapay zekâ saldırılara karşı çok güçlü bir savunma ve karşılık verme mekanizması da oluşturabilmektedir. Büyük ölçekli siber saldırılarda insanların yetişemeyeceği noktalarda hızlı karar verme ve uygulamaya geçme özelliği yapay zekâyı benzersiz bir destek ve savunma sistemine dönüştürmektedir[16].

Bulut sistemler çok yeni uygulamalar olmasa da son yıllarda artan bir hızla gelişmektedir. Daha hızlı, keskin ve ihtiyaç anında ulaşılabilen veri kaynakları olan bulut sistemlerin avantajları olduğu kadar dezavantajları da bulunmaktadır. Bulutta saklanan ve erişime açık olan verilerin hack'lenmesi veya manipüle edilmesi daha olasıdır. Ancak doğru güvenlik önlemleriyle donatılan bulut sistemler daha dayanıklı ve güvenli hâle getirilebilir. Verinin anlık değişikliklerinin izlenmesi ve birden fazla konumda saklanabilmesi bir saldırı sırasında veya sonrasında veri değişimini veya kaybını önleyebilir[14].

Bulut sistemlerin güvenliği için birçok çalışma yapılsa da veri merkezleri, ağ altyapıları ve yeni teknolojik çözümler gelişirken, artan nesnelerin interneti (IoT) cihazları da riskleri beraberinde getirmektedir. IoT cihazların bulut sistemlere duyduğu ihtiyaç bu alanla ortaklaşa önlemler alınması gerekliliğini artırmaktadır[17].

4.3 Siber Güvenlikle IoT Uygulamaları

IoT bir anlamda "Tehditlerin İnterneti" olarak da düşünülmektedir. Birbiriyle bağlantılı cihazların, araçların, evlerin sayısı her geçen gün artarken IoT uygulamaları askeri alanda da hızla yaygınlaşmaktadır.

Her yeni teknoloji gibi IoT uygulamalarının da yaygınlaşmasıyla birlikte askeri sistemlerde yeni potansiyel saldırı alanları doğmaktadır. Bu saldırı arayüzleri şu şekilde sıralanabilir:

- IoT cihazlarının kendisi (sensörler vb.),
- IoT cihazları arasındaki ve cihazlarla bağlı oldukları sunucu sistemleri arasındaki iletişim kanalları,
- Sunucu sistemlerindeki IoT cihazlarına özgü uygulamalar.

Genişleyen saldırı yüzeyi, örneğin fitness cihazlarıyla bile askeri birliklere dair lokasyon ve aktivite gibi son derece önemli bilgileri elde etmek mümkün hâle gelebilmektedir[18].

Bunun yanı sıra İnsansız Hava Araçlarını (UAV) hedef alan saldırılar ile bu araçlar ele geçirilebilmekte ve bu sayede askeri operasyonlara müdahale edilebilmektedir[19].

Askeri sistemlerde kullanılan IoT cihazlar daha kararlı ve çeşitli teknik kabiliyetlere sahip saldırganlarla karşı karşıyadır. Her ne kadar yakın zamandaki operasyonlarında NATO'nun veya NATO ülkelerinin karşılaştığı hasımları yüksek teknik kabiliyetlere sahip olmasa da bu durum hızla değişmektedir. 2011 yılında İran'ın siber

savaş birimi tarafından Afganistan-İran sınırında gözetleme görevi yürüten Lockheed Martin yapımı RQ-170 İHA'sının şifrelenmemiş haberleşme birimleri istismar edilmek suretiyle kontrolünün ele geçirilerek alıkonulması bu konuya güzel bir örnek oluşturmaktadır[20].

Bu ve benzeri durumlardan alınan derslerle NATO tarafından düzenlenen siber tatbikatlarda olduğu gibi, IoT sistemlerinin de dahil olduğu içeriklerle çeşitlendirilmiş tatbikatların düzenli olarak gerçekleştirilmesi gerekmektedir.

IoT cihazlar için alınabilecek en iyi önlemlerden biri sürekli izlenmeleridir. En ufak değişikliklerin veya izinsiz girişlerin kaydını tutabilen uygulamalarla donatılan IoT cihazlar için güvenlik artacağı gibi olası tehditler de fark edilebilmektedir. Aynı zamanda IoT ağlarının da giriş yetkilendirmeleri ve izlenmesi gibi önlemlerle güçlendirilmesi gereklidir[21].

IoT cihazların sürekli güncel tutulması önemlidir. Her güncelleme zaman geçmeden cihazlara yüklenmeli ve eski versiyonlardan kaynaklanan riskler bertaraf edilmelidir. IoT cihazların sensör bağlantıları da kontrol altında tutulmalıdır. Dışarıdan müdahale edilemez şekilde kurgulanan sensörler güvenliği artıracaktır[22].

Askeri platformların da IoT kullanmaya başlamasıyla birbiriyle bağlantılı hareket edebilen uçaklar, gemiler, insansız hava ve kara araçları, silahlar, hava savunma sistemleri, iletişim sistemleri ve kişisel korunma ekipmanları "Askeri Nesnelerin İnterneti (Internet of Military Things -IoMT) kavramını ortaya çıkarmıştır. Bu kapsamda insansız sistemlere sürü yeteneği kazandırılması da kolaylaşabilecektir. IoMT ordular için yepyeni silah teknolojileri ve operasyon kabiliyetleri yaratırken beraberinde yeni karşıt güçler de ortaya çıkmaktadır. Bu noktada gelecekte nasıl bir geleneksel savaş kavramı olacağı tartışma konusudur. Gelecekte kullanılacak insansız savunma ve saldırı platformları için siber savaş kavramı tek bir konumdan bütün sistemlerin ışık hızında kontrol edilerek koordineli olarak kullanıldığı bir savaş ortamı yaratabilir[13].

5. NATO'NUN GÜNCEL SİBER GÜVENLİK STRATEJİLERİ

Güçlü devletlerin bir araya geldiği ittifaklardan biri olan NATO'nun da siber saldırılara karşı kendi stratejileri bulunmaktadır. NATO'ya yapılan siber saldırıların sıklığı her geçen yıl artarken bu saldırılarda daha kompleks, yıkıcı ve zorlayıcı yöntemler kullanılmaktadır. NATO ve müttefiklerinin ittifakın önemli görevleri olan topluluk savunması, kriz yönetimi ve koordineli güvenlik gibi alanlarda güçlü ve esnek siber güvenlik yaklaşımlarına ihtiyacı bulunmaktadır[23].

5.1 NATO Siber Savunma Politikası

NATO hızla değişen tehditler karşısında barışa verdiği desteği devam ettirmek adına Eylül 2014'teki Galler zirvesinde müttefiklerinin de katılımıyla bir siber güvenlik politikası benimsemiştir. Bu politikaya göre siber güvenlik ittifakın önemli merkezi görevlerinin bir parçası sayılacak ve uluslararası kanunların geçerli olduğu siber uzay ile uyumlu bir şekilde uygulanacaktır.

2016'nın Temmuz ayında düzenlenen Varşova zirvesinde siber uzay NATO tarafından hava, kara ve deniz gibi bir alan olarak kabul edilmiştir. Siber uzayın bir operasyon alanı olarak kabulü NATO'nun görevleri ile operasyonlarının daha iyi korumasını ve eğitim ile askeri planlamalara daha fazla odaklanmasını sağlamıştır. NATO'nun değişmez görev yetkisi savunmadır. Bu nedenle NATO'nun siber uzaya yaklaşımı her alanda olduğu gibi orantılı, savunma odaklı ve uluslararası kanunlarla uyumludur.

NATO Bilgisayar Olayları Müdahale Kabiliyeti (NATO Computer Incident Response Capability -NCIRC) NATO'nun kendi ağlarını koruyan bir sistemdir. Sistem merkezi yönetimle sürekli olarak NATO'nun çeşitli sitelerinde güvenliği sağlarken hazırda bekleyen acil müdahale ekipleri gerektiğinde NATO ve müttefikleri için ayrıca koruma sağlamaktadır.

Estonya'nın Tallin şehrinde bulunan NATO İşbirlikçi Siber Savunma Mükemmeliyet Merkezi siber savunma eğitimi, danışmanlığı, araştırma ve geliştirme faaliyetlerinin yürütüldüğü bir merkezdir. Bu merkez, NATO Komuta Merkezinin bir parçası olmasa da siber güvenlikte NATO tarafından tanınmıştır.

İtalya Latina'da bulunan NATO İletişim ve Bilgi Sistemleri Okulu ise müttefik güçlere iletişim alanında personel yetiştirmektedir. Bu merkezin yakın zamanda Portekiz'e taşınarak siber savunma eğitimlerinin de dahil olduğu eğitim programları oluşturması hedeflenmektedir.

Son olarak Almanya Oberammergau'da bulunan NATO okulu müttefik operasyonları, stratejileri, politikaları, doktrinleri ve prosedürlerini yürütmek adına siber güvenlik ile ilgili eğitimler sağlamaktadır[24].

6. DEVLETLERİN GÜNCEL SİBER GÜVENLİK STRATEJİLERİ

Siber uzay genellikle hava, kara, deniz ve uzayın da dahil olduğu "beşinci" savaş bölgesi olarak tanımlanmaktadır[14].

Uluslararası sistemde birçok devlet kendi siber savunma ve saldırı yeteneklerini artırmak amacıyla siber güvenlik stratejileri ortaya koymaya başlamış ve bu süreçleri sürdürmek amacıyla da kurumsal yapılar tesis etmişlerdir. Bu çerçevede ABD, Rusya, Çin, İran, İsrail ve İngiltere'nin etkili siber güvenlik kapasitelerine sahip oldukları iddia edilebilir[25].

6.1 ABD

Siber güvenlik hemen hemen bütün ülkelerin en önemli askeri stratejilerinden biri hâline gelmiştir. Siber saldırılar ülkelerin ekonomilerini hedef alarak zayıflamalarına ve bireyleri hedef alarak politik kayıplara neden olurken aynı zamanda ciddi itibar kayıplarına da yol açmaktadır. Siber saldırılara karşı alınacak önlemler yüksek bütçe rakamları ortaya çıkardığından savunma mekanizmaları da geçmişte geri plana atılmıştır. Ancak gelecekteki savaşların daha fazla siber uzaya taşınacak olması ülkeleri bu alanda ciddi yatırımlar yapmaya yöneltmiştir.

ABD'nin Meade Üssü'nde kurduğu Siber Komutanlığı bu yatırımların önemli örneklerinden biridir. Ortak askeri komuta merkezi olarak görev yapan üstte askeri olmayan varlıkların da korunması hedeflenmektedir.

Ayrıca Arlington'da kurulan Siber Güvenlik ve Altyapı Güvenliği Ajansı (Cybersecurity and Infrastucture Security Agency -CISA) en yeni federal ajanslardan biridir. 2018 yılında eski ABD Başkanı Donald Trump'ın imzaladığı Siber Güvenlik ve Altyapı Güvenliği Ajansı Yasası da siber saldırılara karşı koordineli bir çalışma yapılmasının önemini vurgulamaktadır[6].

ABD aynı zamanda, 2016 yılında ABD Askeri Akademisinde kurulan Ordu Siber Enstitüsü (Army Cyber Institue -ACI) gibi siber araştırma birimleriyle de siber uzayda güçlü bir gelecek oluşturma çabasındadır[14].

ABD Savunma Bakanlığı (DoD) da siber uzay ile ilgili olarak 2018 yılında beş temel hedef belirlemiştir.

Buna göre;

- Müşterek kuvvetler siber uzay yardımı ile görevlerini birlikte yürütebilecektir.
- Müşterek kuvvetlerin siber uzay operasyonlarının gelişmesiyle daha da güçlenmesi ve ABD'nin askeri avantajlarının artırılması hedeflenmelidir.
- ABD'nin kritik altyapılarının tek başına veya bir operasyon dahilinde olası bir siber saldırıya karşı korunması önemlidir.
- DoD'nin bilgi ve sistemlerinin DoD içinde ve DoD dışında kötücül siber aktivitelere karşı güvenliğinin sağlanması gerekmektedir.
- DoD siber çalışmalarının ajanslar arası, farklı endüstrilerde ve uluslararası ortaklarla birlikte yürütülmesi amacıyla genişletilmesi hedeflenmelidir.

ABD Savunma Bakanlığı bu hedefler doğrultusunda siber savaşlar için daha yıkıcı bir ortak güç oluşturma kararı almıştır. Kararları doğrultusunda siber kabiliyetlerin gelişiminin hızlandırılması ve verimliliğin artması için veri analizleri ve otomasyonun güçlenmesi ile hâlihazırda sunulan ticari siber yeteneklerin kiralanması planlanmıştır. Ayrıca siber saldırılara karşı uluslararası yeni ortaklıklar kurulması da avantaj sağlayabilmektedir.

Siber çağda verilere erişimin açık ve güvenli bir şekilde sağlanması herkes için faydalı olacaktır. ABD siber güvenlik stratejileri bu iletişimi ve bilgiyi sağlarken güvenliğin tam olarak ortaya konulduğu bir altyapıyı hedeflemektedir[26].

ABD'nin aksine Rusya ve Çin, 2035 yılına kadar siber hegemonya için mücadele edecek yeni teknolojilerin gelişimini hedefleyen hızlandırma stratejilerini kapalı olarak planlamaktadır. Aynı zamanda Çin ABD'yi bir siber silah yarışı başlatmakla suçlayarak kendilerine yapılan birçok siber saldırının kaynağının ABD olduğunu iddia etmektedir[4].

6.2 Rusya

Rusya'nın siber uzaya yaklaşımı diğer ülkelere göre çok büyük farklılıklar göstermektedir. Birçok ülkenin siber güvenlik politikaları maruz kalınan saldırı ve terörizm ile şekillenirken, Rusya saldırı öncelikli ve küresel bağımsız bir siber uzay yerine siber egemenlik eksenli güçlenmeyi hedeflemektedir[14].

Son yıllarda batıdaki askeri ve sivil altyapılara yapılan Rus siber saldırıları ciddi zorluklar yaratmaktadır. Rus askeri istihbaratınca gerçekleşen siber saldırılar Rusya'nın gelecek siber stratejileri hakkında bilgi vermektedir. Rus Siber Savaş Doktrinleri savunma öncelikli bildirimler yapsa da saldırı kabiliyetli siber operasyonların arttığı ve bu yapıya uygun siber departmanların desteklendiği düşünülmektedir[27].

Rus askeri teorisyenleri genellikle siber veya siber savaş terimlerini kullanmamaktadır. Bu terimlerin yerine, siber operasyonları, bilgisayar ağı operasyonlarını, elektronik savaşı, psikolojik operasyonları ve bilgi operasyonlarını içeren bütünsel bir kavram olan "Geniş Bilgi Savaşı" (Information Warfare -IW) terimini kullanmaktadırlar.

Rusya'nın, siber uzayda gösterdiği saldırı kökenli yaklaşım siber suçlulara, hack savunucularına ve siber kartellere sunduğu rahat hareket etme imkânlarıyla da bilinmektedir. Ayrıca bu grupların bünyesinde veya bağımsız olarak hareket eden Rus ve Doğu Avrupa kökenli hacker'ların dünyanın en iyileri olduğu düşünülmektedir. Bu hacker'lar bazı durumlarda farklı ülkelerce de kullanılabilmektedir[28].

Rusya'nın siber güvenlik stratejisi kapsamında son yıllarda ön plana çıkan diğer bir hedef ise internetin denetimi ve yönetimi alanında ABD'nin sahip olduğu küresel hegemonyanın kırılmasıdır. Bu amaç doğrultusunda Rusya kendi ulusal yazılım ve donanımlarını geliştirmekte, Rus gençliğinin yerli sosyal medya uygulamalarını kullanmalarını teşvik etmekte, ulusal siber uzay alanını küresel siber uzaydan ayıracak şekilde internet denetimlerini artırmakta, kamusal alanda Wi-Fi kullanımını denetlemekte, Özel Sanal Ağ (VPN) uygulamalarını sınırlandırmakta ve yerli anti-virüs programlarını geliştirmektedir.

Rusya'nın 2007 yılında dış politika alanında sorun yaşadığı Estonya'ya, 2008 yılında Gürcistan ve Litvanya'ya, 2009 yılında Kırgızistan'a ve 2014 yılında Ukrayna'ya yönelik DDoS atakları şeklinde siber saldırılar gerçekleştirdiği de iddia edilmektedir[25].

2016 yılında Rusya'nın İnternet Araştırmaları Ajansının, ABD seçimlerini sosyal medya üzerinden etkilemeye çalışması sonrası ABD'ye karşı yapılan politik içerikli siber saldırılara devam edilmiştir[29].

6.3 Çin

Çin geniş yüzölçümü, büyük nüfusu ve hızla geliştirdiği ekonomik ve askeri altyapısı sayesinde son yıllarda önemli bir küresel güç hâline gelmiştir. Bu nedenle Çin yönetimlerinin gerek askeri ve siyasi gerekse ekonomik ve teknolojik alanlardaki düşünce, niyet ve planları diğer devletlerce yakından takip edilmektedir. Ayrıca dünya genelindeki 3,4 milyar internet kullanıcısının 721 milyonunun Çin'de olduğu düşünüldüğünde, küresel ölçekli siber güvenlik stratejilerinin belirlenmesi konusunda Çin'in önemi ve etkisinin büyüklüğü ortaya çıkmaktadır[25].

Çin ilk Ulusal Siber Güvenlik Stratejisi'ni 27 Aralık 2016 tarihinde açıklamıştır. Stratejinin temel hedefi düzenli, güvenli ve bütün ulusa açık bir siber uzay kurgulanırken küresel anlamda Çin'in siber güç hâline gelmesidir. Çin'in Ulusal Siber Güvenlik Stratejisi'nin dokuz temel hedefi bulunmaktadır[30]:

- Siber âlem egemenliğini savun,
- Ulusal güvenliği koru,
- Kritik bilgi altyapısını koru (Critical Information Infrastructure -CII),
- Sağlıklı bir çevrimiçi kültürü oluştur,
- Siber suçla, casuslukla, terörle savaş,
- Siber yönetimi güçlendir,
- Temel siber güvenliği güçlendir,
- Siber âlem savunma kabiliyetlerini arttır,
- Uluslararası işbirliğini güçlendir.

6.4 İngiltere

İngiltere en son Ulusal Siber Güvenlik Stratejisini 2016-2021 yılları arasında belirlemiştir. Bu stratejiyle 1,9 milyar pound yatırım yapılarak dönüşümler planlanmıştır. 2021 yılı sonrası için benzer merkezi kaynaklı bir yatırım planı düşünülmemektedir. Mevcut stratejiyle İngiltere'nin siber güvenlik stratejilerinin geleceği, bilinen siber güvenlik uygulamalarının nasıl kullanılabileceği ve efektif bir politika ile siber saldırıların stratejik çerçeveleri incelenmiştir[31].

İngiltere'nin Ulusal Siber Güvenlik Stratejisi'nde üç önemli hedefe yönelen bir eylemler dizisi ortaya koyduğu ifade edilebilir.

- **Savunma:** İngiliz hükümetleri, ulusal bilişim altyapısının savunmasını güçlendirmeyi ve İngiltere'nin kritik verilerini ve sistemlerini hedef alan siber tehditlere karşı korunmayı sağlamalıdır. Bu hedefin başarılması konusunda ise kamu ve özel sektör birlikte hareket etmelidir.
- **Caydırıcılık:** İngiltere siber tehditlere karşı mevcut aktif ve pasif mukavemet unsurlarını güçlendirmeli ve etkin bir caydırıcılık algısı oluşturmalıdır.
- **Kalkınma:** İngiliz hükümetleri siber tehditlere karşı İngiltere'nin siber kapasitesini geliştirmelidir. Bu kapsamda İngiltere'nin büyüyen siber güvenlik endüstrisinin geliştirilmesine destek verilmelidir.

6.5 İsrail

İsrail özellikle 2010 yılı sonrasında Başbakan Binyamin Netanyahu'nun kişisel inisiyatifiyle, etkili siber savunma ve saldırı kapasitesini geliştirmek için ciddi bir atılım içinde olmuştur. Söz konusu planlar dahilindeki ulusal güvenlik stratejileri kapsamında yönlendirilen kamu-özel sektör ortaklığı ve akademik çevrelerin işbirliği sonucunda, İsrail kısa sürede ABD, Rusya ve Çin'den sonra siber uzayda etkili bir güç hâline gelmiştir[25].

İsrail'in siber stratejilerinin temelinde Kritik Altyapının Korunması (Critical Infrastructure Protection -CIP) yaklaşımı bulunmaktadır. Geçmişte sivil siber güvenlik yöntemleriyle yapılan çalışmaların günümüz siber uzayında yetersiz kalmasıyla, bütün siber uzay güvenlik ve saldırı çalışmaları İsrail Ulusal Siber Direktörlüğü (Israel National Cyber Directorate -INCD) altında toplanmıştır[32].

6.6 İran

Son zamanlarda gelişme gösteren ülkelerden biri olan İran da siber uzayda güç gösterisi yapan bir altyapıya sahiptir. İran'ın artan siber operasyonları ve saldırılarının ardında dört temel hedef bulunmaktadır.

- Uluslararası yaptırımlardan kurtularak ekonomik modernizasyon,
- Ortadoğu'daki bölgesel düşmanların yenilmesi,
- Ayetullah rejiminin korunarak muhalefetin bastırılması,
- İdeolojik düşmanların cezalandırılarak itibarsızlaştırılması.

Bu hedefler doğrultusunda İran hükümeti siber güvenlik ve siber savaş alanında hızlı adımlarla güçlü yatırımlar yapmaktadır. IronNet ile inovasyon ve savunma şirketleri güçlendirilirken, IronDefense ağ tespiti ve cevaplaması için analitik yöntemler geliştirmekte ve IronDom ise kolektif bir savunma anlayışıyla hizmet verilen herkese güvenli bir iletişim imkânı sunmaktadır[33].

İran'ın siber saldırı stratejisini geliştirmeye yönelik planları, 2010 yılında ABD ve İsrail tarafından planlandığı iddia edilen ve nükleer tesislerini hedef alan Stuxnet saldırısı sonrasında bir misilleme refleksiyle hız kazanmıştır. Ancak ilk etapta bir misilleme motivasyonuyla hızlanan İran'ın siber saldırı kapasitesini geliştirmeye yönelik gayretleri, ilerleyen dönemlerde alınan tedbirlerle, İran'ı siber uzayda etkili bir aktör hâline getirme hedefine dönüşmüştür[25].

7. TÜRKİYE'DE ASKERİ SİSTEM VE PLATFORMLARIN SİBER GÜVENLİĞİ

Türkiye'nin internet kullanımı sosyal medya, özel sektörün artan gereksinimleri ve devlet ağının nitelikleri doğrultusunda hızla yükselen bir profildedir. Giderek artan söz konusu "bağlantılılık" durumu, Türkiye'nin kritik milli altyapısının siber ağlara olan bağımlılığı ve karşılaşılan siber saldırılar, Türk milli güvenlik ajandasına siber güvenliğin de girmesine neden olmuştur. Bu bağlamda Ankara, 20 Ekim 2020 itibariyle "Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi ve Koordinasyonuna İlişkin Karar" ile siber güvenlik koordinasyonuna ilişkin ilk milli hukuki düzenlemesini yapmıştır[34]. Türk Silahlı Kuvvetleri bünyesinde bir "Siber Savunma Komutanlığı" kurulmuş ve Türk hükümeti 2011 yılında ülkenin kurumlar arası ilk siber tatbikatını düzenlemiştir[35].

Askeri sistemlerin güvenliğinden sorumlu olan Siber Savunma Komutanlığı diğer askeri birimlerin siber güvenliğini güçlendirmek için olumlu adımlar atmakta ve uluslararası siber tatbikatlarda ciddi başarılar elde etmektedir. Siber güvenliğin savunma alanında, ülkeler komuta kademesi başta olmak üzere, askeri karar alma mekanizmalarındaki kişilerin siber alanın getirdiği fırsat ve tehditlere ilişkin bilinçlendirilmesi için ciddi eğitim yatırımları yapmaktadır[36].

Ülkemizde siber güvenlik alanında ilk olan "Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı", 20 Haziran 2013 tarihli ve 28683 sayılı Resmî Gazete' de yayımlanarak yürürlüğe girmiştir. İki yıllık bu dönem içerisinde siber güvenlik mevzuatının geliştirilmesi, kritik altyapıların güvenliğinin sağlanması, toplumda siber güvenlik farkındalığının oluşturulması, siber tehditlerin tespiti ve önlenmesi konularında çalışmalar yürütülmüştür[37].

Ayrıca 2013 yılında, BTK bünyesinde faaliyetlerini sürdüren Ulusal Siber Olaylara Müdahale Merkezi (USOM) kurulmuş, belirlenen kritik altyapı sektörleri başta olmak üzere kurum ve kuruluşlarda Siber Olaylara Müdahale Ekipleri (SOME) faaliyetlerine başlamıştır. Ulusal siber güvenlik organizasyonunun oluşturulmasıyla ülkemizde kurumsal ve organizasyonel yapıların kurularak güçlendirilmesi sağlanmıştır[38].

Sonrasında yayınlanan "2016-2019 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı" ile de siber güvenlik risklerinin yönetilebilir ve kabul edilebilir düzeylerde tutulabilmesi için siber savunmanın güçlendirilmesi, kritik altyapıların korunması, siber suçlarla mücadele edilmesi, farkındalık ve insan kaynağı geliştirilmesi, siber güvenlik ekosisteminin geliştirilmesi ve siber güvenliğin milli güvenliğe entegrasyonu konularında çalışmalar yürütülmüştür[37].

Teknolojinin vazgeçilmezliği ve sürekli gelişimiyle birlikte siber güvenliğe ilişkin faaliyetlerin de süreklilik içerisinde yürütülmesi gerekmektedir. Bu doğrultuda hazırlanan Ulusal Siber Güvenlik Stratejisi ve Eylem Planı (2020-2023) ile siber tehditlerin etkilerinin azaltılması, ulusal kabiliyetlerin geliştirilmesi, güvenli bir ulusal siber ortamın oluşturulması ve ülkemizin siber güvenlik alanında uluslararası seviyede en üst sıralarda yer alması hedeflenmektedir.

2013-2014 dönemi ile 2016-2019 döneminde gerçekleştirilen ve süreklilik arz eden eylemler, mevcut durum ve planlanan çalışmalar kapsamında gözden geçirilmiş ve gerekli iyileştirmelerin yapılması sağlanmıştır. Bu çerçevede, belirlenen stratejik amaçlar sekiz ana başlıkta toplanmıştır:

- Kritik Altyapıların Korunması ve Mukavemetin Artırılması,
- Ulusal Kapasitenin Geliştirilmesi,
- Organik Siber Güvenlik Ağı,
- Yeni Nesil Teknolojilerin Güvenliği,
- Siber Suçlarla Mücadele,
- Yerli ve Milli Teknolojilerin Geliştirilmesi ve Desteklenmesi,
- Siber Güvenliğin Milli Güvenliğe Entegrasyonu,
- Uluslararası İşbirliğinin Geliştirilmesi.

Önümüzdeki dönemde ulusal siber güvenliğin sağlanmasına ilişkin olarak gerçekleştirilecek faaliyetlerin kapsamının belirlendiği Ulusal Siber Güvenlik Stratejisi ve Eylem Planı (2020-2023) ile bu alanda Türkiye'nin 2023 vizyonunun gerçeğe dönüşmesi hedeflenmektedir[39].

Siber güvenlik konusunda yenilikçi ve proaktif çözümleriyle öncü bir rol üstlenen STM de bu alanda aktif olarak yer almaktadır. STM tarafından Ankara'da kurulan ve Türkiye'de bir ilk olan Siber Füzyon Merkezi (SFM) hem kamu hem de özel sektörden birçok kuruma Siber Tehdit İstihbaratı dahil olmak üzere bütünleşik bir yapıda hizmet vermektedir. Kritik teknoloji ve bilgi varlıklarını koruyan proaktif ve önleyici faaliyetleri içeren merkez, Siber Tehdit İstihbarat Merkezi, Siber Operasyon Merkezi ve Zararlı Yazılım Analiz Laboratuvarı (Z-Lab) olmak üzere üç ana merkezden oluşmaktadır[40].

STM'nin siber güvenlik portföyünde tamamlayıcı bir ürün olarak sunduğu yerli ve milli bütünleşik siber güvenlik karar destek sistemi CyDecSys, ağ topolojisi oluşturma, zafiyet tespit etme, riske göre sınıflandırma ve saldırı ağacı oluşturma gibi işlemleri otomatik hâle getirerek, siber güvenlik süreçlerinin yönetimine destek olmaktadır[41].

Çeşitli kaynaklardan (deep/dark webten, sosyal medyadan, bloglardan, forumlardan vb.) otomatize bir şekilde siber tehdit istihbarat verilerini toplayan CyThreat sistemi de siber tehdit aktörlerinin aktivitelerinin tespit edilmesi, siber saldırıların gerçekleşmeden önüne geçilmesi ve koruyucu önlem alınmasını mümkün kılmaktadır[42].

Bugshield platformu ise sürekli sızma testi metodolojisiyle istismar edilebilir siber güvenlik açıklarını bulan bir sistemdir. Bu platformla, kurumların güncel siber tehditlerden korunarak güvenlik seviyelerinin artırılması hedeflenmektedir[43].

8. SONUÇ

Sistemler, silahlar ve kurumlar dijital olarak daha fazla geliştikçe, siber tehditlere karşı daha savunmasız hâle geldikleri bilinmektedir. Geleceğin teknolojileriyle ilgili araştırmalar arttıkça öngörülerde yaşanan değişimler de çoğalarak daha belirsiz sonuçlar doğurmaktadır. COVID-19 pandemisinin küresel ekonomide neden olduğu değişim ve yeniden şekillendirme etkisi öngörülemediği gibi, siber uzay çağının da ne tür yenilik ve değişiklikler getireceği henüz bilinmemektedir. Kesin olan tek şey siber uzayın herkesin hayatının bir parçası hâline geldiği ve bununla ilgili teknolojileri kontrol eden kişilerin geleceğin şekillendirilmesinde etkili olabileceği değerlendirilmektedir[14].

KAYNAKÇA

[1] *IT Governance*, "What is Cyber Security? Definition and Best Practices", https://www.itgovernance.co.uk/what-is-cybersecurity. (Erişim Tarihi: 9 Mart 2021)

[2] De Groot, Juliana; (2020), "What is Cyber Security? Definition, Best Practices & More", *Digital Guardian*, (5 Ekim 2020), https://digitalguardian.com/blog/what-cyber-security. (Erişim Tarihi: 9 Mart 2021)

[3] Nelson, Oliviah; "Importance of Cybersecurity in Military", *Cyberexperts*, https://cyberexperts.com/importance-of-cybersecurity-in-military/. (Erişim Tarihi: 9 Mart 2021)

[4] *NATO Association of Canada*, (2020), "The World In A State Of Cyber Warfare", (17 Aralık 2020), https://natoassociation.ca/the-world-in-a-state-of-cyber-warfare/. (Erişim Tarihi: 9 Mart 2021)

[5] Khalifa, Ehab; "Military Cyber Threats: Transformations in Unconventional Security Threats", *International Affairs Forum*, https://www.ia-forum.org/Files/YFXUQN.pdf. (Erişim Tarihi: 9 Mart 2021)

[6] Wilson, J.R.; (2019), "Military cyber security: threats and solutions", *Military & Aerospace Electronics*, (18 Aralık 2019), https://www.militaryaerospace.com/trusted-computing/article/14073852/military-cyber-security-tactical-network. (Erişim Tarihi: 9 Mart 2021)

[7] Seng, Ho Wei; "Cyber Attacks and the Roles the Military Can Play to Support the National Cyber Security Efforts", *Mindef Singapore*, https://www.mindef.gov.sg/oms/safti/pointer/documents/pdf/v42n3%204%20Cyber%20Attacks%20and%20the%20Roles%20the%20Military%20can%20play.pdf. (Erişim Tarihi: 9 Mart 2021)

[8] *Center For Strategic & International Studies*, "Significant Cyber Incidents Since 2006", https://csis-website-prod.s3.amazonaws.com/s3fs-public/210129_Significant_Cyber_Events.pdf. (Erişim Tarihi: 9 Mart 2021)

[9] Snyder, Don; D. Powers, James; Bodine-Baron, Elizabeth; Fox, Bernard; Kendrick, Lauren; H. Powell, Michael; (2015), "Improving the Cybersecurity of U.S. Air Force Military Systems Throughout Their Life Cycles", *RAND Corporation*, https://www.rand.org/pubs/research_reports/RR1007.html. (Erişim Tarihi: 9 Mart 2021)

[10] Martin, Nichols; (2020), "BAE Unveils Cybersecurity Platform for Military Platforms; Michael Weber Quoted", *ExecutiveBiz*, (14 Ekim 2020), https://blog.executivebiz.com/2020/10/bae-unveils-cybersecurity-platform-for-military-platforms-michael-weber-quoted/. (Erişim Tarihi: 9 Mart 2021)

[11] *MSİ*, (2020), "MSi's Secure Sentinel Platform Protects Unmanned Aerial Vehicles Against Cyber Attacks", (Şubat 2020), https://cdn2.hubspot.net/hubfs/6101815/Mission_Secure_February2020/PDF/MSi_Case_UV_online.pdf. (Erişim Tarihi: 9 Mart 2021)

[12] Orye, Erwin; M. Maennel, Olaf; (2019), "Recommendations for Enhancing the Results of Cyber Effects", *Cyber Defence Centre of Excellence*, (Haziran 2019), https://ccdcoe.org/uploads/2019/06/Art_06_Recommendations-for-Enchasing-the-Results-of-Cyber-Effects.pdf. (Erişim Tarihi: 9 Mart 2021)

[13] Sciarrone, Marie O'Neill; (2017), "Cyber Warfare: The New Front", *George W. Bush Institute*, (Spring 2017), https://www.bushcenter.org/catalyst/modern-military/sciarrone-cyber-warfware.html. (Erişim Tarihi: 9 Mart 2021)

[14] Wright, Aaron; (2020), "The Future Of Cyber Conflict", *The Cove*, (16 Ağustos 2020), https://cove.army.gov.au/article/the-future-cyber-conflict. (Erişim Tarihi: 9 Mart 2021)

[15] E. Denning, Dorothy; (2019), "Is Quantum Computing a Cybersecurity Threat?", *American Scientist*, (Mart-Nisan 2019), https://www.americanscientist.org/article/is-quantum-computing-a-cybersecurity-threat. (Erişim Tarihi: 9 Mart 2021)

[16] Johnson, James; Krabill, Eleanor; (2020), "AI, Cyberspace, And Nuclear Weapons", *War On The Rocks*, (31 Ocak 2020), https://warontherocks.com/2020/01/ai-cyberspace-and-nuclear-weapons/. (Erişim Tarihi: 9 Mart 2021)

[17] Arora, Shivam; (2021), "5 Things You Must Know About Cyber Security in the Cloud", *Simplilearn*, (1 Şubat 2021), https://www.simplilearn.com/things-you-must-know-about-cyber-security-in-the-cloud-article. (Erişim Tarihi: 9 Mart 2021)

[18] Sly, Liz; (2018), "U.S. soldiers are revealing sensitive and dangerous information by jogging", The Washington Post, (29 Ocak 2018), https://www.washingtonpost.com/world/a-map-showing-the-users-of-fitness-devices-lets-the-world-see-where-us-soldiers-are-and-what-they-are-doing/2018/01/28/86915662-0441-11e8-aa61-f3391373867e_story.html. (Erişim Tarihi: 9 Mart 2021)

[19] Ahmed, Mohiuddin; Haskell-Dowland, Paul; (2019), "Aerial threat: why drone hacking could be bad news for the military", *The Conservation*, (7 Ekim 2019), https://theconversation.com/aerial-threat-why-drone-hacking-could-be-bad-news-for-the-military-124588. (Erişim Tarihi: 9 Mart 2021)

[20] *Wikipedia*, "Iran–U.S. RQ-170 incident", https://en.wikipedia.org/wiki/Iran%E2%80%93U.S._RQ-170_incident. (Erişim Tarihi: 9 Mart 2021)

[21] *Forcepoint*, "IoT Cybersecurity", https://www.forcepoint.com/tr/cyber-edu/iot-cybersecurity. (Erişim Tarihi: 9 Mart 2021)

[22] *Center For Internet Security*, "Cybersecurity Spotlight – Internet of Things (IoT)", https://www.cisecurity.org/spotlight/cybersecurity-spotlight-internet-of-things-iot/. (Erişim Tarihi: 9 Mart 2021)

[23] *NATO*, (2020), "Cyber defence", (25 Eylül 2020), https://www.nato.int/cps/en/natohq/topics_78170.htm. (Erişim Tarihi: 9 Mart 2021)

[24] *NATO*, (2016), "NATO Cyber Defence", (Temmuz 2016), https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_07/20160627_1607-factsheet-cyber-defence-eng.pdf. (Erişim Tarihi: 9 Mart 2021)

[25] Darıcılı, Ali Burak; (2020), "Devletlerin güncel siber güvenlik stratejileri", *Anadolu Ajansı*, (2 Aralık 2020), https://www.aa.com.tr/tr/analiz/devletlerin-guncel-siber-guvenlik-stratejileri/2062810. (Erişim Tarihi: 9 Mart 2021)

[26] *U.S. Department of Defense*, (2018), "Cyber Strategy", https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF. (Erişim Tarihi: 9 Mart 2021)

[27] Lilly, Bilyana; Cheravitch, Joe; (2020), "The Past, Present, and Future of Russia's Cyber Strategy and Forces", *IEEE*, (2 Temmuz 2020), https://ieeexplore.ieee.org/document/9131723. (Erişim Tarihi: 9 Mart 2021)

[28] Connell, Michael; Vogler, Sarah; (2016), "Russia's Approach to Cyber Warfare", CNA *Analysis & Solutions*, (Eylül 2016), https://apps.dtic.mil/sti/pdfs/AD1019062.pdf. (Erişim Tarihi: 9 Mart 2021)

[29] Maurer, Tim; Hinck, Garrett; (2018), "Russia's Cyber Strategy", *Italian Institute For International Political Studies*, (21 Aralık 2018), https://www.ispionline.it/en/pubblicazione/russias-cyber-strategy-21835. (Erişim Tarihi: 9 Mart 2021)

[30] *United States Information Technology Office*, "China Publishes First National Cybersecurity Strategy", http://www.usito.org/news/china-publishes-first-national-cybersecurity-strategy. (Erişim Tarihi: 9 Mart 2021)

[31] *RUSI*, "Future UK Cyber Security Strategy Project", https://rusi.org/projects/future-uk-cyber-security-strategy-project. (Erişim Tarihi: 9 Mart 2021)

[32] *ETH Zürich*, (2020), "Israel's National Cybersecurity and Cyberdefense Posture", (Eylül 2020), https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2020-09-Israel.pdf. (Erişim Tarihi: 9 Mart 2021

[33] Hlavek, Adam; (2020), "The 4 strategic goals behind recent Iranian cyber attacks", *Security Boulevard*, (26 Ekim 2020), https://securityboulevard.com/2020/10/the-4-strategic-goals-behind-recent-iranian-cyber-attacks/. (Erişim Tarihi: 9 Mart 2021)

[34] *Resmi Gazete*, (2020), "The 4 strategic goals behind recent Iranian cyber attacks", (29 Aralık 2020), https://www.resmigazete.gov.tr/eskiler/2020/12/20201229-9.pdf. (Erişim Tarihi: 9 Mart 2021)

[35] Kasapoğlu, Can; "Türkiye'nin Gelecekteki Siber Savunma Ortamı", *EDAM*, https://edam.org.tr/document/CyberNuclear/SiberKitapTR/edam_siber_guvenlik_b1.pdf

[36] *TÜBİSAD*, (2017), "Türkiye'nin Siber Güvenlik Stratejisine Yönelik Değerlendirmeler", (Şubat 2017), http://www.tubisad.org.tr/tr/images/pdf/dtp_siber_guvenlik_raporu_4_0.pdf. (Erişim Tarihi: 9 Mart 2021)

[37] *Bilgi Teknolojileri ve İletişim Kurumu*, "Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı", https://www.btk.gov.tr/uploads/pages/2-1-strateji-eylem-plani-2013-2014-5a3412cf8f45a.pdf. (Erişim Tarihi: 9 Mart 2021)

[38] *Bilgi Teknolojileri ve İletişim Kurumu*, "USOM ve Kurumsal Siber Olaylara Müdahale Ekibi", https://eng.btk.gov.tr/usom-ve-kurumsal-siber-olaylara-mudahale-ekibi. (Erişim Tarihi: 9 Mart 2021)

[39] *T.C. Ulaştırma Ve Altyapı Bakanlığı*, "Ulusal Siber Güvenlik Stratejisi ve Eylem Planı (2020 – 2023)", *International Telecommunication Union*, https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/NationalCybersecurityStrategyOfTURKEY.pdf. (Erişim Tarihi: 9 Mart 2021)

[40] *STM*, "Siber Füzyon Merkezi", https://www.stm.com.tr/tr/cozumlerimiz/siber-guvenlik-ve-bilisim/siber-fuzyon-merkezi. (Erişim Tarihi: 9 Mart 2021)

[41] *STM*, (2019), "STM Siber Güvenlik Yetkinliklerini 4. Uluslararası Siber Savaş ve Güvenlik Konferansı'nda Sergiliyor", (Kasım 2019), https://www.stm.com.tr/uploads/docs/PR/1582287337_20191120stm-icwc.pdf. (Erişim Tarihi: 9 Mart 2021)

[42] *STM*, "CYTHREAT", https://www.stm.com.tr/tr/cozumlerimiz/siber-guvenlik-ve-bilisim/cythreat. (Erişim Tarihi: 9 Mart 2021)

[43] *STM*, "En yeni siber güvenlik ürünümüz olan 'STM Bugshield' Platformu'nun lansmanını gerçekleştirdik.", https://www.stm.com.tr/tr/medya/haberler/en-yeni-siber-guvenlik-urunumuz-olan-stm-bugshield-platformunun-lansmanini-gerceklestirdik. (Erişim Tarihi: 9 Mart 2021)

thinktech

STM Teknolojik Düşünce Merkezi

http://thinktech.stm.com.tr