SİBER SAVAŞLARIN GÖLGESİNDE İSRAİL'İN TEKNOLOJİK GÜCÜ VE ETİK SORUNLAR

Prof. Dr. Ali Murat Kırık
murat.kirik@marmara.edu.tr
ORCID: 0000-0002-5771-4843
Marmara Üniversitesi İletişim Fakültesi

ÖZET

İsrail'in siber güvenlik alanındaki liderliği, gelişmiş teknolojileri, güçlü istihbarat yapısı ve özel sektör işbirlikleriyle dikkat çekmektedir. Ancak bu üstünlük, ciddi etik ihlaller ve insan hakları sorunlarını da beraberinde getirmektedir. NSO Group tarafından geliştirilen Pegasus gibi casus yazılımlar, bireylerin mahremiyetini ihlal ederek uluslararası tepkilere yol açmıştır. Gazze'deki sivil altyapıya yönelik siber saldırılar, iletişim ağlarını devre dışı bırakmış ve insani krizleri derinleştirmiştir. Yapay zeka destekli hedefleme sistemleri, savaşlarda orantısız güç kullanımına neden olarak masum sivillerin hayatını riske atmaktadır. İsrail'in siber stratejisi, bölgesel rekabetlerde önemli bir araç olarak öne çıkarken, siber saldırılar İran gibi ülkelerle yaşanan gerilimlerde sıkça kullanılmaktadır. Stuxnet gibi siber operasyonlar, İsrail'in siber savaş alanındaki etkinliğini kanıtlarken, bu tür saldırılar uluslararası güvenliği tehdit etmektedir. Ayrıca, Demir Kubbe gibi stratejik savunma sistemlerinin siber saldırılarla devre dışı bırakılma ihtimali, siber güvenliğin önemini daha da artırmaktadır. Bu nedenle, siber güvenlik alanında uluslararası işbirliği, etik düzenlemeler ve denetim mekanizmalarının geliştirilmesi gerekmektedir. İsrail gibi siber güçlerin, siber teknolojilerin etik kullanımına öncelik vermesi, küresel barış ve güvenlik açısından büyük önem taşımaktadır. Bu çalışmanın amacı İsrail'in siber gücünü aktararak yapmış olduğu etik ihlaller ve insanlık dışı faaliyetlerde bu gücü nasıl kullandığını ortaya koymaktır.

Anahtar Kelimeler: Siber Güvenlik, İsrail, Etik İhlaller, Siber Savaş, İnsan Hakları

Makalenin Geliş Tarihi: 22 Aralık 2024
Makalenin Kabul Tarihi: 09 Ocak 2025

ISRAEL'S TECHNOLOGICAL POWER AND ETHICAL ISSUES IN THE SHADOW OF CYBER WARFARE

ABSTRACT

Israel's leadership in cyber security is notable for its advanced technologies, strong intelligence structure and private sector co-operation. However, this superiority is not without serious ethical violations and human rights issues. Spyware such as Pegasus, developed by the NSO Group, has caused international outcry by violating the privacy of individuals. Cyber-attacks on civilian infrastructure in Gaza have disabled communication networks and deepened humanitarian crises. AI-assisted targeting systems have led to the disproportionate use of force in wars, putting innocent civilian lives at risk. While Israel's cyber strategy stands out as an important tool in regional rivalries, cyber attacks are frequently used in tensions with countries such as Iran. While cyber operations such as Stuxnet prove Israel's effectiveness in cyber warfare, such attacks threaten international security. Moreover, the possibility of disabling strategic defence systems such as Iron Dome through cyber attacks further increases the importance of cyber security. Therefore, it is necessary to develop international cooperation, ethical regulations and control mechanisms in the field of cyber security. It is of great importance for global peace and security that cyber powers such as Israel prioritise the ethical use of cyber technologies. The aim of this study is to analyse the ethical violations and humanitarian violations committed by Israel by transferring its cyber power.

Keywords: Cyber Security, Israel, Ethical Violations, Cyber Warfare, Human Rights

GİRİŞ

Günümüzde ulusal güvenlik planlamacıları, reaktif ve taktiksel siber savunmadan proaktif ve stratejik siber savunmaya doğru bir yönelim göstermektedirler; bu da uluslararası askeri caydırıcılığı içermektedir. Nükleer silahların inanılmaz gücü, caydırıcılık stratejisinin doğmasına yol açmaktadır; burada orduların amacı savaşları kazanmak yerine onları engellemek olmaktadır. Siber saldırılar, nükleer patlamalarla kıyaslanamasa da, uluslararası güvenlik için ciddi ve artan bir tehdit yaratmaktadır (Geers, 2010, s. 298). Nitekim 21. yüzyılın hızla dijitalleşen dünyasında, teknolojik gelişmeler uluslararası ilişkilerde derin bir dönüşüm yaratmaktadır. Devletler, siber saldırıları ve dijital gözetim tekniklerini kullanarak artık savaş alanlarını sanal dünyaya taşımakta; güç mücadelesini, ağlar, veriler ve dijital

altyapılar üzerinden sürdürmektedir. Bu bağlamda, İsrail, bölgedeki stratejik hedeflerini gerçekleştirmek ve güvenliğini sağlamak amacıyla siber teknolojileri en üst düzeyde kullanan ülkelerden biri olarak öne çıkmaktadır. Siber teknolojilerin bu denli etkin bir şekilde kullanılması, uluslararası güvenlik paradigmasında değişimlere yol açarken, sivil haklar ve etik değerler açısından da çeşitli tartışmalara sebep olmaktadır. İsrail'in siber alandaki stratejik gücü, askeri kapasitelerinin yanı sıra teknoloji yatırımları ve siber güvenlik altyapısına verdiği önemden kaynaklanmaktadır. Özellikle son yıllarda, İsrail'in savunma ve güvenlik politikaları, dijital saldırı ve savunma sistemlerine büyük bir bütçe ayırmasıyla dikkat çekmektedir. Bu alandaki gelişmiş altyapı, İsrail'in bölgesel rakiplerine karşı üstünlük sağlamasına yardımcı olurken, aynı zamanda uluslararası kamuoyunda tepki çekmesine neden olmaktadır. İsrail'in siber saldırı politikalarının, bölgedeki sivil altyapılara ve toplumlara yönelik de tehditler oluşturması, ciddi bir etik sorun olarak değerlendirilmektedir.

Siber dünyada bilgilere ve bilgi sistemlerine yönelik artan kötü niyetli girişimler ve saldırılar, "siber güvenlik-savunma" kavramını gündeme getirmiştir. Diğer yandan, karşı tarafın bilgi ve sistemlerine zarar verme ya da olumsuz etkiler yaratma isteği "siber saldırı-taarruz" kavramını ortaya çıkarmıştır. Bilgi ve iletişim teknolojilerinin gelişmesiyle siber ortamın sunduğu fırsatlar, yaşamı giderek daha bağımlı hale getirirken; bu ortamın tehdit, saldırı, can ve mal güvenliğini tehlikeye sokma gibi amaçlarla kullanılması, bireyler, toplumlar ve ülkeler üzerinde büyük kayıplara neden olmuş; dolayısıyla güvenlik anlayışında önemli bir değişim süreci başlamıştır (Şenol, 2016, s. 10-11). Siber savaşın, fiziksel savaşlardan farklı bir dinamiğe sahip olması, uluslararası hukuk açısından yeni ve karmaşık meseleleri de beraberinde getirmektedir. Uluslararası hukuk kuralları, ülkelerin egemenlik haklarını korurken; siber saldırılar, sınır ötesi, hızlı ve çoğunlukla iz bırakmayan yapısı nedeniyle bu kuralların dışında kalabilmektedir. İsrail'in siber saldırılarının uluslararası hukuku ihlal edip etmediği, sık sık tartışılmakta ve bu saldırıların etik sınırları zorladığı savunulmaktadır. Özellikle, siber saldırıların etkileri sadece hedef ülkeleri değil, bölgedeki tüm toplumsal düzeni de tehdit edebilmektedir.

Her ne kadar etik dışı birçok faaliyette bulunsa da İsrail, siber güvenlik alanında yenilikçi bir güç olarak, sızma testleri için kullanılan işletim sistemleri ve güvenlik araçlarının geliştirilmesinde etkin bir rol üstlenmiştir. NATO üyesi ülkeler kadar, NATO dışındaki Çin ve Rusya gibi ülkeler de İsrail'in geliştirdiği siber savunma teknolojilerinden faydalanmaktadır. İsrail'in ürettiği çözümler, birçok ülkenin bilgi güvenliği denetimlerinde ve mevzuatlarında yer bulmakta, bu alanda geniş bir şekilde kullanılmaktadır (Bozkurtlar, 2021,

s.9). İsrail'in siber saldırılarında hedef aldığı alanların başında ise enerji, su ve sağlık gibi kritik altyapılar gelmektedir. Bu tür saldırılar, sadece bir ülkenin askeri gücünü değil; aynı zamanda sivil toplumun günlük yaşamını, ekonomisini ve psikolojik sağlığını da doğrudan etkilemektedir. Özellikle sağlık sistemleri ve altyapılara yönelik siber saldırılar, sivil halk üzerinde büyük zararlar bırakabilir ve bu tür saldırıların hedef alınması, savaş hukuku açısından kabul edilemez bulunmaktadır. İsrail'in bu tür kritik altyapılara yönelik saldırılar gerçekleştirmesi, siber teknolojinin etik dışı kullanımının en net örneklerinden biri olarak değerlendirilmektedir.

İsrail'in büyük ve gizli savunma Ar-Ge faaliyetleri, çoğu zaman gelişmiş ve bilgi teknolojileri yoğun sistemlerin ortaya çıkmasına yol açan kapsamlı tematik araştırmalar yürütmektedir. Bu çalışmalar, istihbarat toplama ve işleme sistemleri, hassas güdümlü mühimmat, insansız hava araçları (İHA) ve aktif füze savunma sistemleri gibi gelişmiş teknolojilerle sonuçlanmaktadır. Savunma Ar-Ge harcamalarının, ülkenin GSYİH'sinin %1,5'ine ulaştığı tahmin edilmektedir. İsrail, savunma araştırmaları için özel bir askeri akademi ya da araştırma enstitüsü yerine, akademik ve sanayi kurumlarını kullanmaktadır (Tabansky & Ben Israel, 2015, s.20). Bu sebeplere bağlı olarak istihbarat toplayabilmek adına İsrail'in siber saldırıları, sivil toplumların mahremiyetine yönelik de ciddi bir tehdit oluşturmaktadır. Özellikle dijital casusluk ve izleme sistemleriyle, kişisel verilerin toplanması ve bireylerin izlenmesi, gizlilik haklarının ihlali olarak yorumlanmaktadır. İsrail, geliştirdiği casus yazılımları hem kendi stratejik çıkarlarını korumak hem de diğer ülkelerde bilgi toplamak için kullanmaktadır. Bu durum, bireylerin özel hayatlarına yönelik müdahalelerin etik ve hukuki sınırlarını zorlamakta, siber güvenliğin ötesinde toplumsal bir tehdit olarak karşımıza çıkmaktadır. İsrail'in siber savaş stratejilerinin yalnızca savunma amaçlı olmadığı, aynı zamanda saldırı amaçlı bir politika izlediği yönünde eleştiriler bulunmaktadır. Siber teknolojilerin böylesine yaygın bir şekilde kullanımı, İsrail'i siber savaş konusunda küresel bir tehdit haline getirebilirken, siber saldırıların kontrolsüz bir şekilde yayılması, dijital dünyada yeni bir güvenlik açığı oluşturmaktadır. Bu güvenlik açığı, sadece İsrail'i değil, diğer birçok ülkeyi de siber saldırılara karşı savunmasız bırakmaktadır.

Tüm bunlara ek olarak, İsrail'in siber operasyon stratejisi, sağlamlık, dayanıklılık ve savunmadan oluşan "Üç Katmanlı Çerçeve"ye dayanır. İlk katman olan "sağlamlık," bir organizasyonun geniş koşullarda siber tehditlere karşı direnç gösterme yeteneğidir (Adamsky, 2017, s. 117). Kısacası bu makale, İsrail'in siber saldırı ve güvenlik politikalarının bölgedeki olumsuz etkilerini, insan hakları ve uluslararası hukuk açısından değerlendirmeyi

amaçlamaktadır. Siber teknolojilerin askeri stratejilerde bu denli merkezi bir rol üstlenmesi, devletlerin sorumluluklarını yeniden gözden geçirmesi gerektiğini göstermektedir. Özellikle sivillerin güvenliği ve mahremiyeti üzerindeki etkileri göz önünde bulundurulduğunda, bu saldırıların kontrolsüz bir şekilde yayılması, siber güvenlik ve etik alanında ciddi sorunlara neden olmaktadır. İsrail'in siber savaş ve saldırı politikaları, hem bölgesel hem de uluslararası düzeyde güvenlik, etik ve hukuk alanlarında derin tartışmalara yol açmaktadır. Bu bağlamda İsrail'in siber teknolojileri kullanımının yaratabileceği potansiyel zararlar üzerine kapsamlı bir analiz sunulacaktır. Dolayısıyla, İsrail'in siber savaş alanındaki teknolojik gücünü ve bu gücün yarattığı etik sorunları incelemek için literatür taraması yöntemi kullanılacaktır. Literatür taraması kapsamında, siber savaşlar, İsrail'in siber güvenlik ekosistemi ve etik boyutlarla ilgili mevcut akademik çalışmalar, resmi raporlar, politika belgeleri ve güvenilir haber kaynakları sistematik olarak analiz edilerek, konunun güncel durumu ve farklı perspektifleri ortaya konulacaktır.

1. SİBER GÜVENLİK VE SAVAŞLARDA TEKNOLOJİ KULLANIMI

Clausewitz'in (akt. Rid, 2012) savaş kavramı, üç temel unsura dayanmaktadır: şiddet, araçsallık ve politik doğa. Bu unsurlar, herhangi bir saldırı veya savunma eyleminin bir savaş olarak nitelendirilebilmesi için birlikte bulunmalıdır. Geçmişteki birçok siber saldırı, bu unsurların tümünü karşılamadığı için savaş olarak kabul edilmez. İlk unsur olan şiddet, savaşın temel karakteristiğidir. Clausewitz'e göre, savaş, düşmanı istenilen bir sonuca zorlamak için güç kullanımını içerir. Şiddet unsuru olmaksızın bir eylem, "savaş" teriminin metaforik bir kullanımı olmaktan öteye geçemez. Gerçek bir savaş eylemi, fiziksel olarak ölümcül veya en azından potansiyel olarak ölümcül olmalıdır. Bu şiddet, savaşan tarafların sürtüşme ve belirsizliklerden etkilenmediği durumlarda kontrolsüz bir şekilde artma eğilimindedir. İkinci unsur, savaşın araçsal karakteridir. Clausewitz'e göre, savaş bir araçtır ve her aracın bir amacı olmalıdır. Bu bağlamda, şiddet bir araç, düşmanın iradesini kırma hedefi ise amaçtır. Bu araçsal yaklaşım, savaşın taktik, operasyonel, stratejik ve politik düzeyde gerçekleşen çok yönlü bir süreç olduğunu gösterir. Amaç, rakibi çaresiz bir pozisyona getirmek ve iradesi dışında karar vermeye zorlamaktır. Bu nedenle, araç ve amaç arasındaki bu ilişki savaşın temel bir özelliğidir. Üçüncü unsur, savaşın politik doğasıdır. Savaş, daima politik bir amaca hizmet eder ve izole bir eylem olamaz. Clausewitz'in ünlü ifadesiyle, "Savaş, politikanın başka araçlarla devamıdır." Bu bakış açısına göre, savaşın politik bir varlık veya temsilci tarafından yürütülmesi ve bu varlığın iradesinin çatışma sırasında açıkça

ortaya konması gerekir. Politik doğası nedeniyle savaş, her zaman bir politik hedefe hizmet eder ve bu hedef, savaş sürecini yönlendiren asıl itici güçtür.

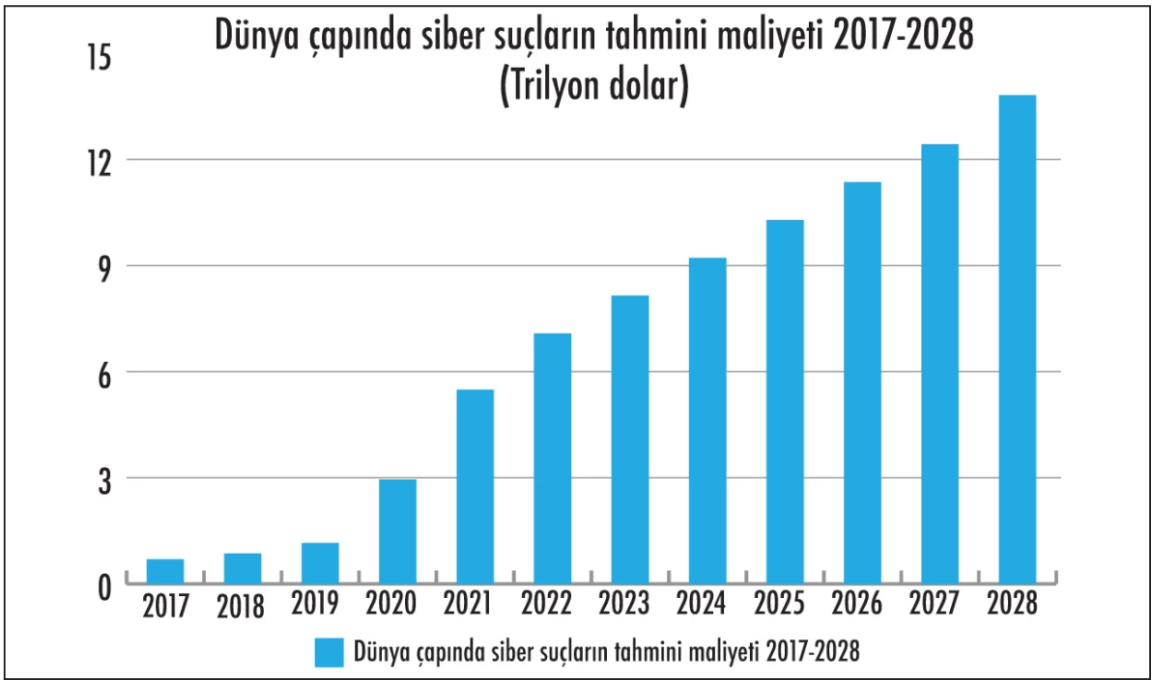
Literatüre bakıldığında, yeni savaş türlerini tanımlayan kavramlar arasında ortak bir dil bulunmamaktadır. Yazarlar, olguları açıklamak için farklı terimler geliştirmiş ve bu durum, alanın rekabet eden terimlerle dolmasına neden olmuştur. Askeri işlerde devrim (RMA), dördüncü nesil savaş, elektronik savaş, bilgi savaşı, ağ merkezli savaş ve siber savaş bu bağlamda öne çıkan kavramlardır. Bu yeni tür çatışmaları anlamak, etkili politikalar geliştirmek açısından kritik öneme sahiptir. Nükleer patlamalar milyonlarca insanın ölümüne yol açsa da, büyük bir siber saldırının toplumsal düzeni bozma etkisi benzer düzeyde ciddi olabilir. Cetron ve Davies (akt Greathouse, 2013, s.23) bu durumu "kitlesel imha silahları değil, kitlesel bozulma silahları" olarak tanımlamaktadır. Şangay İşbirliği Örgütü de "bilgi savaşı"nı, devletlerin birbirine karşı bilgi alanında yürüttüğü, siyasi, ekonomik ve sosyal sistemleri baltalamayı ve toplumu istikrarsızlaştırmayı amaçlayan bir çatışma olarak tanımlamaktadır. Bu tanım, bilgi savaşının uluslararası çatışmalardaki yıkıcı etkisini vurgulamaktadır.

Siber savaşlar hem devletler hem de kurumlar düzeyinde gerçekleşmektedir. Zira siber silahlar, kurumları hedef alarak fiziksel zarar verme ve istihbarat toplama amacıyla kullanılan gelişmiş dijital araçlardır. Bu silahlar genellikle devlet destekli operasyonlar kapsamında üretilirken, bazen devlet dışı aktörlerin de bu araçlara erişebildiği iddia edilmektedir. Stuxnet, endüstriyel kontrol sistemlerine zarar vererek nükleer santrifüjleri sabote etmesiyle dikkat çekerken, Night Dragon, küresel petrol ve enerji şirketlerine saldırılar düzenlemiştir. Flame, karmaşık bir siber silah olarak, bilgi çalma amacıyla devlet kurumlarını hedeflemiş, Duqu ise endüstriyel sistemlerden bilgi toplayarak gelecekteki saldırılara zemin hazırlamıştır. Gauss, bireysel hedeflere yönelik bir casusluk operasyonu yürütürken, Shamoon, özellikle Suudi Arabistan'daki petrol tesislerini hedef alarak büyük çapta kesintilere neden olmuştur. Duqu 2.0 ise İran’ın nükleer programıyla ilgili müzakerelere katılan ülkelere karşı siber casusluk operasyonları yürütmüştür (Çahmutoğlu, 2020, s.10-11). Bu örnekler, siber silahların yalnızca ekonomik ve askeri alanlarda değil, diplomatik süreçlerde de etkili olabildiğini göstermektedir. Siber uzayda güç mücadelesinin bir parçası haline gelen bu araçlar, uluslararası güvenlik dengelerini de doğrudan etkilemektedir.

Devlet destekli siber saldırılar daha çok hükümetler veya devletle bağlantılı kurumlar tarafından gerçekleştirilen yasa dışı, suç teşkil eden veya yıkıcı bilgisayar tabanlı eylemler

olarak tanımlanmaktadır. Son yıllarda bu tür saldırılarda önemli bir artış gözlemlenmiştir. Her ne kadar teknolojik gelişmeler saldırıların izini sürmeyi kolaylaştırsa da, bağımsız olarak doğrulanabilir kanıt elde etme zorluğu, saldırgan devletlerin gizlenmesini ve bu tür saldırıları teşvik etmesini sağlamaktadır. Literatürde devlet destekli siber saldırılar üç ana kategoriye ayrılmaktadır. İlk kategori, bu saldırıların askeri güdülerine odaklanır. Bazı araştırmacılar, siber saldırıların zayıf askeri güce sahip devletler için geleneksel silahlı çatışmalara alternatif olarak kullanılabileceğini savunmaktadır. Teknolojiye olan bağımlılık, güçlü devletlerin savunmasız kalabileceği açıklar yaratmaktadır. Diğer bir görüşe göre ise siber saldırılar, konvansiyonel askeri operasyonları tamamlayıcı bir unsur olarak kullanıldığında daha etkili olmaktadır (Akoto, 2021). Bu bağlamda, siber saldırılar modern savaş stratejilerinin ayrılmaz bir parçası haline gelmiştir. Özellikle altyapı sistemlerini hedef alan saldırılar, ekonomik ve toplumsal istikrarı tehdit edebilecek boyutlara ulaşmaktadır. Devletlerin bu saldırılara karşı siber savunma kapasitelerini artırmaları ve uluslararası iş birliğini güçlendirmeleri gerekmektedir. Aksi halde, siber saldırılar, yalnızca askeri değil, ekonomik ve sosyal alanlarda da derin etkiler yaratabilmektedir.

Nitekim ekonomik kayıpları da göz önünde bulundurmak gerekmektedir. 2010 yılında Symantec ve Ponemon Enstitüsü tarafından hazırlanan raporda, siber saldırıların firma başına yıllık ortalama kaybının 7,24 milyon dolar olduğu belirtilmiştir. 2012 yılında Ponemon Enstitüsü tarafından yapılan çalışmada ise haftalık başarılı siber saldırı sayısının 50'den 102'ye, saldırılardan kurtarma süresinin 14 günden 24 güne çıktığı ve yıllık ortalama kaybın 6,5 milyon dolardan 8,9 milyon dolara yükseldiği rapor edilmiştir. Bu veriler, siber güvenliğin sadece teknolojik değil, aynı zamanda ekonomik bir sorun olarak ele alınması gerektiğini vurgulamaktadır. Anderson da bilgi güvenliğini finansal açıdan çözülmesi zor bir problem olarak tanımlamaktadır (Şentürk vd., 2016, s.39-40). Tüm bu kayıplar, devletlerin siber saldırılarla mücadele etmek için artan bütçeler ayırmasını ve güvenlik altyapılarına daha fazla yatırım yapmasını zorunlu kılmaktadır. Ayrıca, siber saldırıların ekonomik maliyeti yalnızca doğrudan finansal kayıplarla sınırlı kalmayıp itibar zedelenmesi ve devletlerin bilgilerinin ele geçirilmesine de neden olmaktadır.



Şekil 1: Dünya Çapında Siber Suçların Tahmini Maliyeti
Kaynak: (Doğaner,2024)

Şekil 1'de dünya çapına gerçekleşen siber suçların tahmini maliyeti görülmektedir. 2017'den 2028'e kadar dünya çapında siber suçların tahmini maliyetindeki sürekli artışı göstermektedir. 2020 itibarıyla hızlı bir yükseliş trendine giren bu maliyet, 2028 yılında 15 trilyon dolara ulaşması beklenen bir seviyeye çıkmıştır. Bu artış, siber suçların etkisinin giderek daha büyük ekonomik sonuçlara yol açtığını ortaya koymakta ve dijital güvenlik önlemlerinin yetersizliğine dikkat çekmektedir. Grafik ayrıca, teknolojinin yaygınlaşmasıyla birlikte siber tehditlerin ve bunların mali etkilerinin de hızla büyüdüğünü vurgulamaktadır. Bu durum, hem bireyler hem de devletler için siber güvenlik yatırımlarının artırılması gerektiğini göstermektedir.

2. İSRAİL'İN SİBER GÜÇ KAPASİTESİNİN TARİHSEL GELİŞİMİ VE SİBER GÜVENLİK POLİTİKALARI

Siyonist siyasi ideoloji, 19. yüzyıl Avrupa'sındaki modern milliyetçilikle birlikte ortaya çıkmış ve İsrail topraklarında bir Yahudi demokratik devleti kurarak Yahudi diasporasının bu topraklara toplanmasını hedeflemiştir. Ancak, değişken jeopolitik ortam bu hedefi oldukça zorlu hale getirmiştir. İsrail'in kurucu liderleri, sürekli olarak aşağıdaki unsurları içeren bir ulusal güvenlik stratejisi geliştirmiştir. İsrail'in siber güvenlik stratejisi, ulusal güvenlik anlayışının bir parçası olarak erken dönemlerde şekillenmiştir. İsrail, 1990'lardan itibaren bilgi teknolojilerine ve dijital altyapılara ciddi yatırımlar yaparak siber alanda dünya lideri bir

güç haline gelmiştir. Savunma amaçlı geliştirilen teknolojiler, siber güvenlik sektörünün temelini oluşturmuş, üniversitelerle iş birliği içinde inovasyon ekosistemini güçlendirmiştir. Özellikle İsrail Savunma Kuvvetleri'nin (IDF) 8200 Birimi, siber güvenlikte öncü bir rol üstlenmiş ve bu alanda birçok yeniliğin öncüsü olmuştur. İsrail'in uluslararası arenada siber güç olarak tanınmasını sağlayan temel adımlardan biri, 2010 sonrası dönemde özel sektördeki şirketlerin ve start-up ekosisteminin devlet destekli güvenlik yaklaşımlarıyla entegre olmasıdır. Aynı zamanda, siber saldırılara karşı savunma yetenekleri, ulusal güvenlik stratejilerinin vazgeçilmez bir parçası haline gelmiştir. Bu süreç, İsrail'in sadece siber savunma değil, siber saldırı yeteneklerinde de küresel liderlerden biri olmasını sağlamıştır (Tabansky, 2016, s. 55-56).

İsrail, 2002 yılında kritik altyapıların korunması (CIP) için 84/B kararı ile dünyanın öncülerinden biri olmuştur. Bu karar, Ulusal Bilgi Güvenliği Otoritesini (NISA veya Re'em) ve politika odaklı bir yönlendirme komitesini CIP'nin uygulanmasından sorumlu kılmıştır. Ancak hükümet, İkinci İntifada'nın (2000-2005) getirdiği yüksek gerilim nedeniyle hızlı ve etkili çözümler ararken, bu görevi Shin Bet'e (İsrail İç Güvenlik Servisi) verdi. Shin Bet'in uzmanlığı sayesinde kısa vadede başarı sağlanırken, uzun vadede eleştiriler ortaya çıkmıştır. NISA'nın Shin Bet'in bir parçası olması, ajansa geniş yetkiler ve önemli ölçüde bilgiye erişim sağlamış, ancak bu durum inovasyonu ve ekonomik büyümeyi kısıtlamıştır. Ayrıca, güvenlik önlemlerinin maliyetinin, bu önlemlerden etkilenen kuruluşlar tarafından karşılanması zorunluluğu tepki toplamıştır (Frei, 2020, s.10).

Siber teknolojilerin askeri alanda bir silah olarak kullanılması beklentisi, pratikte göründüğü kadar basit olmadığını ortaya koymuş, ancak sivil sistemlerin bilgisayarlarını hedef almanın çok daha kolay olduğu anlaşılmıştır. Bu durum, Orta Doğu'nun en dijitalleşmiş ülkesi olarak ifade edilen İsrail'in, böyle bir saldırıya karşı potansiyel olarak son derece savunmasız olduğu gerçeğini savunma güvenlik tasarımcılarının fark etmesine yol açmıştır. Bu farkındalık, aralarında bu makalenin yazarının da bulunduğu, İsrail Savunma Bakanlığı Savunma Ar-Ge Direktörlüğü liderleri tarafından yönlendirilmiştir. 2002 yılında İsrail hükümeti, elektrik üretim tesisleri ve su temin sistemleri gibi kritik altyapıları denetlemek ve korumak amacıyla "Bilgi Güvenliği Otoritesi" (Information Security Authority) adıyla yeni bir kurum oluşturmuştur. Bu girişim, İsrail'i gelecekteki siber savaşlara hazırlanan dünyadaki ilk ülke haline getirmiştir. Bu adım, yüzeyde göründüğünden daha derin bir anlayışın sonucuydu. Kritik sistemlerin bilgisayarlı kontrol cihazlarına olan bağımlılığı o kadar artmıştı ki, bu

cihazların bozulmasının yalnızca “sanalla” sınırlı kalmayıp, gerçek fiziksel zararlara yol açabileceği anlaşılmıştır. Bu durum, bilgi güvenliği çağının sona erdiğini ve siber güvenlik çağının başladığını göstermiştir. Siber teknolojilerle fiziksel zarar verme potansiyeli, 2010 yılında İran’ın uranyum zenginleştirme tesislerindeki santrifüjlerin çökmesiyle küresel farkındalığa taşınmıştır (Ben Israel, 2021). Bu olay, “sanal” siber saldırılar yoluyla fiziksel zarar vermenin mümkün olduğunu ilk kez geniş bir kitleye göstermiştir. Güneşli bir günde çakan şimşek etkisi yaratan bu durum, konunun geniş bir kamuoyu tartışması haline gelmesine neden olmuştur.

İsrail, 2011 yılında siber güvenlik alanında küresel bir lider olma hedefiyle 3611 kararını çıkarmıştır. Bu karar, sadece güvenlik değil, aynı zamanda teknolojik, diplomatik ve ekonomik ilerleme hedeflerini de içermiştir. 3611 kararı ile Ulusal Siber Büro (INCB) kuruldu ve ulusal siber savunma stratejisi için 27 spesifik hedef belirlenmiştir. Bu hedefler arasında; bilgi paylaşım platformlarının oluşturulması, siber saldırıları tespit ve engellemeye yönelik teknolojilerin geliştirilmesi, araştırmaların desteklenmesi ve siber güvenlik alanında insan kaynağının artırılması yer almıştır. Ayrıca, bu karar, hükümet ile özel sektör arasındaki iş birliğini dengelemesiyle önceki 84/B kararına göre önemli bir ilerleme olarak değerlendirilmiştir. 2015 yılında alınan 2443 kararı ile Ulusal Siber Güvenlik Ajansı (NCSA) faaliyete geçirilmiştir. NCSA, Shin Bet’in CIP görevlerinin büyük bir kısmını devralarak daha bağımsız ve kapsayıcı bir yapıya kavuşmuştur. Ajans, işletmelerin sınırlı insan ve finansal kaynaklarına destek sağlamak, hukuki çerçeveler oluşturmak ve siber olaylara müdahale için sektörel ekipler (CERT-IL) kurmak gibi görevleri üstlenmiştir. Aynı yıl alınan 2444 kararı ise NCSA’ya ulusal siber doktrini geliştirme sorumluluğunu vermiştir. Bu karar ile uluslararası iş birliği, kamu bilgilendirme çalışmaları, lisanslama, denetim, eğitim ve düzenlemelere odaklanılmıştır. 2017 yılında alınan 3270 kararı ile Ulusal Siber Direktörlük (INCD) kurulmuştur. Bu yapı, NCSA ve INCB’yi birleştirerek daha merkezi ve etkin bir siber güvenlik yönetimi sağlamıştır. INCD, İsrail’in siber güç statüsünü güçlendirmek ve ulusal güvenlik, ekonomi ve teknoloji alanlarında daha entegre bir strateji izlemek amacıyla çalışmalarına başlamıştır (Frei, 2020, s.10).

İsrail, siber çağın getirdiği tehditlere ve fırsatlara erken önlem alan ilk ülkelerden biridir. Siber alan, İsrail'in ulusal yaşamını derinden etkileyerek hem ekonomik büyümenin itici gücü hem de askeri bir avantaj alanı haline gelmiştir. Dünya nüfusunun sadece %0,001’ini temsil eden İsrail, ABD hariç dünya genelindeki tüm siber girişimlerle eşdeğer sayıda girişime ev

sahipliği yapmaktadır. Ancak, bu bağımlılık beraberinde güvenlik açıklarını da getirmektedir. İsrail, siber alana rakiplerinden çok daha fazla bağımlı olduğu için saldırılara karşı daha savunmasızdır. 2023'ün başlarında, İsrail ekonomisini ciddi şekilde etkileyebilecek 1.000'den fazla saldırı engellenmiştir. Gazze'deki Hamas'a karşı savaşın ilk aylarında ise bu sayı 3.400'e yükselmiştir. Kritik altyapı sistemleri, İsrail Savunma Kuvvetleri (IDF) ve istihbarat sistemleri hedef alınmıştır. Siber saldırılar, yalnızca ekonomik değil, askeri operasyonlar üzerinde de büyük etki yaratma potansiyeline sahiptir. Basit bir trafik ışığı kesintisi bile kuvvetlerin harekete geçirilmesini geciktirebilmektedir. Bu nedenle, İsrail'in siber güvenlik stratejisi hem bir zorunluluk hem de bir fırsat olarak görülmektedir. İsrail'in toplum yapısı ve teknolojik yetkinlikleri, siber alandaki bu stratejik yaklaşımı desteklemektedir (Freilich, 2023, s.5). Siber gücün bir ayağı da savunma sistemleridir. Bu noktada Demir Kubbe Hava Savunma Sistemi'ne de değinmek gerekmektedir.

Demir Kubbe**,** İsrail'in geliştirdiği ve kısa menzilli roketlere karşı oldukça etkili bir hava savunma sistemi olarak bilinmektedir. Demir Kubbe'nin kökenleri, İsrail'in 1990'lı yıllardan itibaren yaşadığı roket saldırıları ve artan güvenlik tehditlerine dayanmaktadır. Özellikle Lübnan'daki Hizbullah ve Gazze Şeridi'ndeki Hamas gibi grupların İsrail'e düzenlediği roket saldırıları, İsrail'i etkili bir hava savunma sistemi geliştirmeye yöneltmiştir. Bu ihtiyaç doğrultusunda, İsrail Savunma Bakanlığı, Rafael Advanced Defense Systems ve Israel Aerospace Industries gibi şirketlerle işbirliği yaparak Demir Kubbe projesini başlatmıştır. Demir Kubbe'nin kuruluş tarihi kesin olarak belirtilmese de, 2000'li yılların başında proje aşamasına geçildiği ve 2011 yılında aktif olarak kullanılmaya başlandığı bilinmektedir. 2006 İsrail-Hizbullah Savaşı, Demir Kubbe'nin geliştirilmesi için önemli bir dönüm noktası olmuştur. Bu savaşta Hizbullah'ın İsrail'e yaptığı yoğun roket saldırıları, İsrail'in böyle bir sisteme ihtiyacı olduğunu bir kez daha ortaya koymuştur. Demir Kubbe, radar sistemleri, komuta kontrol merkezleri ve kesici füzelerden oluşan entegre bir sistemdir. Sistem, radarlar sayesinde gelen roketleri tespit eder ve bu roketlerin yörüngelerini hesaplar. Daha sonra, kesici füzeler hedeflenen roketleri havada imha eder. Demir Kubbe, özellikle kısa menzilli ve orta menzilli roketlere karşı oldukça etkilidir (Şengül, 2019, s.28-29). Hızla gelişen teknoloji ve değişen tehditler karşısında, Demir Kubbe'nin sürekli olarak güncellenmesi ve iyileştirilmesi gerekmektedir. Bu da ek maliyetler ve kaynaklar anlamına gelir.

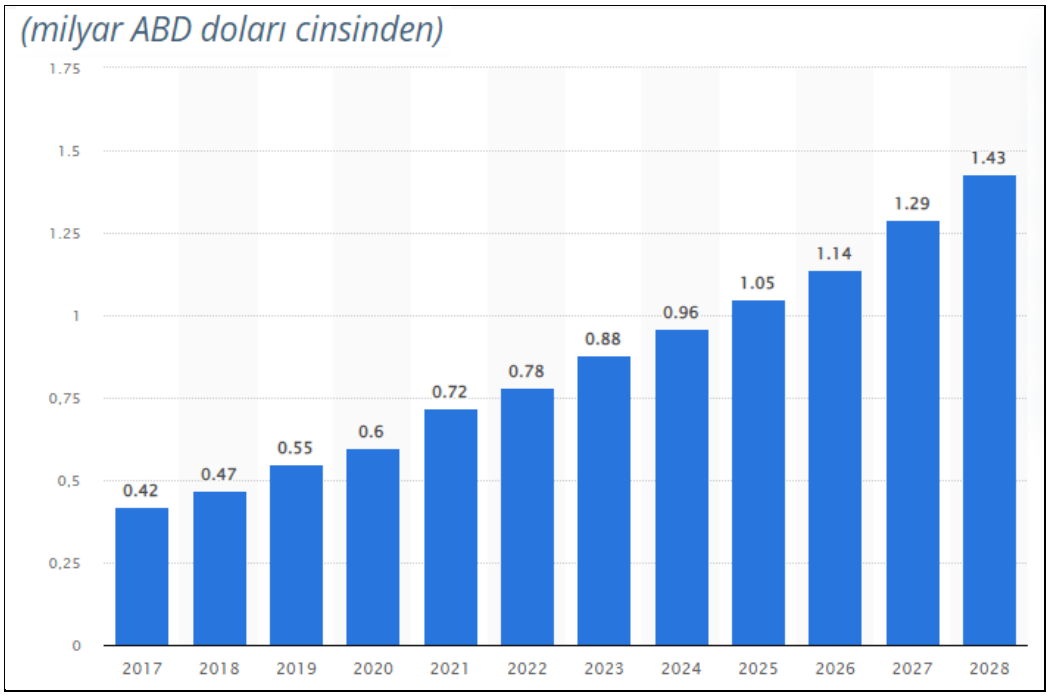
Tüm bunlara ek olarak; İsrail Ulusal Siber Direktörlüğü (INCD), siber güvenlik stratejilerini belirleyen ve uygulayan bağımsız bir organ olarak doğrudan Başbakan'a raporlama

yapmaktadır. Bu yapı, mevcut güvenlik kurumlarının siber güvenlik görevlerini üstlenmesinin bürokratik engeller yaratacağı düşüncesiyle oluşturulmuş ve siber güvenlikte kapsamlı, uzun vadeli bir yaklaşım benimsenmiştir. INCD, ulusal savunma kampanyalarını yönetmek ve siber tehditlere karşı stratejiler geliştirmekle sorumludur. Ayrıca uluslararası iş birliğini yönlendirir ve siber güvenlik alanındaki yasal çerçeveleri oluşturur. İsrailli uzmanlar, siber alandaki tehditlerin kimliğini tespit etmenin ve saldırganları ayırt etmenin zor olduğu gerçeğini göz önünde bulundurarak, geleneksel stratejilerden sapmışlardır. Bu yaklaşım, siber güvenlik ekosistemini daha geniş ve entegre bir şekilde ele alarak tüm ulusal güvenlik paydaşlarını birleştiren bir yapı kurmayı hedeflemiştir. INCD, siber güvenlik stratejilerini tek bir çatı altında toplayarak, ülke çapında etkili bir yönetim ve savunma sistemi kurmuştur (Adamsky, 2017).

Kısacası İsrail, siber güvenlik alanında önemli yatırımlar yaparak dünya çapında güçlü bir siber savunma altyapısı geliştirmiştir. Ülke, siber güvenliği ulusal güvenliğin ayrılmaz bir parçası olarak kabul etmekte ve bu alanda devlet, özel sektör ve akademi arasındaki işbirliğini teşvik etmektedir. İsrail, 2000'li yılların başından itibaren siber güvenlikteki stratejik önceliklerini belirleyerek, güçlü bir siber savunma kapasitesi oluşturmuş ve siber tehditlere karşı hızlı müdahale edebilmek için çeşitli savunma sistemleri geliştirmiştir. Bu yatırımlar arasında, Demir Kubbe gibi fiziksel savunma sistemleriyle entegrasyon sağlamak ve ulusal düzeyde siber tehditlere karşı etkili bir politika izlemek yer alır. Ayrıca, İsrail'in siber güvenlik alanındaki özel şirketleri de uluslararası pazarda önemli bir yer edinmiş ve ülkenin siber güvenlik sektörünü küresel çapta rekabetçi bir konuma getirmiştir.

İsrail’in siber gücünün durumu, Cyber Security Ventures adlı alandaki 500 önde gelen şirketin yer aldığı yıllık anketle ortaya konmaktadır. Bu ankette 354 Amerikan şirketi yer almakta, ardından 42 İsrail şirketi gelmektedir. Birleşik Krallık, İsrail’in yarısı kadar şirketle üçüncü sırada yer almakta ve ardından çeşitli diğer ülkelerden gelen şirketlerin uzun bir listesi takip etmektedir. Anketin sonuçlarına göre, İsrail’de bulunan ancak vergi ve ticaret sebepleriyle Amerika Birleşik Devletleri’nde kaydedilen yaklaşık 40 kadar İsrail şirketi daha bulunmaktadır. Dolayısıyla gerçek sayılar, 310 Amerikan şirketine karşılık 80 İsrail şirketi olmaktadır; yani dört kat daha fazla, oysa iki ülkenin ekonomileri ve nüfusları arasındaki oran çok daha yüksektir (Unna, 2019, s.171). Buna ek olarak veriler de İsrail’in siber güvenliğe ciddi bir yatırım yaptığını ortaya koymaktadır. Aşağıda yer alan Şekil-2’de görüldüğü gibi

İsrail'deki siber güvenlik pazarının 2017'den 2028'e kadar geliri milyar ABD doları cinsinden görülmektedir.



Şekil 2: İsrail'deki siber güvenlik pazarının 2017'den 2028'e kadar geliri
Kaynak: (Statista,2023)

Şekil 2'den de anlaşılacağı üzere; İsrail'deki siber güvenlik pazarının geliri, 2023 ile 2028 yılları arasında 0,88 milyar ABD doları ile 1,43 milyar ABD doları arasında artması beklenmektedir. Bu pazarın geliri gözlemlenen dönemde kademeli olarak artmıştır. Siber güvenlik, İsrail'deki yüksek teknoloji sektörünün önemli bir endüstrisidir. 2022 yılında, 2015 ile 2021 yılları arasında İsrail'deki siber güvenlik şirketlerine yapılan yatırımların sayısı artmıştır.

3. İSRAİL'İN SİBER GÜCÜNE YÖNELİK ETİK PROBLEMLER VE TEKNOLOJİK SİLAHLARIN SİVİL ZARARI

İsrail'in siber alanda caydırıcılık stratejisini kullanması, diğer güvenlik alanlarında uyguladığı "birikimli caydırıcılık" yaklaşımıyla benzerlik göstermektedir. Bu strateji, rakiplerini fiili güç kullanımıyla korkutmayı ve bir sonraki saldırıyı engellemeyi hedefler. Ancak bu stratejinin etkinliği tartışmalıdır. Dahası, İsrail'in bu stratejiyi nasıl uyguladığı – eğer gerçekten uyguladıysa – sınırlı ve dolaylı bir yaklaşıma işaret etmektedir. Yani, bu strateji, rakiplerin gözünde açık bir tehdit oluşturmaktan ziyade, dolaylı ve gizli bir caydırıcılık mekanizması olarak ortaya çıkmaktadır. Bir diğer önemli nokta, İsrail'deki politika yapıcıların, özellikle Başbakan Benjamin Netanyahu'nun, siber caydırıcılığın gerekliliğini vurgulamasıdır.

Netanyahu, siber savaşların "belirsiz ve öngörülemez" olduğunu ifade etmiş ve "siber alanda dengeyi sağlamak için savunma ile caydırıcılığın bir arada kullanılması gerektiğini" belirtmiştir. Ayrıca, siber saldırıların kaynağının genellikle gizli olması nedeniyle, caydırıcılığın sağlanmasının zorlaştığını ve bu konuya dikkat edilmesi gerektiğini söylemiştir (Lupovici, 2022, s.134). Bu söylemler, İsrail'in siber güvenliği, geleneksel askeri güvenlik yaklaşımlarına benzer bir şekilde ele aldığını göstermektedir.

İsrail'in Ulusal Siber Güvenlik Stratejisi, 2017 yılında yayımlandı ve ülkenin ulusal güvenliğiyle ilgili ikinci resmi belge oldu. İlk belge, David Ben-Gurion'un 1953'teki stratejik prensipleri hakkındaki açıklamalarıydı. Bu yeni belge, İsrail'in dijital savunma hedeflerini ve önceliklerini yeniden belirlemeyi amaçlıyor. Ayrıca, son 20 yılda geliştirilen kurumsal ve yasal çerçeveleri gözden geçirmeyi hedefliyor. Stratejinin temel noktalarından biri, tamamen sivil bir siber güvenlik alanı oluşturulmasıdır. Bu alan, askeri siber savunma ile desteklense de askeri faaliyetler bu stratejiye dahil edilmemektedir. İsrail'in siber güvenlik anlayışının en büyük farklarından biri, sivil ve askeri alanların açıkça ayrılmasıdır. Ayrıca, kamu-özel sektör iş birliğinin uygulanması, İsrail'in bilgi teknolojileri endüstrisini güçlü bir ekonomik sektöre dönüştürmüş ve ülkeyi uluslararası bir yüksek teknoloji merkezi yapmıştır. Günümüzde, İsrail, dijital güvenlik altyapısını özel şirketler ve girişim sermayesi fonları (örneğin, Jerusalem Venture Partners Cyber Labs) aracılığıyla kurmuş durumdadır. Ayrıca, yüksek teknoloji şirketleri ve akademik topluluklar arasındaki iş birliği ile birçok start-up ve araştırma projesi yürütülmektedir (Zhukova & Trushkina, 2023, s.179-180).

Casusluk ve etik dışı kullanım, özellikle gelişmiş teknolojiyle birlikte, kişisel gizliliği ihlal eden ve bireylerin güvenliğini tehlikeye atan ciddi bir sorun haline gelmiştir. İsrail, özellikle NSO Group'un Pegasus casus yazılımı gibi teknolojilerle, casusluk faaliyetlerinde ve etik dışı kullanımda tartışmalı bir rol oynamaktadır. Pegasus, İsrail merkezli NSO Group tarafından geliştirilen bir casus yazılımdır ve özellikle hedeflenen kişilerin telefonlarına gizlice sızarak tüm verileri toplar. 2011 yılında ilk kez tanıtılan Pegasus, başlangıçta Meksikalı yetkililerin ünlü suçlu El Chapo'yu yakalamalarına yardımcı olmuş, daha sonra Avrupa'da teröristlerin ve suç örgütlerinin yakalanmasında da kullanılmıştır. Bu yazılım, telefonlardaki çağrı kayıtları, rehberdeki kişiler, otomatik video ve ses kayıtları, konum verileri gibi kişisel bilgileri gizlice toplar. Pegasus, güvenlik güçlerinin suçluları tespit etmeleri için etkili bir araç gibi görünse de, aynı zamanda büyük bir gizlilik ihlali riski taşır. Pegasus'un yetenekleri oldukça gelişmiştir ve sadece canlı kamera görüntülerini hacklemekle sınırlı kalmaz. Aynı zamanda ekran görüntülerini okuyarak bu görüntüler hakkında geri bildirimde bulunabilir. Yazılım,

şifreli içerikleri aşabilir ve birçok farklı uygulama üzerinden takip yapabilir, örneğin Skype, WhatsApp, Viber gibi popüler iletişim araçlarında bile izleme yapabilir (Chawla, 2021, s.1). Ayrıca, GPS kullanarak hedeflerin konum bilgilerini hassas bir şekilde takip edebilir. Bu özellikler, Pegasus'u hem etkili hem de tehlikeli bir casus yazılım haline getirmektedir, çünkü kullanıcılar farkında olmadan izlenebilir ve kişisel bilgiler gizlice toplanabilir. Bu yazılım, yalnızca suçluları izlemek ve yakalamak için değil, aynı zamanda politikacıları, gazetecileri ve aktivistleri gözetlemek amacıyla da kullanılmıştır. Örneğin, bazı ülkelerde hükümetler, muhalefet liderlerinin telefonlarını dinlemek, gazetecilerin haber kaynaklarını ortaya çıkarmak ve toplumsal olayları kontrol etmek için Pegasus'u devreye sokmuştur. Bu tür kullanımlar, kişisel gizliliğin ihlali, ifade özgürlüğüne müdahale ve insan hakları ihlalleri gibi ciddi etik sorunları gündeme getirmektedir.

İsrail'e yönelik siber saldırılar da yapılmıştır. Uluslararası hacker grubu Anonymous, İsrail hükümetine ait ağ sitelerini hedef alarak geniş çaplı bir siber saldırı düzenlemiştir. Bu saldırılar, İsrail'in Gazze'ye yönelik askeri operasyonlarına tepki olarak 2012 Kasım ayında başlamıştır. Anonymous'un bu saldırılarının amacı, İsrail'in siber altyapısını hedef alarak medya aracılığıyla dikkat çekmekti. Ancak, İsrail Ulusal Siber Büro'su, saldırganların çoğu önemli siteyi kapatamadığını ve zarar vermediklerini açıklamıştır. İsrailli yetkililer, Anonymous'un bu saldırıyı medyada daha fazla yankı uyandırmak için düzenlediğini, amacının ülkenin hayati altyapısına zarar vermek olmadığını belirtmişlerdir. Yine de, saldırı sonucunda birçok web sitesine erişim engellenmiştir. 7 Nisan 2013'te ise Anonymous, "OpIsrael" adlı operasyonlarının devamı olarak İsrail Savunma Gücü ve önemli kurumlarının sitelerini hedef alan büyük bir siber saldırı düzenleyeceğini açıklamıştır. İsrail, Kasım 2012'de Gazze'deki operasyonları sırasında 44 milyon siber saldırıya uğradığını duyurmuştur. Bu saldırılar, dünya kamuoyunun İsrail'in politikalarına karşı tepkisini internet aracılığıyla dile getirmesine olanak tanımıştır (Polat, 2020, s.39-40). Bu tür büyük saldırıların çoğu bir devletin arkasında olsa da Anonymous'un eylemleri, hacker gruplarının organize olduğu ve bireysel tepkilerin de rol oynadığı bir durumdur.

Buna ek olarak "Lavender" ise İsrail ordusunun Hamas mensuplarını hedef olarak belirlemek için geliştirdiği bir yapay zekâ öneri sistemidir. Bu sistem, Gazze'deki bireyleri, kişisel özellikler, hareket desenleri, sosyal ilişkiler gibi verilerle analiz ederek, militan profilleriyle eşleştirmeye çalışır. Ancak sistemin en büyük sorunu, verilerin doğru bir şekilde analiz edilmemesi ve insan hatalarının da bu sürece dahil olmasıdır. "Lavender" hedefleri hızla

belirleyerek askeri "öldürme zincirini" otomatikleştirir ve bu da daha az insan denetimiyle daha hızlı kararlar alınmasını sağlar. Bunun sonucunda, potansiyel olarak masum insanlarla birlikte, gerçek hedefler de öldürülebilir. İsrail'in bu tür teknolojilere dayanarak hedef belirleme yapması, askeri stratejilerinde hız ve verimliliği ön plana çıkarırken, insan hakları ihlallerine ve masum insanların zarar görmesine yol açmaktadır. İsrail ordusunun bu sistemlere dayalı saldırı stratejileri, savaşın insani boyutunu göz ardı etmekte ve savaşta doğru hedeflerin seçilmesinin önünü açmaktadır. "Lavender" gibi sistemler, önyargılı veri setlerine dayanarak yanlış hedefler belirleyebilir ve bu durum, savaşın dehşetini artırmakta, insan hayatını göz ardı etmektedir (Schwarz, 2024). Saldırıların ilk haftalarında, İsrail ordusu, Lavender'ın işaretlediği her düşük rütbeli Hamas üyesi için 15 veya 20'ye kadar sivilin öldürülmesini "kabul edilebilir hata" olarak görmezden gelmiştir. Bu yaklaşım, askeri stratejilerin hız ve verimlilik adına insani kayıpları göz ardı etmesine yol açmış ve İsrail'in etik ihlallerini açıkça ortaya koymuştur. İsrail, Gazze'ye yönelik saldırılarda siber gücünü önemli bir stratejik araç olarak kullanmıştır. Bu saldırılarda, hem askeri operasyonları desteklemek hem de Hamas'ın iletişim altyapısını hedef almak amacıyla siber saldırılar gerçekleştirilmiştir. İsrail'in siber saldırıları, Hamas'ın dijital iletişim ağlarını keserek, grup içindeki bilgi akışını engellemeyi amaçlamıştır. Ayrıca, hedeflenen altyapılara yönelik siber saldırılarla Gazze'nin elektrik, internet ve telefon şebekelerine zarar verilmiş, bu da sivil halkın iletişim olanaklarını daha da kısıtlamıştır. Bu strateji, sadece askeri hedeflere yönelik değil, aynı zamanda psikolojik bir savaş unsuru olarak da kullanılarak, Gazze halkının moralini bozmayı hedeflemiştir. İsrail katliam yapmıştır. Gazze'ye yönelik saldırılarda, özellikle sivil yerleşim alanlarına yönelik yoğun hava saldırıları, onlarca masum insanın ölümüne yol açmıştır. Bu saldırılar, yalnızca askeri hedefleri değil, sivil altyapıları da hedef alarak, halkın temel yaşam koşullarını olumsuz yönde etkilemiştir. İsrail'in bu eylemleri, uluslararası hukuk ve insani normlara aykırı olarak, sivil kayıpların artmasına ve büyük bir insani krizin ortaya çıkmasına neden olmuştur.

Öte yandan; Ortadoğu'daki uzun süredir devam eden İran-İsrail rekabetinde, günümüzde İsrail'in pozisyonunun güçlendiği açıkça görülmektedir. İsrail, özellikle Körfez ülkeleri başta olmak üzere, Arap devletleriyle daha yakın ilişkiler kurarak bölgedeki siyasi, askeri ve ekonomik etkinliğini artırmıştır. Buna karşılık, İran daha çok Suriye, Lübnan, Yemen ve Irak gibi kriz içindeki kırılgan ülkelere nüfuz etmeye çalışmış, ancak burada kurduğu varlık, kendisine askeri, ekonomik ve diplomatik sorunlar yaratmakta, aynı zamanda düşmanlar edinmesine yol açmaktadır. İstihbarat faaliyetleri açısından bakıldığında, İsrail'in bölgedeki

ve İran içindeki etkisinin oldukça büyük olduğu gözlemlenmektedir. İsrail, gerçekleştirdiği operasyonlarla güvenlik, askeri ve istihbarat yeteneklerini test etmekte, İran'ın karşılık verme kapasitesini, zayıf yönlerini ve güvenlik açıklarını belirlemektedir. Dolayısıyla, İran'ın sert söylemleri karşısında, İsrail'in saldırıları ve diğer eylemleri, İran'ın söylem ve eylemlerindeki tutarsızlıkları da ortaya çıkarmaktadır. Sonuç olarak, İran'ın saldırılara karşı koyma konusundaki yetersizlikleri, güvenlik zafiyetleri ve kırılganlıkları, İsrail'i daha büyük operasyonlar için teşvik etmektedir (Mercan, 2021, s. 7). Hatırlanacağı üzere İsrail, İran'ın nükleer tesislerine yönelik siber saldırılar düzenleyerek, özellikle 2010'daki Stuxnet virüsüyle büyük zarar vermiştir. Bu saldırılar, İran'ın askeri ve endüstriyel altyapısını hedef almıştır. Günümüzde de İsrail, siber saldırılarıyla İran'ın dijital güvenlik açıklarını kullanmaya devam etmekte, İran ise karşılık olarak İsrail'in altyapılarına saldırılar düzenlemektedir. Her iki ülke de siber savaş alanında güçlü kapasitelere sahip olup, bu çatışmalar modern savaşın yeni boyutlarını oluşturmaktadır.

İsrail'in siber gücü dendiğinde değinilmesi gereken bir diğer husus da Mossad'dır. Mossad, İsrail'in ulusal istihbarat teşkilatıdır ve dış istihbarat toplama, casusluk ve terörle mücadele gibi görevlerle tanınmaktadır. Siber güvenlik alanında da aktif olan Mossad, siber saldırılar düzenleyerek düşmanlarının dijital altyapılarına zarar vermektedir. Mossad, yalnızca geleneksel casusluk faaliyetleriyle değil, aynı zamanda siber saldırılarla da etkili bir şekilde görev yapmaktadır. 2007 yılında gerçekleşen Orchard Operasyonu, bu tür bir siber-fiziksel saldırının önemli bir örneğidir. Bu operasyon kapsamında, Mossad, Suriye'nin Al-Kibar bölgesindeki gizli nükleer reaktörü hedef almıştır. Mossad, önce bir "truva atı" programı aracılığıyla, Suriye'nin üst düzey bir yetkilisinin bilgisayarına sızmış ve son derece hassas bilgileri ele geçirmiştir. Ardından, İsrail hava kuvvetleri, elektronik savaş yöntemlerini kullanarak Suriye'nin hava savunma sistemlerini etkisiz hale getirmiş, böylece İsrail jetlerinin Suriye hava sahasına girip hedefe ulaşmalarını sağlamıştır (Açıkalın, Baykız, 2024, s.209). Bu saldırı, hem siber güvenlik hem de askeri operasyonların birleştiği nadir bir örnek olup, Mossad'ın siber operasyonlarda ne denli ileri düzeyde teknik yeteneklere sahip olduğunu göstermektedir.

İsrail'in teknolojik ve istihbarat gücünü ortaya koyan bir diğer olay, çağrı cihazları ve telsizlerin patlatılmasıdır. 17 ve 18 Eylül 2024 tarihlerinde, Hizbullah tarafından kullanılacağı öngörülen binlerce çağrı cihazı ve yüzlerce telsizin, İsrail'in saldırıları sonucu Lübnan ve Suriye'de eş zamanlı olarak patladığı bildirilmiştir. Olayda, aralarında en az 12 sivilin de

bulunduğu toplam 42 kişinin hayatını kaybettiği ifade edilmiştir. Bu saldırı, Ekim 2023'te başlayan İsrail-Hizbullah çatışmasının ardından Hizbullah için yaşanan en büyük güvenlik ihlali olarak değerlendirilmiştir. Hizbullah'ın çağrı cihazları operasyonu, çok yönlü bir istihbarat ve elektronik harp saldırısı olarak görülmektedir. İsrail'in bu operasyonda sinyal istihbaratı, insani istihbarat, siber espiyonaj ve saldırgan siber saldırı araçlarını kullanmış olabileceği düşünülmektedir. Bu yöntemler nedeniyle operasyonun bir siber saldırı olarak tanımlanması olasılık dahilinde olsa da aslında elektronik harp olarak adlandırılmasının daha doğru olacağı savunulmaktadır. Operasyonun arkasında İsrail'in ordusunun, özellikle Unit 8200 biriminin olduğu düşünülmektedir. Hatırlanacağı üzere Hizbullah, telefonlarını analog çağrı cihazlarıyla değiştirmişti. Bu cihazlar üzerinden yapılan sabotajla, tedarik zincirine müdahale edilerek çağrı cihazlarının değiştirildiği öngörülmektedir. Bu operasyonun, çağrı cihazlarının üretim sürecine sızarak gerçekleştirildiği ve Hizbullah'a paravan bir şirket aracılığıyla satıldığı ihtimalleri üzerinde durulmaktadır. 3000 civarında çağrı cihazının modifiye edilmiş olduğu düşünülmektedir (Bıçakcı, 2024). İsrail'in çağrı cihazları ve telsizlere yönelik gerçekleştirdiği operasyon, etik açıdan tartışmalı bir durum ortaya koymaktadır. Savaş ve istihbarat stratejilerinin gerekçesi, askeri hedeflere ulaşmak olsa da, sivillerin ve masum kişilerin zarar görmesi, bu tür operasyonların etik sınırlarını sorgulatmaktadır. Ayrıca, tedarik zincirine sızarak cihazları manipüle etmek ve bu yöntemle hedefe ulaşmak, savaşta kullanılan taktiklerin insan hakları ve uluslararası hukuk açısından ne denli sorgulanması gerektiğini gündeme getirmektedir.

Yukarıda da değinildiği gibi Demir Kubbe, İsrail'in kısa menzilli roketler ve havan mermilerini tespit edip imha etmek için geliştirdiği, mobil bir hava savunma sistemidir. Geçmişteki bazı iddialara göre; Çin merkezli bir bilgisayar korsanı grubu, İsrail'in milyar dolarlık Demir Kubbe füze savunma sisteminden veri çalmıştır. Çin hükümeti tarafından desteklendiği düşünülen Comment Crew adlı hacker grubu, 2011 yılından itibaren, Demir Kubbe projesiyle ilişkili olarak, İsrail'in önde gelen savunma şirketlerinden Elisra Group, Israel Aerospace Industries (IAI) ve Rafael Advanced Defense Systems (RADS) hedef alarak siber saldırılar gerçekleştirmiştir. İsrail İnternet Derneği Genel Müdürü Dina Beer'in Bloomberg'e verdiği bilgiye göre, bu siber saldırılar, İsrail'in Filistin ile yaşadığı çatışmalar sırasında, İsrail'e yönelik siber tehditlerin arttığı bir döneme denk gelmiştir. Son dönemlerde İsrail Demiryolları ve hastanelerinin internet sitelerine yönelik saldırıların yanı sıra, İsraillilerin internet bağlantılarını yavaşlatan hizmet engelleme (DDoS) saldırıları da yaygınlaşmıştır (Gibbs, 2014).

Demir Kubbe’nin hacklendiği iddiaları çok daha yoğun şekilde medya gündemine gelmiştir. Türkiye'nin Milli İstihbarat Teşkilatı (MİT), İsrail'in Mossad teşkilatının hedef aldığı Filistinli hacker Omar A'yı kurtarmıştır. Omar A, Gazze'deki bilgisayar programcılığı eğitimini tamamladıktan sonra, İsrail'in Demir Kubbe füze savunma sistemini hackleyip, Filistin Direniş Grubu Hamas’a roket fırlatmalarını sağlamıştır. İsrail istihbaratı, üç yıllık araştırmanın ardından Omar A'yı hedef almış ve ona, Mossad ajanları aracılığıyla çeşitli iş teklifleri sunmuştur. 2022’de Omar, Malezya'da Mossad ajanları tarafından kaçırılmış ve işkence edilmiştir. MİT, Omar'ı gizlice izleyerek, yerini tespit etmiş ve Türk yetkililer, Malezya ile işbirliği yaparak onu kurtarmıştır. Bu operasyon, MİT’in İsrail'e karşı yürüttüğü karşı istihbarat faaliyetlerinin son örneği olmuştur (www.middleeastmonitor.com, 2023). Demir Kubbe gibi ileri düzey füze savunma sistemlerinin hacklenmesi teorik olarak mümkün olsa da, sistemler yüksek güvenlik önlemleriyle korunmaktadır. Ancak, geçmişte siber saldırılarla bu tür sistemlerin zafiyetlerinin hedef alındığı örnekler olmuştur.

İsrail, gelişmiş savunma teknolojilerini kullanırken, özellikle siber savaş ve elektronik harp alanlarında birçok etik ihlale yol açan uygulamalara imza atmıştır. Ayrıca, bazı durumlarda, İsrail'in elektronik savaş araçları ve casusluk faaliyetleri, manipülasyona sebep olurken sivil can ve mal kaybına da yol açmaktadır.

4. SONUÇ VE DEĞERLENDİRME

Anlaşılacağı üzere İsrail’in siber gücü, gelişmiş teknolojik altyapısı ve istihbarat kapasitesi sayesinde uluslararası arenada dikkat çekici bir konuma sahiptir. Ancak bu gücün kullanımı, etik ihlallerin artmasına ve insan haklarının ihlal edilmesine yol açmaktadır. Özellikle Pegasus gibi casus yazılımlar, devletlerin güvenliğini sağlama bahanesiyle sivillerin mahremiyetini ihlal ederek ciddi bir tehdit oluşturmaktadır. Bu durum, siber güvenliğin devletler için bir savunma aracı olmasının ötesinde, bireylerin temel haklarını tehdit eden bir mekanizmaya dönüşmesine neden olmaktadır.

İsrail’in siber stratejisinde caydırıcılık önemli bir yer tutsa da, bu stratejinin sivil alanlarda yol açtığı zararlar göz ardı edilemez. Gazze gibi bölgelerde gerçekleştirilen siber saldırılar, sivil halkın temel iletişim kanallarını devre dışı bırakarak insani krizleri derinleştirmektedir. Bu saldırılar, yalnızca askeri hedefleri değil, doğrudan sivil yaşamı hedef alarak savaş hukukunun ve insan haklarının ihlal edilmesine neden olmaktadır. Bu bağlamda, siber saldırıların askeri bir gereklilikten ziyade, masum siviller üzerinde yıkıcı bir etkiye sahip olduğu açıktır.

Yapay zeka destekli saldırı sistemlerinin kullanımı, siber savaşların insan unsuru gözetilmeksizin yürütülmesine yol açmaktadır. Hedef belirleme süreçlerinde yapay zekanın rolü, etik ihlalleri daha da artırmakta ve insan hayatının bir algoritmaya indirgenmesine sebep olmaktadır. Bu durum, savaşlarda orantısız güç kullanımına zemin hazırlayarak, uluslararası normların ihlaline yol açmaktadır. Siber teknolojilerin kontrolsüz bir şekilde kullanımı, etik sınırların belirsizleşmesine ve daha fazla insan kaybına neden olmaktadır.

İsrail'in siber gücü, bölgesel rekabetlerde de etkili bir araç olarak öne çıkarken, uluslararası güvenliği tehdit eden bir unsur haline gelmektedir. Stuxnet gibi siber saldırılar, rakip devletlerin altyapısını hedef alarak siber savaşın yıkıcı etkilerini gözler önüne sermektedir. Bu tür saldırılar, yalnızca hedef ülkelere zarar vermekle kalmamakta, aynı zamanda küresel barışı tehdit eden bir dinamiğe dönüşmektedir. Siber saldırıların kontrol altına alınmaması halinde, devletlerarasındaki çatışmaların siber alanlarda daha geniş bir yıkıma yol açması kaçınılmazdır.

Demir Kubbe gibi stratejik savunma sistemlerinin hacklenme ihtimali, siber güvenliğin savunma politikalarındaki kritik rolünü ortaya koymaktadır. Ancak bu sistemlerin siber saldırılarla devre dışı bırakılması, yalnızca askeri bir zafiyet değil, aynı zamanda etik bir problem olarak değerlendirilmektedir. Savunma sistemlerine yönelik siber saldırılar, milyonlarca insanın hayatını tehlikeye atarak, uluslararası toplumda endişe yaratmaktadır. Bu bağlamda, siber saldırıların kapsamı ve etkisi, siber güvenlik alanında etik kuralların ve uluslararası düzenlemelerin aciliyetini ortaya koymaktadır.

Kısacası İsrail'in siber gücü, hem bölgesel hem de küresel ölçekte önemli bir aktör olarak öne çıksa da, etik ihlallerin artması bu gücün meşruiyetini zedelemektedir. Siber saldırıların sivilleri doğrudan hedef alması ve bireylerin mahremiyetini ihlal etmesi, uluslararası toplumun daha güçlü bir tepki vermesini zorunlu kılmaktadır. Siber savaşların etik boyutları dikkate alınmaksızın yürütülmesi, gelecekte daha büyük insani krizlerin ve çatışmaların yaşanmasına yol açabilir. Bu nedenle, siber teknolojilerin etik ve sorumlu bir şekilde kullanılması, sadece devletlerin güvenliği için değil, aynı zamanda küresel barış için de hayati önem taşımaktadır.

Siber güvenlik alanında uluslararası işbirliği ve etik standartların geliştirilmesi, gelecekte olası ihlallerin önüne geçmek için kritik bir adımdır. İsrail ve diğer siber güçlerin, siber alanlarda hareket ederken insani değerleri ve etik sınırları göz önünde bulundurmaları gerekmektedir.

Aksi takdirde, siber savaşların sonuçları, fiziksel savaşlardan çok daha yıkıcı ve uzun vadeli olabilir. Bu nedenle, siber güvenlik alanında küresel bir düzen oluşturulması, tüm insanlık için daha güvenli bir gelecek inşa etmenin anahtarı olacaktır.

KAYNAKÇA

Açıkalın, Ş. N., & Baykız, T. (2024). Değişim Ve Dönüşümün Eşiğinde Siber Savaş. *Muhafazakar Düşünce Dergisi, 20*(67-Dijital Çağda Siyaset), 200-220.

Adamsky, D. (Dima). (2017). The Israeli Odyssey toward its National Cyber Security Strategy. *The Washington Quarterly, 40(2), 113–127.*

Akoto, W. (2021). *International trade and cyber conflict: Decomposing the effect of trade on state-sponsored cyber attacks. Journal of Peace Research, 002234332096454.* doi:10.1177/0022343320964549.

Ben Israel, I. (2021). "How did Israel become a Global Cyber Power?", *https://forbes.co.il/e/how-did-israel-become-a-global-cyber-power/*, Erişim Tarihi: 17.12.2024.

Bıçakcı, S. (2024). "Lübnan'da patlayan çağrı cihazları: Elektronik harp, siber sabotaj ve kötülüğün sıradanlığı, *https://fikirturu.com/jeo-politika/lubnanda-patlayan-cagri-cihazlari/,* Erişim Tarihi: 23.09.2024.

Bozkurtlar, B. (2021). "Ulus Devletlerin Siber Güvenlik Stratejileri Ve Siber Vatan Kavramıyla Bir Değerlendirme. *https://www.academia.edu/61993666/ULUS_DEVLETLER%C4%B0N_S%C4%B0BER_G%C3%9CVENL%C4%B0K_STRATEJ%C4%B0LER%C4%B0_VE_S%C4%B0BER_VATAN,* Erişim Tarihi: 09.11.2024.

Chawla, A. (2021). Pegasus Spyware–'A Privacy Killer'. *Available at SSRN 3890657*.

Çahmutoğlu, E. (2020). Siber Uzayda Güç ve Siber Silah Teknolojilerinin Küresel Etkisi. *Analytical Politics,* 1(1), 63-79.

Doğaner, A. (2024). "Siber saldırılara sigorta kalkanı", *https://istanbulticaretgazetesi.com/siber-saldirilara-sigorta-kalkani,* Erişim Tarihi: 19.12.2024.

Frei, J. (2020). Israel's national cybersecurity and cyberdefense posture. *Policy and Organizations. css. ethz. ch/en/publicatios/risk-and-resilience-reports.html*, Erişim Tarihi: 12.12.2024.

Freilich, C. D., Cohen, M. S., & Siboni, G. (2023). *Israel and the cyber threat: How the startup nation became a global cyber power*. Oxford University Press.

Geers, K. (2010). The challenge of cyber attack deterrence. *Computer Law & Security Review, 26*(3), 298-303.

Gibbs, S. (2014). Chinese hackers steal Israel's Iron Dome missile data, *https://www.theguardian.com/technology/2014/jul/29/chinese-hackers-steal-israel-iron-dome-missile-data,* Erişim Tarihi: 18.11.2024.

Greathouse, C. B. (2013). *Cyber War and Strategic Thought: Do the Classic Theorists Still Matter? Cyberspace and International Relations, 21–40.* doi:10.1007/978-3-642-37481-4_2

Lupovici, A. (2022). Uncertainty and the study of cyber deterrence. *Cyber Security Politics,*

Mercan, M.V. (2021). "Ortadoğu'da Nükleer Gerginlik: İran- İsrail Güç Mücadelesi", *İHH İnsani ve Sosyal Araştırmalar Merkezi Dergisi.*

Middleeastmonitor (2023). "Turkiye intelligence agency protects Palestinian hacker from Israel's Mossad, *https://www.middleeastmonitor.com/20231122-turkiye-intelligence-agency-protects-palestinian-hacker-from-israels-mossad/,* Erişim Tarihi: 11.10.2024.

Polat, S. (2020). Milli Güvenlik Açısından Siber Güvenlik, T.C. Ankara Hacı Bayram Üniversitesi Lisansüstü Eğitim Enstitüsü Amme İdaresi Anabilim Dalı Yüksek Lisans Tezi.
Rid, T. (2012). Cyber war will not take place. *Journal of strategic studies*, *35*(1), 5-32.

Schwarz, E. (2024). Gaza war: Israel using AI to identify human targets raising fears that innocents are being caught in the net. *The Conversation. https://theconversation. com/gaza-war-israel-using-ai-to-identify-human-targetsraising-fears-that-innocents-are-being-caught-in-the-net-227422,* Erişim Tarihi: 29.05.2024.

Statista (2023). "Revenue of the cybersecurity market in Israel in Israel from 2017 to 2028", *https://www.statista.com/forecasts/1389392/revenue-of-the-cybersecurity-market-in-israel, Erişim* Tarihi: 17.12.2024.

Şengül, B. (2019). İsrail'in Güvenlik Algısı Ve Yansımaları: Demir Kubbe Savunma Sistemi. *Dumlupınar Üniversitesi İİBF Dergisi*(3-4), 19-34.

Şenol, M. (2016). Siber Güçle Caydırıcılık Ama Nasıl?, *Uluslararası Bilgi Güvenliği Mühendisliği Dergisi,* 2(2), 10-17.

Şentürk, H., Çil, C. Z., & Sağıroğlu, Ş. (2016). Siber Güvenlik Yatırım Kararları Üzerine Literatür İncelemesi. *Politeknik Dergisi*, 19(1), 39-51.

Tabansky, L. (2016, May). Towards a theory of cyber power: The Israeli experience with innovation and strategy. In *2016 8th International Conference on Cyber Conflict (CyCon)* (pp. 51-63). IEEE.

Tabansky, L., & Ben Israel, I. (2015). *Cybersecurity in Israel.* Cham: Springer International Publishing.

Unna, Y. (2019). National Cyber Security in Israel. *Cyber, Intelligence, and Security*, *3*(1), 167-173.

Zhukova, I. V., & Trushkina, N. (2023). Critical Infrastructure in the Conditions of Crisis Events and War Threats: The Experience of Israel. Modern Aspects of the Modernization of

Science: Status, Problems, and Development Trends, *Materials of the 34th International Scientific and Practical Conference.*