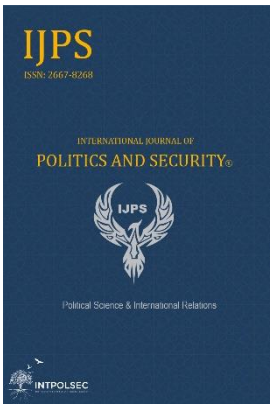
International Journal of Politics and Security (IJPS)

ISSN: 2667-8268
https://dergipark.org.tr/tr/pub/ijps



Siber Güvenlik ve Askerî Alanda Blok Zinciri Teknolojisinin Potansiyel Etkileri: Türk Silahlı Kuvvetleri Örneği

Author(s) / Yazar(lar) : Elif EFE - Kerim Eser AFŞAR

Source / Kaynak: International Journal of Politics and Security (IJPS) / Vol. 5 / No. 2 / October 2023, pp. 101-127.

DOI: 10.53451/ijps.1232114

Date of Arrival **:** 10.01.2023
Date of Acceptance **:** 18.03.2023

To cite this article:

Efe, Elif ve Kerim Eser Afşar. "Siber Güvenlik ve Askerî Alanda Blok Zinciri Teknolojisinin Potansiyel Etkileri: Türk Silahlı Kuvvetleri Örneği". *International Journal of Politics and Security (IJPS)*, Vol. 5, No. 2, 2023, pp. 101-127. DOI:10.53451/ijps.1232114

IJPS, 2023: 5(2):101-126
International Journal of Politics and Security, 2023: 5(2):101-126

Siber Güvenlik ve Askerî Alanda Blok Zinciri Teknolojisinin Potansiyel Etkileri: Türk Silahlı Kuvvetleri Örneği

Elif EFE[*]
Kerim Eser AFŞAR[**]

Özet

Teknolojide İkinci Dünya Savaşı sonrası yaşanan ivme ile ortaya çıkan siber savaş ve siber güvenlik kavramları ülkelerin askerî alanda yaptığı harcamaların en kritik kalemlerinden birinin "veri güvenliği'' olmasına neden olmuştur. Verilerin güvenliğini arttırmak amacıyla geliştirilen teknolojilerden biri blok zinciri teknolojisidir. Bu çalışmada, Türk Silahlı Kuvvetleri'nin (TSK) kullandığı "intranet" kapalı ağ sistemi yerine blok zinciri temelli bir ağ yapısının kullanılmasının siber güvenlik ve savunma ekonomisi bağlamında bir incelemesi yapılmaktadır. Çalışmanın amacı, askerî alanda blok zinciri temelli ağ yapısının TSK özelinde güçlü ve zayıf yanlarını tespit etmek, fırsat ve tehditleri belirlemektir. Blok zinciri teknolojisinin verilere yönelik sağladığı değiştirilemezlik, tahrip ve tahrif edilemezlik, silinemezlik özellikleri neticesinde potansiyel ekonomik maliyetleri azaltabileceği sonucu elde edilmiştir. Bu nedenle makalede, literatürle uyumlu olarak, askerî alanda blok zinciri teknolojisine geçilmesine yönelik ar-ge çalışmalarına hız verilmesi gerekliliği savunulmaktadır.

Anahtar Kelimeler: *Askerî Blok Zinciri, Hyperledger Fabric, Savunma Ekonomisi, Siber Güvenlik, Siber Savunma*

Potential Effect of Blockchain Technology in Cyber Security and Military Applications: The Case of Turkish Armed Forces

Abstract

The emergence of cyber war and cyber security after the Second World War has made data security a critical aspect of military expenditure for countries. One of the technologies developed to increase the security of data is blockchain technology. This study discusses the use of a blockchain-based network system instead of the "intranet" utilized by the Turkis Armed Forces (TAF) as part of cyber security and defense economics. The study aims to evaluate the use of blockchain technology in military applications, specifically for the TAF through a SWOT analysis. Blockchain technology can reduce potential economic costs using unrevisability, indestructibility, and indelibility. Therefore, in the article, coherent with the literature, the necessity of accelerating R&D efforts for the transition to blockchain technology in military applications is advocated.

Key Words: *Cyber Security, Cyber Defense, Defense Economics, Hyperledger Fabric, Military Blockchain*

1. Giriş

Dünya ortalamasına göre 2020 yılında savunma harcamaları, kamu harcamalarının %5,5'ini oluşturmaktadır. Türkiye'deki kamu harcamalarının 2000 yılında %9,2'si savunma harcamalarına ayrılmışken, bu kalem 2016 yılına kadar dünya

[*] Öğr. Gör., Millî Savunma Üniversitesi, Kara Astsubay Meslek Yüksekokulu, Balıkesir/Türkiye, eefe@msu.edu.tr, ORCID: 0000-0002-0281-6949
[**] Dr. Öğr. Üyesi, Dokuz Eylül Üniversitesi, İzmir/Türkiye, eser.afsar@deu.edu.tr, ORCID: 0000-0002-9853-0186
Date of Arrival: 10.01.2022 – **Date of Acceptance:** 18.03.2023

ortalamasına paralel olarak azalış göstermiş, 2017 yılında dünyadaki eğilimden farklılaşarak artmaya başlamıştır. 2020 yılında Türkiye'nin kamu harcamalarının %7,5'i savunma harcamalarına ayrılmıştır.

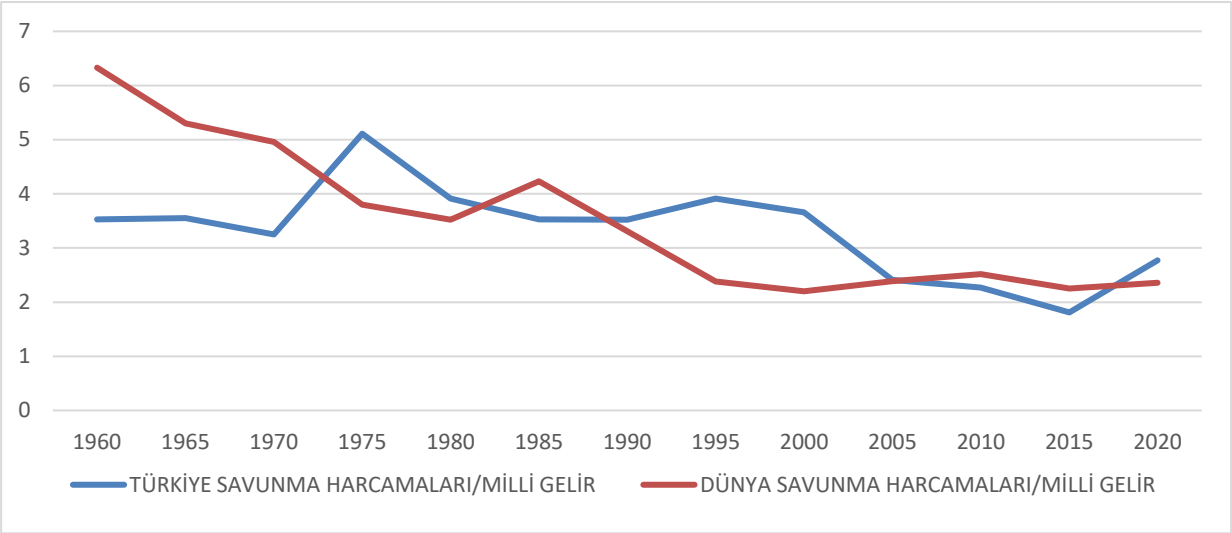
Şekil 1'deki Dünya Bankası verilerine göre küresel çapta 1981 yılında 404 milyar dolar olan askerî harcamalar, 2020 yılında 1,928 trilyon dolara ulaşarak yaklaşık 5 kat artarken, savunma harcamalarının dünya gelirine oranı %4 düşüş göstermiştir. Savunma harcamalarının dünya geliri içerisindeki payı, İkinci Dünya Savaşı sonrası düşmesine rağmen, Soğuk Savaş dönemindeki silahlanma yarışı nedeniyle yeniden yükselmeye başlamıştır. SSCB'nin (Sovyet Sosyalist Cumhuriyetler Birliği) dağılmasıyla birlikte Soğuk Savaşın bitmesi, dünya genelinde savunma harcamalarının payını giderek azaltmıştır.

Türkiye'de de benzer bir durum yaşanarak 1961 yılında 468 milyon dolar olan askerî harcamalar 2020 yılında 17,2 milyar dolara ulaşarak 37 misli artarken, millî gelire oranı %3,8 den, %2,8'e düşmüştür. 1962'de %3,7 olan askerî harcamaların millî gelir içindeki payı, Kıbrıs Barış Harekâtı nedeniyle 1975 yılında %5,1'e ulaşmıştır. Soğuk Savaş döneminin bitmesi, müttefiklerle ilişkilerin yumuşaması ve ekonomik engellerin kaldırılması ile 1986 yılında savunma harcamalarının millî gelire oranı 1961 yılındaki seviyeye geri dönmüştür.[1]

Global Firepower 2022 raporuna göre Türkiye, dünyanın en güçlü orduları sıralamasında 13. sıradadır.[2] NATO üyesi ülkeler arasında ise 5. sıradaki en güçlü ordu Türk Silahlı Kuvvetleri (TSK)'ndedir.[3] Türkiye'de 2015 yılında millî gelir içerisindeki en düşük seviyesine (%1,8) ulaşan savunma harcamaları, 2016 yılından itibaren maruz kalınan iç ve dış tehditler sonucunda dünya ivmesinin aksine artmaya başlamıştır. Tehditlerin boyutu, Türkiye'nin söz konusu gücünü koruması için askerî harcamalarını devam ettirmesini ve teknolojik gelişmeleri takip etmesini bir zorunluluk haline getirmiştir. 1980 yılında dünya çapındaki askerî harcamalarda %0,72 paya sahip olan Türkiye, 2020 yılında %0,91'lik bir paya sahip olmuştur. 2020 yılında 17,72 milyar dolarlık savunma harcaması ile dünya sıralamasında ilk yirmi içinde yer almaktadır.[4]

[1]Kullanılan tüm veriler Dünya Bankasından alınmıştır. Bu konuda bkz. The World Bank, World Development Indicator, Military Expenditure.
[2]https://www.globalfirepower.com/countries-listing.php, erişim 23.07.2022.
[3]https://www.globalfirepower.com/countries-listing-nato-members.php, erişim 23.07.2022.
[4]Deniz İstikbal, "Türkiye'nin Savunma Harcamaları", *Kriter Dergi* 6, no.66, (2022): 54-55.

Şekil 1: Dünya ve Türkiye Savunma Harcamalarının Millî Gelir İçindeki Yüzdelik Payı (1960-2020)[5]



İkinci Dünya Savaşı'ndan sonra teknolojinin hızlanarak bugün geldiği düzeyle geleneksel savaşlar ve savunma harcamaları dışında siber alana yönelik savaşlar ve siber savaşlara yönelik savunma harcamaları kavramları ortaya çıkmıştır. Bu değişim sanayi toplumu kavramının yerini bilgi toplumuna bırakmasıyla bağlantılıdır.[6] Dijital ağların yoğunlaşması, hemen her alandaki değişimi dijitalleşmeyle ilişkili hale getirmiştir. Teknolojik gelişmelerin yol açtığı dönüşüm ile askerî alan küresel düzeyde siber savaşlara evrilmiş ve bu yeni durum nedeniyle savunma harcamaları içinde yeni harcama kalemleri ortaya çıkmıştır.

Siber güvenlik için en kritik faktör verilerin güvenliği ve doğruluğudur. Veri güvenliğinin sağlanması amacıyla verilerin kaydediliş biçimi ve saklanması için sürekli yeni teknolojiler geliştirilmektedir. Nakamoto'nun (2008) öncü çalışması ile şifreleme temelli ve merkeziyetsiz bir ağ yapısı ortaya çıkmıştır.[7] Blok zinciri teknolojisi olarak adlandırılan bu yapı, dağıtık defter teknolojisini (Distributed Ledger Technology[DLT]) de barındırdığı için güvene dayalı olmayan, kriptolojik kanıta dayalı bir veri aktarım ve kayıt sistemi olanağı sunmuştur. 2008 yılından günümüze kadar birçok alanda kullanılan blok zinciri teknolojisinin askerî alanda da kullanılması için öncü çalışmalar yapılmaktadır.

[5]The World Bank, World Development Indicator, Military Expenditure.
[6]Nurcan Törenli, *Enformasyon toplumu ve küreselleşme sürecinde Türkiye*, Bilim ve Sanat Yayınları, Ankara, 2004, s.10-11.
[7]Satoshi Nakamoto, ''A peer-to-peer electronic cash system'', 4: 2, 2008.

Gelişen teknolojiyle siber güvenlik ihtiyacının milli güvenlik kavramı ile eşleştiğini ifade eden Türk Silahlı Kuvvetlerinin ’de birincil derecede önem verdiği öncelikli amacı, veri güvenliğinin en yüksek seviyede sağlanmasıdır.[8] 15 Temmuz darbe girişimine hazırlık sürecinde yapılan merkezi sistemler üzerindeki veri değişiklikleri, verilerin çalınması veya Kozmik Oda[9] Soruşturmasında incelenen belgelerle ilgili veri güvenliği problemleri ortaya çıkmıştır. Önerilen özel izinli blok zinciri teknolojisinde sadece ilgili kısımlara erişim izni tanınabileceği, tüm verilere erişiminin engellenebileceği gibi içsel saldırıların (veri çalınması, tahrif edilmesi, silinmesi gibi) yanı sıra blok zinciri teknolojisi dışsal bir saldırıya karşı da (bilişim sistemlerine başka devletlerin ulaşması gibi) sistemde kayıtlı verilerin güvenliğini ve tamlığını merkezi sunucular üzerinden oluşturulan DNS yapısına (intranet) göre en yüksek seviyede muhafaza edebilecek dağıtık yapıda DNS sistemine sahiptir. Söz konusu olası saldırılara karşı askerî alanda bilgi akışı ve güvenliğinin verimliliği kritik bir role sahip olduğundan yüksek güvenlik katmanlı, esnek ve kullanışlı bir sistem olan Hyperledger Fabric “gerçek anlamda” yüksek güvenlikli ve güvenilir bir bilgi akışı sağlayabilmektedir. MSB(TSK) içi tüm kapalı ağ sisteminin blok zinciri teknolojisine geçilmesi ile sadece “veri saklama” amacıyla kullanımı dahi siber güvenlik alanında birçok siber saldırının önüne geçebilmektedir. Geleneksel ağ yapısına yapılan DoS, DDoS vb. saldırılar önlenebilmekte, verilerin değişmezliği ve deftere kaydedilen bilgilerin silinemezliği, özellikle içeriden yapılan saldırıların tamamen izlenebilir olmasını sağlamaktadır. Askerî verilerin güvenliğinin alternatif maliyeti söz konusu olduğunda, veri güvenliğinin hayati öneme sahip olduğu söylenebilir. Literatürde, özellikle ABD-İran arasındaki siber savaşta, ‘‘gizli’’ ar-ge sonuçlarının çalınması ve çalınan teknolojinin geliştirilerek pazardaki yerinin işgal edilmesi konunun önemini gösteren iktisadi örneklerdendir.

Çalışmanın geri kalanı dört bölüm olarak kurgulanmıştır. Birinci bölümde literatür taraması ve araştırmanın önemine değinilmiştir. İkinci bölümde askerî alanda siber güvenliğin önemi anlatılmıştır. Üçüncü bölümde, blok zinciri teknolojisi tanıtılmış ve askerî alanda kullanımı tartışılmıştır. Dördüncü bölümde, blok zinciri teknolojisinin askerî alanda

[8] https://www.msb.gov.tr/SlaytHaber/milli-savunma-bakani-sn-fikri-isik-ulastirma-denizcilik-ve-haberlesme-bakani-sn-ahmet-arslan-ile-siber-guvenlik-isbirligi-protokolunu-imzaladi, erişim 24.10.22

[9] Kozmik Oda: Genelkurmay Başkanlığı'na bağlı Seferberlik Tetkik Kurulu'ndaki (STK) mühürlü kozmik odaların kapısı yüz ve parmak izi tanıyan, 17 haneli şifrelerle açılmaktadır. Çok sınırlı sayıda personelin girmek için yetkili olduğu odalarda, olası bir savaşta devlet büyüklerinden iş adamlarına kadar ülke için önemli olan isimlerin nasıl ve nerede korunacağına dair detaylı planlar yer almaktadır. https://www.ntv.com.tr/turkiye/kozmik-oda-nedir,lqaMw53CdEq8SlGV-ASz_A, erişim 28.10.22

uygulanabilirliği ile güçlü/zayıf yönleri incelenerek Türk Silahlı Kuvvetleri açısından siber güvenlik ve iktisadi anlamda bu teknolojiye geçilmesi gerekliliğine yönelik öneriler ortaya konulmuştur.

2. Literatür Taraması

Uluslararası literatürde McAbee, Tummala & McEachen (2019) askerî istihbarat sistemlerine blok zinciri teknolojisinin dahil edilmesinin potansiyel kullanım alanlarını araştırmıştır.[10] Lilly & Lilly (2021), ABD, Çin ve Rus ordularının savaşta blok zinciri teknolojilerine yönelik uygulamaları ele almış ve dünyadaki askerî blok zinciri projelerine odaklanmıştır.[11] Taylor ve diğerleri (2020) çalışmasında siber güvenlik için blok zinciri uygulamalarını sistematik olarak gözden geçirmiştir.[12] Lee & Kim (2021) siber savunmanın blok zincirinde ortaya koyduğu fırsatları, uygulamaları ve zorlukları ele almıştır.[13] Polcumpally (2022), blok zincirinin askerî uygulamalarda kullanımının önemine vurgu yaparak Hindistan için henüz bir pilot çalışmanın söz konusu olmadığını, Hindistan ordusunun diğer orduların bu teknolojiyi benimsemesini beklemeden bir an önce yapısal değişikliklere başlayarak, blok zinciri teknolojisinin etkisini anlamak için ordu içinde sanal alanlar oluşturması gerektiğini iddia etmiştir.[14] Zhu ve diğerleri (2020) blok zinciri teknolojisini, askerî alanda gelecek vaat eden uygulamalar bağlamında ele almıştır.[15]

Ulusal literatürde, askerî alana yönelik blok zinciri ile ilgili az sayıda çalışma vardır. Konacaklı (2019) çalışmasında ‘‘Hyperledger Fabric’’ ile modeli oluşturulan hava operasyonlarının ‘‘iz verisinin’’ emniyetini sağlamaya yönelik bir uygulama geliştirerek ulusal iletişim sistemi ve yazılımlarla donatılmış ağ yapılarının Türkiye’de veri güvenliğini korumada çok önemli görevler üstlenebileceğini göstermiştir.[16] Angin (2020), askerî otonom sistemlerde veri güvenliği sağlanmasına yönelik blok zinciri mimarisi önererek güvenilir iletişim sağladığı

[10]McAbee, Ashley, Murali Tummala, and John McEachen. "Military intelligence applications for blockchain technology.", Proceedings of the 52nd Hawaii International Conference on System Sciences, 2019, s.6031-6040.
[11]Bilyana Lilly and Sale Lilly. ‘‘Weaponising Blockchain: Military Applications of Blockchain Technology in the US, China and Russia.’’ The RUSI Journal 166:3, 2021, s.46-56.
[12]Paul J Taylor, et al. ‘‘A systematic literature review of blockchain cyber security.’’ Digital Communications and Networks 6:2, 2020, s.147-156.
[13] Suhyeon Lee and Kim Seungjoo, ‘‘Blockchain as a Cyber Defense: Opportunities, Applications, and Châllenges.’’, IEEE Access 10, 2021, s.2602-2618.
[14]Arun Teja Polcumpally, ‘‘Blockchain technology and its importance in the military applications.’’, CSS, 2022.
[15]Ying Zhu., et al. ‘‘A study of blockchain technology development and military application prospects.’’, *Journal of Physics: Conference Series*. Vol. 1507. No. 5. IOP Publishing, 2020.
[16]Enis Konacaklı, *Ulusal güvenlik için blokzinciri tabanlı siber güvenlik modeli*, Yüksek Lisans Tezi, Eskişehir Teknik Üniversitesi, 2019.

ve içerik manipülasyonuna yönelik siber saldırılara karşı güvenilirliği arttırdığı sonucuna ulaşmıştır.[17] Karaarslan ve Konacaklı (2021), ‘‘Hyperledger Fabric’’ mimarili blok zinciri ile hava kuvvetlerinin sahip olduğu lojistik yönetiminin kayıtlarının ve takibinin güvenliğinin arttırılmasına yönelik bir model oluşturmuştur.[18]

Bu çalışmanın amacı, askerî alanda ‘‘Blok Zinciri Temelli Ağ Yapısının’’ TSK özelinde güçlü ve zayıf yanlarını tespit etmek, fırsat ve tehditleri belirlemektir. Literatürde blok zinciri teknolojisinin askerî alandaki kullanımının zayıf yönleri/dezavantajları ve iktisadi bağlamı çoğunlukla ihmal edilmiştir.[19] Bu makalede ‘‘SWOT analizi’’ yöntemiyle askerî alanda blok zinciri teknolojisi kullanımının ihmal edilen unsurlarına odaklanılmıştır.

3. Siber Güvenlik

Günümüzde küresel düzeyde neredeyse tüm ülkeler dijital sistemlere entegre olmuştur. Dijitalleşen verilerin güvenli hâle getirilmesi ise “siber güvenlik” kavramının önemini ortaya koymaktadır. Özellikle teknolojinin çıkış noktası kabul edilen silahlı kuvvetler teknolojik gelişmelere öncülük etmektedir. Siber savaşların ortaya çıkması ile söz konusu olduğu askerî ve istihbarat faaliyetlerine yönelik güvenlik açıkları bunun yanında ekonomik maliyetleri nedeniyle hem savunma harcamaları hem de ar-ge çalışmaları dünya genelinde bu yöne evrim geçirmek zorunda kalmıştır. Mckinsey şirketi 10 Mart 2022 tarihinde yayımladığı ‘‘Cybersecurity trends: Looking over the horizon’’ isimli çalışmada, 2025 yılına kadar veri güvenliği alanında yapılacak harcamaların 101,5 milyar dolar olacağını belirtmektedir.[20]

[17]Pelin Angin, "Blockchain-Based Data Security in Military Autonomous Systems." Avrupa Bilim ve Teknoloji Dergisi, 2020, 362-368.
[18]Enis Konacaklı ve Enis Karaarslan, *Blokzincirinin Askerî Lojistik Takip Sistemlerinde Kullanılması*, Siber Güvenlik ve Savunma: Blokzinciri ve Kriptografi, Ankara, Nobel Yayınevi, 2021.
[19]Kamu yönetiminde blok zinciri teknolojisinin potansiyel etkiler için Şat (2019), Karahan ve Tüfekçi (2019a), Karahan ve Tüfekçi (2019b) çalışmaları örnek gösterilebilir. Ancak bahsi geçen çalışmalar SWOT analizi kapsamında değildir. Bu çalışmada olduğu gibi henüz hayata geçmemiş bir blok zinciri uygulamasının SWOT analizi için bkz. Küçükkıralı ve Afşar (2022).
[20] https://www.mckinsey.com/business-functions/risk-and-resilience/our-insights/cybersecurity/cybersecurity-trends-looking-over-the-horizon, erişim 24.07.2022.

3.1. Enigma ve Siber Savaşların Kökeni

Savaşların siber alana dönüşmesindeki başlangıç noktası İkinci Dünya Savaşı'nda şifreleme makinelerinin atası kabul edilen, Almanya'nın, ''Enigma'' adı verilen sistem ile iletişim kurmayı başarması olmuştur. Bu iletişim düşmanın mesajları çözmesini engellemek için bir şifreleme yöntemi ile gerçekleşmiştir. Sürekli algoritmaların güncellenmesi işlemi uygulanarak, şifrelemenin çözülmesinin de önüne geçilmeye çalışılmıştır. İlk siber saldırı olarak kabul edilebilecek hamle, Enigma'ya yönelik olarak İngiltere'nin, Turing önderliğinde bir grup ile Enigma'nın şifrelerini çözmeye çalışmasıdır. İngiltere'deki ekip, sürekli yenilenen algoritmalar için bir makine tasarlama gereksinimi ile ''Clossus'' isimli makineyi geliştirmişlerdir. Siber saldırıların atası olarak kabul edilebilecek bu makine ile savaşın erken bitmesi sağlanmıştır. Clossus iletilen bir mesajdaki 25000 karakteri tarayıp anlamlı kısımlarını tespit edebilen bir makinedir.[21] Makinelerin gelişimi bilgisayar teknolojisine bir temel hazırlamıştır. İnternetin gelişimi ise ABD Savunma Bakanlığının kurduğu ''Arpanet'' ile başlamıştır; bu ağ dünyanın ilk internet ağı olarak kabul edilmektedir. Üniversiteler arası kurulan bilgisayar bağlantısı ile ilk iletilmek istenilen ''login'' kelimesinin sadece ilk iki harfi iletilebilmiş, diğer harfleri ise saatler sonrasında iletilmiştir.[22] Bu atılım sonrasında internetin günümüzdeki gelişimine yönelik ağ bağlantısı genişletmeleri süratli biçimde gerçekleşmiştir. Günümüzdeki birçok askerî faaliyetin ağ üzerinden iletilmesi siber savaşları, muharebe çeşitlerinin önemli bir parçası hâline getirmiştir.

3.2. Siber Saldırı ve Savunmaların Küresel Örnekleri

Küresel çapta gerçekleşmiş olan çok sayıda siber saldırı bulunmaktadır. ABD tarafından gerçekleştirilen siber saldırılara yönelik ilk hamle Birinci Körfez Savaşı'nda, Irak'ın tüm askerî donanmaları arasındaki koordinasyonu kesmesiyle gerçekleşmiştir. Bunun yanında ABD tarafından şifreli telsizlerin frekanslarına sızılması, askerî birimlerin aralarında yanlış koordine olmalarına neden olmuştur. İkinci Körfez Savaşı'nda ise ABD sistemlerini daha da geliştirerek sadece telsizlere değil tüm iletişim araçlarına siber saldırıda bulunarak, personelin teslim olmasına yönelik propagandalarda bulunmuştur.[23] ABD, kendi yaptığı saldırılar ve 2001 de yaşadığı saldırılar nedeniyle, 2009 yılında resmî olarak Siber Komutanlığını

[21]Jack B. Copeland (ed.), *The essential* Turing, Clarendon Press, 2004, s.232.
[22]Stephen Lukasik, ''Why the Arpanet was built?'', IEEE Annals of the History of Computing, 33:3, 2010, s.12.
[23] Ali Burak Darıcılı, *Amerika Birleşik Devletleri ve Rusya Federasyonu'nun Siber Güvenlik Stratejilerinin Karşılaştırmalı Analizi*, Doktora Tezi, Uludağ Üniversitesi, Bursa, 2017, s. 63.

‘‘USCYBERCOM’’ adıyla kurmuştur. İran’a karşı 2015 yılında yapılan ‘‘Stuxnet’’ isimli bir virüs ile nükleer santrallerine yönelik bir saldırı yapılmıştır. Bu saldırı santrallerdeki makinelerin parçalanmasına neden olmuş ve İran’ı milyonlarca dolar zarara uğratmıştır. İnternet bağlantısı dahi bulunmayan santrale, reaktör mühendisinin evrensel seri veriyolu (USB) ile sisteme bu zararlı yazılımı entegre ettiği düşünülmektedir.[24] Eski ulusal güvenlik ajansı çalışanı Snowden’ın açıklamasına göre bu virüs ABD ve İsrail tarafından programlanarak, İran’ın nükleer enerji üretimine zarar vermek için ortaya çıkarılmıştır.[25]

2016 yılında ABD’ ye ait insansız hava aracı (İHA) İran tarafından düşürülmüş, teknolojisinin taklit edilmesinin yanı sıra silah aparatları da eklenerek gelişmiş bir modeli üretilmiştir. 2019 yılında ise ABD’ye ait bir İHA, İran tarafından ‘‘siber saldırılar’’ sonucu düşürülmüştür. Dönemin en gelişmiş teknolojisine sahip olan bu İHA’ların değeri 120 Milyon dolardır.[26] Düşürülen İHA’nın maliyeti dışında teknoloji taklidi ile de ar-ge harcamaları yükünden kurtulan İran, ABD’nin, İHA’sını ihraç ederek elde edeceği gelire de dünya üzerinde sahip olabilme fırsatını ele geçirmiştir. Bu bağlamda siber saldırı sonucu maruz kalınan ekonomik zararların çeşitleri de farklılaşmaktadır.

Rusya ise 2000 yılında yayınladığı ‘‘öğreti’’ ile siber güç olma maksadıyla ilk belgesini oluşturmuştur. 2009 yılında yayımladığı bir diğer belge ile teknolojinin gelişmesiyle ortaya çıkacak risklerin önemine vurgu yapmıştır. Resmî bir komutanlığa sahip olmamasına karşın Rusya, orduda ve istihbarat servislerinde pek çok siber yapılanma oluşturmuştur. 2014 yılında ise Rusya, bütçeden 500 milyon dolar ayrıldığını belirterek yazılım uzmanları ve yabancı dil bilen personel istihdam edileceğini, siber tehditlere yönelik olarak bağımsız olmanın önemini resmî olarak ifade etmiştir.[27] Sonraki yıllarda ise orduda faaliyet göstermeleri için siber uzmanlara askerî zorunluluklara karşılık imtiyaz sahibi olacakları tekliflerde bulunulmuştur. Siber alanda çalışmalarını test etmek isteyen Rusya 2019 yılında tüm küresel internet ağı ile bağlantısını keserek, internet altyapısının dünya ağına bağlı olmadan çalışıp çalışmadığını

[24]Marie Baezner and Patrice Robin, ‘‘Stuxnet’’, Center for Security Studies (CSS), ETH Zurich, 4, 2017, s.4-5.
[25] Edward Snowden Interview, ‘‘The NSA and Its Willing Helpers’’, https://www.spiegel.de/international/world/interview-with-whistleblower-edward-snowden-on-global-spying-a-910006.html erişim 22.05.2022.
[26] Hakan Kılıç, ‘‘ABD’nin dev casus uçağı İran tarafından düşürüldü: Peki şimdi ne olacak?’’, https://www.yenisafak.com/gundem/iranin-abd-ucagini-dusurmesi-nasil-sonuclar-doguracak-3495626, erişim 23.05.2022.
[27] Ali Burak Darıcılı ve Barış Özdal, ‘‘Rusya Federasyonu’nun Siber Güvenlik Kapasitesini Oluşturan Enstrümanların Analizi’’, *Bilig*, 83, 2017, s.131.

kontrol etmiştir.[28] Rusya bu testle olası bir saldırı söz konusu olduğunda ağını bir nevi intranete dönüştürerek siber saldırıların zararını en aza indirmeyi amaçlamaktadır.

3.3. Türkiye'de Siber Güvenlik ve Saldırılar

Türkiye'deki duruma baktığımızda ise resmî olarak bir ''siber komutanlık'' olmamasının yanında 2012 yılında TSK Siber Savunma Merkezi Başkanlığı kurulmuş ve bu yapı 2013 yılında TSK Siber Komutanlığına dönüştürülmüştür. Bu komutanlık muharebeden öte savunma amaçlı TSK'ya ait internet sitelerini korumak ve olası saldırıları önlemek üzerine işlev görmektedir. Nükleer tehditlerden sonra TSK siber saldırıların küresel olarak var olan en büyük ikinci tehdit oluşturduğunu ifade etmiştir.[29] Cumhurbaşkanlığına bağlı olarak 2017 yılı içerisinde "Siber Savunma Harekât Merkezi" kurulumu tamamlanarak TSK'nın hizmetine sunulmuştur.[30] Türkiye'ye yönelik sivil siber saldırılardan biri Garanti Bankası'na 2019 yılında gerçekleşmiştir. Kurum yöneticileri internet servisleri tabanlı bir yoğunluk olduğu açıklamasında bulunmuş, müşterilere ait bilgilerin çalınmadığını iddia etmiştir. Yine 2019 yılında Türkiye'nin alışveriş sitelerinden n11.com bazı müşterilerin e-posta adreslerinin çalındığını açıklamıştır.

Basında yer bulan siber saldırılar ve küresel çapta yaşanmış saldırılar göz önüne alındığında olası saldırılara karşı, Türkiye'nin kritik altyapılar (elektrik santralleri, telekomünikasyon, ekonomi, sağlık, askerî alanlar) bağlamında siber güvenliğine yönelik önlemleri arttırması bir zorunluluk hâlindedir. Kritik alanlarda internete bağlılık durumu söz konusu olduğu için olası bir siber saldırıya karşı alınabilecek önlemlerin maliyeti, herhangi bir siber saldırı sonucu oluşacak ekonomik ve güvenlik açısından ortaya çıkacak maliyetin yanında oldukça düşük düzeydedir. Türkiye açısından e-devlet uygulaması değerlendirildiğinde, 2021 yılı Ekim ayı itibariyle 624 kurumun sağladığı 6001 hizmet sayısı siber saldırıların olası etki alanlarını niceliksel olarak ifade etmektedir.[31]

[28]Ozan Baki, ''Rusya, Küresel İnternet Ağıyla Bağlantısını Başarıyla Kesti'', https://www.webtekno.com/rusya-kuresel-internet-agiyla-baglantisini-kesti-h82374.html, erişim 25.05.2022.
[29]Sinan Uslu, ''Türk ordusunun yeni "kuvveti" siber savunma'', https://www.aa.com.tr/tr/turkiye/turk-ordusunun-yeni-kuvveti-siber-savunma/584061, erişim 01.06.2022.
[30]T.C. Savunma Sanayii Başkanlığı, https://www.ssb.gov.tr/WebSite/contentlist.aspx?PageID=1083&LangID=1, erişim 03.06.2022.
[31] T.C. Strateji ve Bütçe Başkanlığı, ''2022 Yıllık Programı'', s.371, https://www.sbb.gov.tr/wp-content/uploads/2021/10/2022-Yili-Cumhurbaskanligi-Yillik-Programi-26102021.pdf , erişim 07.06.2022.

19 Aralık 2019'da dönemin Başbakan Yardımcısına yönelik suikast iddiası ile açılan soruşturma kapsamında FETÖ üyesinin, devletin en gizli belgelerini Kozmik Oda'dan 1,5 terabaytlık hardiske kopyalayarak yurt dışına kaçırması, bu kişinin iç güvenlik ve siber güvenlik uzmanı olması, TSK'ya içeriden erişim ile merkezi sunucularda saklanan bilgilerin ele geçirilmesine yönelik bir saldırıyı gerçekleştirdiğini göstermektedir.[32]

2016 yılında TSK'ya yönelik yapılmış olan 15 Temmuz Darbe Girişimi'nin arka planı veya Ukrayna-Rusya örneğindeki gibi fiziksel bir askerî saldırı sonucunda, TSK'nın bilişim sistemlerine ulaşım elde edilmiş olmasının yaratacağı maliyetler yüksek düzeye ulaşabilir. Kamuoyunda da yer bulan 15 Temmuz Darbe girişiminin arka planında İzmir Cumhuriyet Başsavcılığı tarafından hazırlanan, İzmir'deki askerî casusluk soruşturmasında FETÖ'nün çeşitli usulsüzlükler yaparak sahte delil üretildiği iddialarıyla ilgili İzmir Askerî Casusluk İddianamesinde, TSK içindeki örgüte ait personelin; TSK'nın güvenliğine ait gizlilik içeren belgeleri söz konusu örgütün havuzuna ulaştırdıkları, kurum dışına çıkarabildikleri çeşitli gizlilik derecelerine sahip belgeleri, bu havuza aktardıkları hatta belgeleri tahrif edip değiştirdikleri ve bu şekilde ilgili kurumlara gönderdiklerinin anlaşıldığına yer verilmektedir.[33] Fiziksel saldırılara gerek olmadan içeride ortaya çıkabilecek bir yapının yine var olan bilgileri değiştirmesi, elde etmesi, silmesi gibi durumlar sistemin güvenliğini tehdit edebilmektedir.

Başka devletlerin TSK birimlerine ulaşmaları sonucunda elde edebilecekleri istihbarat faaliyetleri kapsamında gizlilik içeren bilgiler, bu bilgilerin değiştirilmesi veya silinmesinin maliyeti Türkiye için oldukça yüksek olacaktır. 2017 yılında dünya çapında yapılan siber saldırıların sadece ekonomik zararı 600 milyar dolar olmuştur. Dünya Ekonomik Forumu, Küresel Risk Raporu'nda siber saldırıların, 2021 yılı içerisinde küresel ekonomiye maliyetinin 6 trilyon dolar olduğunu tahmin etmektedir.[34] Küresel ölçekte gerçekleşmiş saldırılar göz önüne alındığında, Türkiye'de askerî teknoloji ve enerji alanlarında bağımlılığı azaltmaya yönelik yapılan harcamalar ve yatırımlar (Bayraktar, Nükleer Santraller vb.) sonucunda bu alanlara

[32] https://www.trthaber.com/haber/gundem/kozmik-oda-casusu-bilgileri-harddiskle-feto-elebasina-goturmus-530949.html, erişim 26.10.22
[33] https://www.aa.com.tr/tr/15-temmuz-darbe-girisimi/izmirdeki-askeri-casusluk-sorusturmasinda-kumpas-davasinda-karar/1904912, erişim 26.10.22
[34] ''Global Risks Report'', https://www.weforum.org/reports/global-risks-report-2022/, erişim 07.06.2022.

yönelik ar-ge verilerini ele geçirmek, kendi çıkarları için kullanmak veya değiştirmeye yönelik saldırı riskleri söz konusu olabilecektir.[35]

Tüm bu siber saldırı riskleri göz önüne alındığında, en kritik kurum olan Millî Savunma Bakanlığı'na bağlı birimlerin kullandığı teknolojiyi ''millîleştirmek'', var olan sistemin daha da güvenli hâle getirilmesine yönelik ar-ge harcamalarına yatırım yapmak, stratejik olarak olası durumlara karşı alınabilecek en önemli tedbirler arasındadır. İlk nükleer santrale sahip olma hazırlıkları içerisinde olan Türkiye'nin reaktör sistemini etkileyerek bir nükleer patlamaya yol açmak, millî muharip uçağının yüksek güvenlik altında tutulan kaynak kodlarını ele geçirmek, hatta bu saldırılardan siyasi edinimler elde ederek çeşitli millî zararlar ortaya çıkarmayı hedefleyecek olası siber saldırılar söz konusu olabilecektir.[36]

4. Blok Zinciri Teknolojisi ve Askerî Alanda Siber Güvenlik Uygulamaları

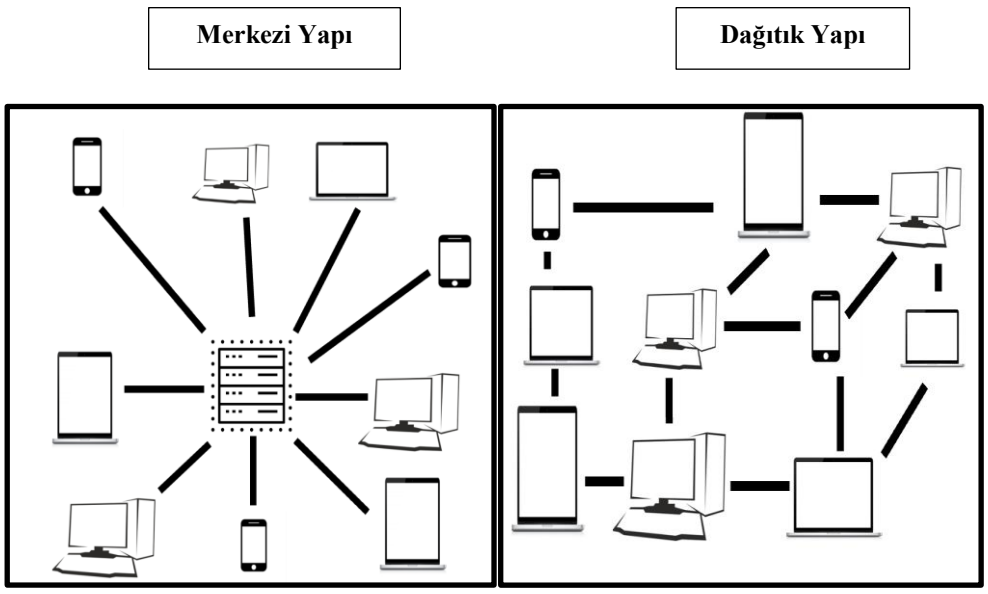
Basitçe blok zinciri teknolojisi, silinemez, yok edilemez, tahrif edilemez veri tabanı ve kayıt sistemi olarak tanımlanabilir. Dünya genelinde devletler blok zinciri teknolojisini uygulamak için yarışmaktadır. ABD, DARPA'nın (Savunma İleri Araştırma Projeleri Ajansı) ''Sanal Ortamlarda Veri Koruması'' (DPRIVE) ile tedarik zinciri saldırılarıyla mücadele etmek, askerî lojistiği yönetmek ve savaş alanında güvenli iletişim kanalları oluşturmak için blok zinciri teknolojisi sistemleri geliştirmeyi amaçlamaktadır. Avrupa Birliği, blok zinciri teknolojisinin çeşitli sektörleri etkileyebileceğini ve dijital AB için temel oluşturmanın önemli olabileceğini ifade etmektedir. Dijital ''Tek Pazar'' girişimi, İletişim ve Teknoloji Genel Müdürlüğü (DG-CONNECT), Avrupa Blok Zinciri Ortaklığı (EBP), Avrupa Blok Zinciri Hizmetleri Altyapısı (EBSI) gibi girişimler, sivil-askerî blok zinciri teknolojisinin geliştirilmesi için yeni atılımlar olarak görülmektedir.[37] Sadece batılı devletler değil, Çin Halk Cumhuriyeti de blok zinciri teknolojisine önemli yatırımlar yapmaktadır. Halk Kurtuluş Ordusu (PLA), istihbarat operasyonları için fon dağıtımını yönetmek, savunma personelinin verilerini korumak, silah yaşam döngüsü, askerî lojistiği sürdürmek ve operasyonları daha güvenli hâle getirmek için blok zinciri teknolojisini kullanmayı planlamaktadır.[38]

[35]''5th Generation Cyber Attacks Are Here And MostBusinesses Are Behind- A New Model For Assessing and Planning Security'', http://www.infosecurityeurope.com, erişim 07.06.2022.
[36] Enis Konacaklı, Age, s.16.
[37]Arun Teja Polcumpally, Age, s.2.
[38]https://www.crowell.com/files/Potential-Uses-of-Blockchain-Technology-In-DoD.pdf , erişim 23.06.2022.

4.1. Blok Zinciri Yapısı

2008 küresel krizinden sonra takma bir isimle Satoshi Nakamoto tarafından Bitcoin: Eşten Eşe Elektronik Nakit Ödeme Sistemi çalışmasında, geleneksel finans sitemine alternatif olarak; finansal aracıların olmadığı, devlet tarafından kontrol edilmeyen ve kişilerin aralarında para alışverişine imkân sağlayan dijital paranın bir parçası olan blok zinciri bir defter olarak tasarlanmıştır. [39] Çıkışı nedeniyle finansal işlemlerde kullanılabilen bir sistem olarak algılanmasına rağmen blok zinciri teknolojisi, tüm değerli kayıtları saklama aracı olarak kullanılmaktadır. Şifreleme bilimi (kriptoloji) ile verilerin saklandığı blok zinciri yapısı merkezi bir yapı üzerinden eşlere bilgi aktarmak yerine, eşler arası dağıtık yapısı ile bilgi akışı sağlayan tamamen güvenilir bloklardan oluşan bir dijital kayıt sistemidir. Şekil 2'de verilen dağıtık mimariye sahip zincir yapısı, blok zinciri teknolojisinin dağıtık eşler arası bağı sayesinde verilerin tek bir merkezde toplanması yerine ağa dahil olan tüm düğümlerde kayıtların var olmasını sağlayarak günümüzde kullanılan merkezi yapılardan daha güvenli bir sistem oluşturmaktadır.

Şekil 2: Geleneksel Ağ ve Blok Zinciri Teknolojisi[40]



Dağıtık yapı sisteminde ağa dahil olan tüm düğümlerin en az %51'i ele geçirilene dek verilerin tümü güvenli bir şekilde kayıtlı kalmaya devam edebilmektedir. Fiziki bir savaş

[39]Satoshi Nakamoto, Age.
[40]https://blokzincir.bilgem.tubitak.gov.tr/blok-zincir.html diyagramı tarafımızca revize edilmiştir.

sırasında merkezin ele geçirilmesi ile söz konusu olabilecek bir erişim vasıtasıyla verilerin hepsi silinebilirken, blok zinciri sisteminde sistemin içerisinde olan tüm düğümlerin ancak tek tek yok edilmesi sonucunda verilerin silinebilmesi mümkün olmaktadır.

Blok zincire kaydedilen veriler belirli bir büyüklüğe ulaştıktan sonra (Tasarım yapılırken ne kadar büyüklükte bir bloklaşması gerektiği kıstas (uzlaşma protokolü) olarak belirlenmektedir), işlenerek zaman damgası ve şifreleme bilimi yardımıyla kalıcı kayıtlı bloklar oluşturulmaktadır.[41] Tasarımda oluşturulan ilk blok ‘‘başlangıç bloğu’’ (genesis block) olarak isimlendirilmektedir.

Bloklar birbirlerine kendilerinden önceki blokun özet fonksiyonu ile bağlanarak blok zincirlerini oluşturur. Özet fonksiyonları (hash kodu) bir önceki bloğun içindeki verilerin tek yönlü fonksiyonlarıdır. Blokta yapılacak en küçük bir değişikliğin özetin tamamının değişmesine sebep olması blok zincirinin değiştirilemez yapısının temelini oluşturmaktadır. Şekil 3’te görüldüğü üzere, her blok kendinden önceki bloğun özet şifrelemesini taşıyarak kendinden sonraki bloğa kendi özet şifrelemesini vererek bağlandığı için bütün bloklar kendinden önceki tüm bloklara ait verileri içerisinde barındırmaktadır.[42] Zaman damgası ile kapatılmış bir bloktaki veriler değiştirilmeye çalışıldığında (hacklenmeye) komşu bloklarındaki kodlar zaman uyumlu olmaktan çıkacağı için “sanal alarmlar” yetkilendirilmemiş bir giriş olduğunu kolaylıkla tespit edebilecektir.

Şekil 3: Blokların Zincirleşme Teknolojisi[43]

[41] ‘‘Blokzincir’’, https://blokzincir.bilgem.tubitak.gov.tr/blok-zincir.html, erişim 08.06.2022.
[42] ‘‘Blokzincir’’, Age, erişim 08.06.2022.
[43] https://www.ig.com/en/trading-strategies/what-is-blockchain-technology--200710, https://emn178.github.io/online-tools/sha256.html verileri kullanılarak tarafımızca düzenlenmiştir, erişim 09.06.2022.

Finansal işlemlerde kullanılan blok zinciri mimarisi, kayıtları okuma ve düğüm olma hakkını her katılımcıya sağlayarak herhangi bir kullanıcı ağa dahil olmak istediğinde bir kısıtlamaya tabi tutulmamaktadır. Bitcoin yapısındaki teknolojilerde ‘‘İş Kanıtı Konsensus Mekanizması’’ (PoW) nedeniyle enerji harcaması oldukça fazladır. Mahremiyet veya gizlilik ihtiyaçları söz konusu ise daha çok kamusal (açık) blok zincirleri yerine izinli veya hibrit yapılar tercih edilmektedir. İzinli yapılar oluşturularak ağ içerisindeki düğümlerin (Eşlerin, MSB çalışanlarının) belirli bir bilgiyi tam güven içerisinde paylaşması sağlanmaktadır. Eşler ancak belirlenmiş olan otoritenin (MSB) izni ile ağa dahil olmaktadır. Hyperledger Fabric, Hyperledger Burrow, R3 Corda bu teknolojilere örnek teşkil etmektedir. Özel izinli zincirlerde gizlilik artarken maliyetler düşer.[44]

4.2. Türk Silahlı Kuvvetleri Siber Altyapısı için Önerilen Blok Zinciri Mimarisi

TSK ve Millî Savunma Bakanlığı bağlamında değerlendirildiğinde kullanılan altyapı intranet odaklı kapalı ağ internet altyapısıdır. TSKNET olarak var olan bu altyapı, kuvvetler namında çeşitli isimlerle (Kara Kuvvetleri KARANET vb.) anılmaktadır.[45] Gerçekleştirilen siber saldırılardan yola çıkılarak internet ile ilişkisi söz konusu olmayan bir reaktör bilgi sisteminin (İran, Stuxnet Saldırısı) bile kontrolü ele geçirilebilmektedir.[46] Geleneksel ağlara yönelik güvenlik endişesi oluşturan hizmet reddi ‘‘DoS’’ (Denial of service) saldırısı ve kaynağın işleme kapasitesine yönelik sınırlı miktarda zaman gerektiren hizmet istekleriyle doldurulması vasıtasıyla gerçekleşen ‘‘DDoS’’ (Distributed denial of service) saldırısı söz konusu olmaktadır.[47] Bu nedenle var olan merkezi sunucular üzerinden oluşturulan Alan Adı Sistemi (Domain Name System [DNS])yapısı TSKNET’te (intranet) saklanan verilerin olası saldırılara karşı önlem alabilmek adına çalışmamızda dağıtık yapıda blok zinciri tabanlı DNS yapısına geçirilmesi önerilmektedir. Bu yapı sayesinde güvenli DNS dağıtımı oluşturulabilecektir. DNS zehirlenmesi gibi saldırılar veya sunucuların siber saldırılar (DDoS, DoS vb.) sonucunda servisten düşme sorunu yaşamasının önüne geçilebilecektir.[48]

[44]Enis Konacaklı ve Enis Karaarslan, Age, s.223.
[45]Cem Çerkezoğlu, *Kara kuvvetleri komutanlığında uzaktan eğitim uygulamaları,* Yüksek Lisans Tezi, Sakarya Üniversitesi, Sakarya, 2006, s.102.
[46] Enis Konacaklı, Age, s.11.
[47]Brij B Gupta and Omkar P. Badve, ‘‘Taxonomy of DoS and DDoS attacks and desirable defense mechanism in a cloud computing environment’’, Neural Computing and Applications, 28:12, 2017, s.1-2.
[48]Enis Konacaklı, Age, s.30.

Öncelikli olarak Bitcoin ağıyla hayata geçen blok zinciri ağları açık blok zinciri ağları olarak sınıflandırılmaktadır. Bu tip ağların askeri alanda kullanımı işlevsizdir. Yukarıda bahsi geçen kapalı ağların siber güvenlik sorunlarının çözümü için Hyperledger Fabric, R3 Corda gibi konsorsiyum blok zinciri ağları geliştirilmiştir. 2015 yılında Linux vakfı tarafından açık kaynak kodlu ve topluluk odaklı altyapılar sağlayan bir platform olarak tanıtılan Hyperledger Fabric bir şirket veya firma değildir. Kurumların talepleri ile veri gizliliğini korurken uygun ölçekte performans sağlamaya yönelik bir blok zinciri teknolojisi yaklaşımı sunmaktadır.[49] Kuzey Atlantik Antlaşması Örgütü (North Atlantic Treaty Organization [NATO])'nün, üyesi olmayan ülkelerin sistemlerine entegre olma ihtimalini istemediği için yaşanan S-400 krizi göz önüne alındığında, Türkiye'nin üye olmayan ülkelere karşı veri paylaşımına izin verilmeyeceğini göz ardı etmemesi gerekmektedir.[50] İzin derecelerinde esnekliğe müsaade eden Hyperledger Fabric platformunun TSK adına önerilmesinin nedenleri, ''bilmesi gereken prensibine''[51] uygun bileşenlere sahip olması, izinli özel bir zincir yapısına sahip olmasının yanında izinli açık zincirlerin eklenmesine olanak tanıması, konsensüs protokolleri açısından madencilik işlemine ihtiyaç duyulmadığı için daha az enerji harcayacağından çevreye zararının daha az olması ve düşük işlemcili cihazlarda çalıştırılabilir olmasıdır.[52] Hyperledger'ın sunduğu blok zinciri tabanlı dağıtık defter teknolojisi açık kaynak kodlu olduğundan esnek, modüler ve geliştirilebilir bir yapıya sahiptir. Bunun yanında Hyperledger'ın sunduğu dağıtık defter teknolojisi iki farklı kategoriden toplam on adet teknoloji sunmaktadır.[53] Bunlardan ilk beş tanesi "frameworks" olarak kategorileştirilen; Hyperledger Burrow, Fabric, Indy, Iroha ve Sawtooth olarak karşımıza çıkmaktadır. İkincisi "tools" olarak belirlenen; Hyperledger Callper, Cello, Composer, Explorer ve Quilt'dir. Buna göre Hyperledger blok zinciri farklı "frameworks" ve "tools" olarak belirlenen dağıtık defter teknolojileriyle kullanıcılar arasında iş birliği sağlayarak verilerin iletimi ve saklanmasında aracı olmaktadır. Aynı zamanda yeni iş ve uzlaşma modellerinde de yeniliği ve verimliliği arttıracak altyapı olanağı sağlamaktadır.

[49]https://www.ibm.com/tr-tr/topics/hyperledger, erişim 21.07.2022.
[50]Sami Yıldırım, ''Yabancı Askerî Üsler ve İthâl Silah Sistemleri Özelinde Türkiye'nin İttifak Sorgulamaları'', 2019, s.322-323.
[51] Savunma Sanayii Güvenliği Yönetmeliği, https://www.resmigazete.gov.tr/eskiler/2010/06/20100604-2.htm, Madde 4/ç, erişim 20.07.2022.
[52]Sharon Cocco and Gari Singh, ''Top 6 technical advantages of Hyperledger Fabric for blockchain networks'', 2018, https://developer.ibm.com/articles/top-technical-advantages-of-hyperledger-fabric-for-blockchain-networks/, erişim 09.06.2022.
[53] https://www.hyperledger.org/wp-content/uploads/2018/07/HL_Whitepaper_IntroductiontoHyperledger.pdf, erişim 10.06.22.

Bununla birlikte kimlik bilgilerinin dijitalleşmesinde ve dijital güvenliğin sağlanmasında teknik imkanlar tanıması Hyperledger'ın tercih edilmesindeki gerekçelerdendir.

Bu çalışmada ise yüksek derecede gizlilik, esneklik ve dayanaklılık sağladığından Hyperledger Fabric önerilmektedir. Farklı kurum ve kuruluşların olduğu bir ağ yapısında gerçek zamanlı bilgi paylaşımı geleneksel sistemde verimsiz ve ağır işlemekle beraber bilgi güvenliği de tehlike altındadır. Askerî alanda bilgi akışı ve güvenliğinin verimliliği kritik bir role sahip olduğundan yüksek güvenlik katmanlı, esnek ve kullanışlı bir sistemin oluşturulması gerekmektedir. Bu bağlamda Hyperledger Fabric kullanıldığı durumda; birden fazla kurum veya kuruluş arasında sağlanan altyapı sayesinde "gerçek anlamda" yüksek güvenlikli ve güvenilir bir bilgi akışı sağlanabilecektir.[54] Hyperledger Fabric'de kurumlar, bir ağ içerisinde farklı iletişim kanallarında bulunarak bilgi akışını sağlamaktadır.[55] Hyperledger Fabric'in bilgi akışı ve güvenliği sağlama konusunda "Özel Veri Koleksiyonları" (Private Date Collections) kritik bir role sahiptir. Çoğunlukla bir kurum veya kuruluş farklı bir kanaldan gelen bilginin gizliliğini sağlamak için ayrı bir iletişim kanalı oluşturması gerekmektedir. Hyperledger Fabric'de ise bir kanaldaki belirli bir kuruluşun alt kümesine ayrı bir kanal yaratmak zorunda kalmadan özel verileri onaylama, taahhüt etme veya sorgulama imkânı veren özel veri koleksiyonları oluşturma olanağı sunulmaktadır.[56]

5. Önerilen Özel Zincir Yapısının SWOT Analizi

SWOT analizi stratejik yapıların belirlenmesi için kullanılmaktadır. Güçlü ve zayıf yönler, TSK için önerilen blok zinciri yapısında içsel faktörlerin belirleyeceği unsurları ifade etmektedir. Fırsatlar ve tehditler ise çevresel (dışsal) etkilerin ortaya çıkarabileceği faktörlerdir.[57] Bu çalışmada SWOT analizine temel olan faktörler ilk olarak yazarların literatüre dayalı argümanlarından türetilmiştir. Elde edilen argümanlar konu hakkında uzman olan üç TSK personelinin ve dört akademisyenin görüşlerine sunulmuş ve argümanlar bu görüşler doğrultusunda güncellenerek bulgu haline getirilmiştir. Tablo 1, güçlü ve zayıf yönler ile fırsat ve tehdit unsurlarını özetlemektedir.

[54]Dongcheng Li, W. Eric Wong and Jincui Guo, ''A survey on blockchain for enterprise using hyperledger fabric and composer.''2019 6th International Conference on Dependable Systems and Their Applications (DSA). IEEE, 2020, s.71-80.
[55]https://hyperledger-fabric.readthedocs.io/en/release-2.2/network/network.html, erişim 11.06.22.
[56]https://HyperLedger-fabric.readthedocs.io/en/release-2.2/private-data/private-data.html, erişim 11.06.22
[57]Emet Gurl, ''SWOT analysis: A theoretical review''. Procedia Computer Science, 2017, s.145-1154.

Tablo 1. TSK Blok Zinciri Teknolojisi Swot Analizi[58]

Güçlü Yönler	Zayıf Yönler	Fırsatlar	Tehditler
MSB mahremiyeti Verilerde değiştirilemez ve silinemezlik Verilerin güvenliği ve tamlığı Afet ve fiziksel saldırılara karşı güvenlik artışı Merkezi sunucu sistemlerine göre daha güvenli olması Kurum içinden gelebilecek saldırılara karşı sistem güvenliğinin sağlanması Açık zincir yapısına göre düşük enerji maliyeti Kâğıt ve belge yükünden kurtulma Kurum içi kimlik denetimi ve teyidi Kanıtlanabilirlik-inkâr edilemezlik Mali denetlenebilirlik	Enerji maliyeti %100 güvenlik sağlanması mümkün olmadığı için çeşitli siber saldırıların gerçekleştirilme ihtimali Zincir altyapısının kuruluş maliyeti Verilerin artışı sonucu oluşabilecek performans sorunları İşlem doğrulama mekanizmasının gecikebilmesi Fabric'de geç iptal edilen işlemlerin performansı olumsuz etkilemesi Zincir kodunun (Chaincode) güvenlik açığı oluşturabilme ihtimali Uzman Eksikliği Sözlü Emir Tespiti	Tespit hatası (insan hatası) azalma Veri girişlerinde ve düzeltmelerde yetkili birim izni Hatalı kimlik tespiti Denetleme kolaylığı Siber güvenlik maliyetlerinde azalma Kalıcı ve doğrulanabilir Muhasebe Kayıtları Bilmesi gereken prensibine sadık kalınabilmesi Hukuki problemlerde inkâr edilemez deliller Kamusal zincirlerin eklenebilmesi Nesnelerin interneti koordinasyonu ile İHA-SİHA pilotaj maliyetlerinin azalması Fiziksel saldırı ile İHA-SİHA teknolojisinin çalınamayacak hâle gelmesi	Goldfinger veya %51 saldırısı Özel Anahtar Saldırısı Sybil Saldırısı DAO (Decentralized Autonomous Organization) Saldırısı Solucan Deliği Saldırısı (Wormhole attack) Bilgi akışında gizlilik sağlandığı için dış tehditlerle karşı karşıya kalma potansiyeli Kurum katılımcıları anonim olamadığından sorumluluk algılarının değişimi nedeniyle adaptasyon problemleri

5.1. Güçlü Yönler

Blok zinciri teknolojisine geçilmesi ile silahlı kuvvetlerin en hayati ilkelerinden biri olan mahremiyet/gizlilik ihtiyacı TSK içi ‘‘bilmesi gereken prensibine’’ sadık kalınarak, verilerin güvenliği ve tamlığı en üst seviyede saklanabilir. Bir başka deyişle blok zinciri teknolojisi

[58] Tablo 1. yazarlar tarafından oluşturulmuştur.

sayesinde merkezi sunucu sistemlerine göre siber saldırılara karşı daha güvenli hâlde veriler saklanabilecektir.

Doğal afet ve fiziksel saldırılara karşı güvenlik blok zinciri teknolojisinin önemli avantajlarından biridir. 12 Ocak 2010 tarihinde Haiti'de meydana gelen Richter ölçeğine göre yedi şiddetindeki yüz binlerce kişinin ölümüne yol açan deprem esnasında kamu binalarının hasar görmesi nedeniyle devlet arşivlerinin büyük bir kısmı yok olmuştur. Devlet arşivleri içinde tapu kayıtlarının da olması, deprem sonrası ciddi karışıklıklar yaratmıştır.[59] Benzer biçimde kamusal veri sisteminin ciddi hasar görmesi, deprem sonrası gönderilen uluslararası yardımların ihtiyaç sahiplerine ulaşmasını engellemiştir. Haiti depremi sonrasında doğal afetler durumunda blok zinciri teknolojisinin faydaları konusunda yeni bir literatür oluşmaya başlamıştır.[60] Benzer bir durum potansiyel bir savaş durumunda da oluşabilmektedir. Suriye'deki savaş sırasında belirli bir bölgeyi ele geçiren her örgüt/grup tapu kayıtlarını ve devlet arşivlerini tahrif etmiştir. Afganistan'da Taliban yönetiminin arşiv belgelerini tahrif ettiğine dönük ciddi ithamlar vardır.[61] Blok zinciri teknolojisi, doğal afet ya da savaş hâllerinde arşiv kayıtlarının yok olması ve tahrif edilmesi konusunda güvenli bir alternatif sunmaktadır.

Siber saldırılara karşı mevcut merkezi sunucu sistemi içerisinde güvenlik önlemi alma çabası azalacaktır. Bu sayede siber güvenlik önlemlerinin maliyetlerinde kayda değer azalışlar söz konusu olacaktır. Zincir teknolojisinin en önemli özelliği, verilerin değiştirilemez ve silinemez olmasıdır. Kurum içinden gelebilecek saldırılara karşı da sistem kendini koruyabilir niteliktedir. Hukuki problemler oluştuğunda kanıtlar yok edilemez, değiştirilemez hâlde kayıtlı olduğu için inkâr edilemez olduklarından problemlerin doğru çözülmesi sağlanabilir. Kalıcı ve doğrulanabilir ''muhasebe kayıtları'' sayesinde tedarik zinciri ile veya kurum içinde ortaya çıkabilecek kayıp/kaçağın önlenmesi ve mali denetlenebilirlik artışı sağlanabilecektir. İspat yükümlülüğü veya denetlemeler için saklanması gereken belgelerin sistem içindeki kalıcılığı nedeniyle kâğıt ve doküman maliyetlerinin ortadan kalkması mümkün hâle gelebilir.

[59] ''Haiti Gov't Says 150K Bodies Recovered In Capital'', https://www.wbur.org/news/2010/01/24/bc-cb-haiti-earthquake, erişim 22.07.22.
[60] Haiti depremi sonrasında doğal afetler durumunda blok zinciri teknolojisinin faydaları konusunda yeni bir literatür oluşmaya başlamıştır. Literatür hakkında bilgi için bkz., Okan Arabacı, ''Blockchain consensus mechanisms: the case of natural disasters.'', UPTEC STS, ISSN 1650-8319; 18028, 2018.
[61] ''Afghanistan's Film Archives Were Saved from the Taliban Once Before. What Now?'', https://www.indiewire.com/2021/10/afghan-film-archives-taliban-1234660410/, erişim 22.07.22.

5.2. Fırsatlar

Özel zincir yapısı ile sisteme yanlış bir veri girişi söz konusu olsa dahi bu yanlış verinin kim tarafından girildiği belirli olduğu için değiştirilip düzeltilmesi amacıyla yetkili düğüm (TSK özelinde bu düğüm yetkili birim komutanı olacaktır) onay vermektedir. Böylece kurum içi kimlik teyidi ve denetimi de sağlanabilir hâlde kalmaktadır. Girilen bilgiler onay verilmeden değiştirilemediğinden söz konusu hatanın hangi kimlik tarafından yapıldığının veya düzeltildiğinin tespiti açık bir şekilde sistemde kayıtlı kaldığı için denetlemelerde ortaya çıkabilecek tespit hatası (insan hatası) en aza indirilebilir.

Özel blok zinciri yapısına ‘‘kamusal blok zinciri yapısı’’ da eklenerek ‘‘konsorsiyum blok zinciri’’ ile TSK içerisindeki tedarik zinciri altyapısı ve ihale sistemleri de dahil edilebilir. Nesnelerin interneti (IOT) ile blok zinciri teknolojisinin koordinasyonu (bütünleşik teknoloji) sayesinde İHA-SİHA kullanımlarında yer pilotlarına ihtiyacın ortadan kalkması, “hacklenerek” düşürülmelerinin zor hâle gelmesinin yanında olası bir fiziksel saldırı aracılığıyla düşürüldüğünde teknolojisinin çalınamayacak olması ile söz konusu ekonomik kayıplar ciddi düzeyde azaltılabilir. Açık zincir yapısındaki onay için yapılan madencilik işlemi özel zincir yapısında yetkili düğüm tarafından yapılarak enerji maliyeti bu yapıda daha düşük gerçekleşmektedir.

5.3. Zayıf Yönler

Merkezi sunucu sistemlerinden özel zincir yapısına geçilirken altyapının kuruluş maliyeti ortaya çıkacaktır. Verilerin saklanmasının ortaya çıkardığı bir enerji maliyeti oluşacaktır. Sisteme entegre edilen verilerin artışı ile performans sorunları ortaya çıkabilecektir. %100 güvenliği kapalı ağ yapılarının (İntranet) da sağlayamadığı gibi blok zinciri yapısında da çeşitli siber saldırıların gerçekleştirilme ihtimali söz konusudur. Hyperledger Fabric’de eş düğümlerin defterleri elinde tutmasından dolayı sisteme yapılacak bir saldırı önemli bilgilerin sızmasına yol açabilecektir. Bunun yanında işlem doğrulama mekanizmasının belirli aşamalar ve eş tiplerinden geçmesinden dolayı bu mekanizma gecikebilmektedir. Aynı zamanda işlem emiri verildikten sonra iptal sürecinin bazı durumlarda geç gerçekleşmesi, sistem performansını olumsuz etkileyebilmektedir.

Fabric kapalı blok zinciri ağı, katılımcıları anonim kılmadığından askerî alandaki kurumların bir kısmı, bu teknolojiyi tercih etme noktasında çekingen davranabilecektir.

Bununla birlikte askerî teknoloji altyapılarında kullanım örneklerinin az olmasından dolayı sistemin uzun vadede yaratacağı sonuçlar açısından belirsizlikler ortaya çıkabilir. Türkiye örneği ele alındığında, sistem mimarisi hakkında bilgili bir ekip oluşturmak Hyperledger Fabric'in daha etkin çalışmasına yol açabilecektir. Dolayısıyla sistem mimarisinde uzman kişilerin eksikliği de bir zayıflık olarak değerlendirilebilir.[62]

Hyperledger Fabric'de akıllı sözleşmelerin "chaincode" (zincir kodu) üzerinden uygulanması kod içerisinde güvenlik açığı riskini oluşturabilmektedir. Blok oluşturulduktan sonra zincir kodunun geri alınması olanaksızdır. Bu yüzden zincir kodu oluşturulmadan önce güvenlik açığının olup olmadığının analiz edilmesi gerekmektedir.[63] Zincir kodunun karmaşık yapısı, güvenlik açığının nereden kaynaklandığını zorlaştırabilmektedir. Askerî alanda bilgilerin kritik derecede önemli olması, zincir kodu üzerinden güvenlik açığının ortaya çıkmamasını zorunlu hâle getirmektedir. Bu yüzden zincir kodu uzmanları, güvenlik açığını bulmak konusunda kritik bir role sahiptir. Hizmete aykırı veya konusu suç teşkil eden asker emirleri gerçekleştirmenin hukuki mahiyeti göz önüne alındığında, merkezi sistemin de zayıf yönü olan sözlü emirlerin sisteme entegre olmaması nedeniyle, blok zinciri teknolojisinde de sözlü emiri veren komutanların kimlikleri tespit edilemeyecektir. Hukuki anlamda bu sürecin zorlukları devam edecektir.

5.4. Tehditler

Golfinger diğer adıyla %51 saldırısı sistemin büyük çoğunluğu elde tutma ile gerçekleşebilmektedir.[64] Türkiye'de yaşanan 15 Temmuz 2016 tarihli darbe girişimi örneğinde ''İçeriden Gelebilecek Veri Elde Etme, Değiştirme, Ele Geçirme İsteği'' blok zinciri yapısında saldırganın sistem içindeki %51 kullanıcıyı ikna etmesi yoluyla gerçekleşebilmesi zincir teknolojisinin siber güvenlik bağlamında MSB'de kullanılmasının önemini göstermektedir. Önerilen blok zinciri modelinde PBFT (Pratik Bizans Hata Toleransı) protokolü kullanılmaktadır. Bu protokolde bilginin ağa yazılması için onaylayanların sayısının 2/3 olması gerekmektedir. [65] Bu bağlamda protokolün önemli bir eksisi n>20 olduğunda düğümler

[62]Billy Brock, ''The Pros and Cons of Hyperledger Fabric'', https://www.verypossible.com/insights/the-pros-and-cons-of-hyperledger-fabric, erişim 28.07.22.
[63]Yangsun Lee, A Study on Intermediate Code Generation for Security Weakness Analysis of Smart Contract Chaincode. Webology, 19:1, 2022.
[64]Melanie Swan, Blockchain: Blueprint for a new economy. O'Reilly Media, Inc., 1st edition, USA, 2015, s. 83.
[65]Süleyman Kardaş, ''Blokzincir teknolojisi: uzlaşma protokolleri.'', Dicle Üniversitesi Mühendislik Fakültesi Mühendislik Dergisi 10.2, 2019, s.481-496.

arasındaki iletişimin üstel olarak artmasıdır. Üstel artan iletişim ise protokolün ölçeklenmesinde problem ortaya çıkarabilir. Bununla birlikte protokol, ağda bulunan kötü niyetli düğümlerin 1/3'ü geçmediği bir durumda çalışmaktadır. Bu sebeple sistem Sybil saldırısına karşı oldukça hassastır. Sistemi yavaşlatmak veya çökertmek için sahte düğümlerin kullanılarak ağı meşgul etmek maksadıyla yanlış bilgilerin gönderilmesi ile gerçekleşen saldırı çeşidi Sybil saldırısıdır.[66] Bu saldırının literatürde sahte "*düğümlerin*" var olan teknolojide yoğun hesaplama yapamaması nedeniyle sadece teorik olarak mümkün olduğu ifade edilmektedir.[67] Özel anahtar saldırısı ise blok zincirine erişimi kendi hesabı üzerinden sahibine açan özel anahtarın kaybedilmesi veya silinmesi ile verinin kaybolmasına sebebiyet vermektedir.[68] Merkeziyetsiz Otonom Organizasyon (Decentralized Autonomous Organization [DAO]) ağına Ocak 2016'da gerçekleştirilen saldırı da saldırgan ağda mevcut 3,6 milyon Ether'i oluşturduğu yeni DAO ağına yönlendirmiştir. DAO saldırısı olarak nitelendirilen bu atak Ethereum'un uygulaması olan DAO ağına zararlı kod içeren akıllı sözleşme ile yapılmıştır.[69] Özel zincir yapısında söz konusu olamayacak bu saldırı tedarik zinciri ve ihale sistemlerinin ağa dahil edilmesi ile oluşturulabilecek konsorsiyum ağına karşı söz konusu olabilecektir. Bir diğer saldırı olan "solucan deliği saldırısı" (wormhole attack) Hyperledger Fabric'de iletişim kanalları içindeki üyelerden birini tehlikeye atmak aracılığıyla kanaldaki tüm defter bilgilerinin kanal dışındaki herkese ulaşmasına yol açabilmektedir.[70]

Tehditler bölümünde siber saldırılar dışında, blok zincir teknolojinin askerî alanda kullanılmasının bir takım politik sonuçları ortaya çıkaracak potansiyeli olabilir. Bilgi akışında, işlem verileri gizlilik kazanabilmektedir. Bu durum farklı ülkelerin askerî alanda bilgi alma sürecini aksatabildiğinden dış tehditlerle karşı karşıya kalınmasına yol açabilir. Bunun yanında kurum katılımcıları anonim olmadığından, kurumların sorumluluk algıları değişebilir. Katılımcı olan kurumun ilgili tüm faaliyetleri deftere kaydedildiğinden "hesap verilebilirlik" algısını değiştirecektir. Bu durum geçiş sürecinde sorunlar ve aksamalara neden olabilir.

[66] John R. Douceur, *The sybil attack. In: International workshop on peer-to-peer systems*. Springer, Berlin, Heidelberg, 2002, s.251.
[67] Oğuzhan Taş ve Farzad Kiani, ''Blok zinciri teknolojisine yapılan saldırılar üzerine bir inceleme'', Bilişim Teknolojileri Dergisi, 11:4, 2018, s.376.
[68] Enis Konacaklı ve Enis Karaarslan, Age, s.226.
[69] Enis Konacaklı ve Enis Karaarslan, Age, s.227.
[70] Nitish Andola, et al., ''Vulnerabilities on hyperledger fabric." *Pervasive and Mobile Computing* 59,101050, 2019.

6. Sonuç

Bu çalışmada, askerî alanda siber güvenlik bağlamında blok zinciri teknolojisinin avantajları ve dezavantajları SWOT analizi yöntemiyle ele alınmıştır. Elde edilen bulgulara göre, blok zinciri teknolojisinin sadece "veri saklama" amacıyla kullanımı bile siber güvenlik alanında birçok siber saldırının önüne geçebilmektedir. Geleneksel ağ yapısına yapılan DoS, DDoS vb. saldırılar önlenebilmekte, verilerin değişmezliği ve deftere kaydedilen bilgilerin silinemezliği, özellikle içeriden yapılan saldırıların tamamen izlenebilir olmasını sağlamaktadır. Türkiye'deki ''Kozmik Oda Soruşturması'' ve ''15 Temmuz Darbe Girişimi'' veri güvenliğinin blok zinciri teknolojisinin kullanarak sağlanmasının kritik derecede önemli olduğunun somut göstergeleridir. Hyperledger Fabric gibi blok zinciri ağları merkezi veri tabanlarındaki verilerin tahrif edilmesini önleyebilir; ağın konsensus mekanizması, emir komuta zincirine uygun olmayan bir başka deyişle hukuksuz emirleri sistemden dışlayabilir. 15 Temmuz Darbe Girişiminin blok zinciri literatüründe sıklıkla kullanılan "Bizans Generalleri Problemi"ne olan benzerliği dikkat çekicidir. Bulgular, literatürde ABD, Çin ve bazı AB ülkeleri özelinde blok zinciri teknolojisini askerî alana entegre etmek üzere yaptığı çalışmalarla uyumludur.

Siber güvenlik alanında yapılacak harcamaların önümüzdeki üç yıla kadar, 100 milyar doların üzerine çıkacağı tahmin edilmektedir. Türkiye gibi her türlü tehdite maruz kalan bir ülkenin yakın gelecekte savunma ve siber güvenlik alanında yapacağı harcamaların artacağı söylenebilir. SWOT analizinden elde edilen bulgulara göre, blok zinciri teknolojisinin askerî alanda kullanımı ile pek çok alanda ekonomik maliyetleri azalttığı görülmektedir. Bir ülkede özellikle askerî verilerin güvenliğinin fırsat maliyeti düşünüldüğünde, veri güvenliğinin hayati öneme sahip olduğu söylenebilir. Literatürde, özellikle ABD-İran arasındaki siber savaşta, ''gizli'' ar-ge sonuçlarının çalınması ve çalınan teknolojinin geliştirilerek pazardaki yerinin işgal edilmesi konunun önemini gösteren örneklerdendir.

Blok zinciri teknolojisinin askerî alanda Türkiye bağlamında farklı kullanım alanları da bulunmaktadır. Gelecek çalışmalarda blok zinciri teknolojisinin, tedarik zinciri, İHA-SİHA'larda nesnelerin interneti ile koordinasyonu (Bütünleşik Teknoloji), ihale yönetimi gibi konularda potansiyel kullanım alanları ile ilgili çalışmaların yapılması, bu çalışmanın bulgularını güçlendirecektir. Bu makalenin, teknoloji odaklı askerî uygulamalar bağlamında blok zincirini ele alan yeni çalışmaları teşvik etmesi öngörülmektedir.

Extended Summary

The notions of cyber war and cyber security, which emerged with the acceleration in technology after the Second World War, caused "data security" to be one of the most critical items of military expenditures of countries. The most important factor in cybersecurity is data security and accuracy. To ensure data security, new technologies for data collection and storage have been constantly developed. One of the technologies developed to increase the security of data is blockchain technology. This study discusses to use of a blockchain-based network system instead of the “intranet” which is utilized at the Turkish Armed Forces (TAF) as part of cyber security and defense economics. With the pioneering work of Nakamoto (2008), a cryptographically based and decentralized network structure has emerged. This structure, known as blockchain technology, has created the possibility of cryptographic evidence-based data transmission, and a recording system that does not rely on trust, since it also incorporates distributed ledger technology (DLT). Pilot studies are being conducted for the use of blockchain technology, which has been used in many areas, including the military since 2008. For example, Defense Advanced Research Projects Agency's (DARPA) Data Protection in Virtual Environments (DPRIVE) project in the United States aims to develop blockchain systems to combat supply chain attacks, manage military logistics, and establish secure communication channels on the battlefield. The European Union states that blockchain technology can affect various sectors in the EU and that it can play an important role in laying the foundations for the digital EU such as the Digital Single Market Initiative, Directorate General for Communications and Technology (DG-CONNECT), European Blockchain Partnership (EBP), and European Blockchain Services Infrastructure (EBSI) seem to offer all sorts of opportunities for the development of civil-military blockchain technology. Not only Western countries but also China is making significant investments in blockchain technology. People's Liberation Army (PLA) plans to use blockchain technology to manage the distribution of funds for intelligence operations, protect the data of defense personnel, maintain the life cycle of weapons and military logistics, and make operations significantly safer. In this context, the objective of the study is to determine the strengths and weaknesses of the blockchain-based network system in military applications, especially the TAF, and to identify the opportunities and threats. Studies on Blockchain in military context in both national and international literature are relatively scarce. The literature mostly neglects the weaknesses/disadvantages and the economic context

of using blockchain technology in military applications. This article focuses on the neglected elements of the use of blockchain technology in the military field using the method of "SWOT analysis". According to the findings of SWOT analysis, it has been determined that the blockchain provides a serious advantage over the traditional network systems in the field of cybersecurity against all other cyber and physical attacks except a private key, %51 (Goldfinger), Sybil, DAO, Wormhole attacks. With the transition to blockchain technology, the need for privacy and confidentiality, which is one of the most important principles of the Armed Forces, can be maintained at the highest level by adhering to the "need-to-know principle" for the TAF. Even in the event of an erroneous data entry into the system with the special chain structure, the authorized node (commander of the authorized unit) may approve modifications and corrections, since the technology reveals who processed the incorrect data. Thus, identity confirmation and control remain possible within the facility. Since the information entered cannot be changed, the identification of the identity that made or corrected the error remains recorded in the system, minimizing the recognition error (human error) that can occur during the checks. Blockchain technology has been found to reduce potential economic costs due to the immutability, indestructibility, and inerasibility of data. Considering the opportunity cost of military data security in a country, it can be said that data security is of critical importance. Therefore, in line with the literature, this article argues that R&D studies for the transition to blockchain technology in military applications should be accelerated. The study is divided into three parts. The first chapter explains the importance of cybersecurity in military applications. In the second part, blockchain technology is presented and its application in the military field is discussed. In the third part, the applicability of blockchain technology in the military field and its strengths/weaknesses have been studied and suggestions have been made on the necessity of switching to this technology in terms of cybersecurity and cost-effectiveness of the Turkish Armed Forces.

Kaynakça

Andola Nitish, Et Al (2019). ‘‘Vulnerabilities On Hyperledger Fabric." *Pervasive And Mobile Computing* 59,101050.

Angin Pelin (2020). Blockchain-Based Data Security İn Military Autonomous Systems, *Avrupa Bilim Ve Teknoloji Dergisi*, 362-368.

Arabacı Okan (2018). Blockchain Consensus Mechanisms: The Case Of Natural Disasters, Uptec Sts, Issn 1650-8319; 18028, 2018.

Baezner Marie Ve Robin Patrice (2017). *Stuxnet* (No. 4), Center For Security Studies(Css) Eth Zurich, S.4-5.

Cebeci Atilla (2022). *Türkiye'nin Seçili Kalkınma Planlarının Karşılaştırmalı Analizi*, Master's Thesis, Trakya Üniversitesi Sosyal Bilimler Enstitüsü.

Copeland B. Jack (Ed.) (2004). *The Essential Turing*, Clarendon Press, S.232.

Çerkezoğlu Cem (2006). *Kara Kuvvetleri Komutanlığında Uzaktan Eğitim Uygulamaları,* Yüksek Lisans Tezi, Sakarya Üniversitesi, Sakarya, S.102.

Darıcılı Ali Burak (2017*). Amerika Birleşik Devletleri Ve Rusya Federasyonu'nun Siber Güvenlik Stratejilerinin Karşılaştırmalı Analizi*, Doktora Tezi, Uludağ Üniversitesi, Bursa, S.63.

Darıcılı Ali Burak Ve Özdal Barış (2017). Rusya Federasyonu'nun Siber Güvenlik Kapasitesini Oluşturan Enstrümanların Analizi, *Bilig*, (83), 121-146, S.131.

Douceur John R. (2002). The Sybilsybil Attack, In *International Workshop On Peer-To-Peer Systems* (Pp. 251-260), Springer, Berlin, Heidelberg, S.251.

Gupta Brij B. Ve Badve Omkar P. (2017). Taxonomy Of Dos And Ddos Attacks And Desirable Defense Mechanism İn A Cloud Computing Environment, *Neural Computing And Applications*, *28*(12), 3655-3682, S.1-2.

Gurl Emet (2017). Swot Analysis: A Theoretical Review, Procedia Computer Science, S.145-1154.

İstikbal Deniz (2022). "Türkiye'nin Savunma Harcamaları", Kriter Dergi, 6:66, S.54-55.

Karahan Çetin Ve Tüfekçi Aslıhan (2019a). Blokzincir Teknolojisinin İç Denetim Faaliyetlerine Etkileri: Fırsatlar Ve Tehditler. *Denetişim*, (19), 55-72.

Karahan Çetin Ve Tüfekçi Aslıhan (2019b). Blokzincir Teknolojisi Ve Kamu Kurumlarınca Verilen Hizmetlerde Blokzincirin Kullanım Durumu. *Verimlilik Dergisi*, (4), 157-193.

Kardaş Süleyman (2019) Blokzincir Teknolojisi: Uzlaşma Protokolleri, Dicle Üniversitesi Mühendislik Fakültesi Mühendislik Dergisi, 10.2: S.481-496.

Konacaklı Enis (2019). *Ulusal Güvenlik İçin Blokzinciri Tabanlısiber Güvenlik Modeli* (Master's Thesis, Eskişehir Teknik Üniversitesi).

Konacaklı Enis Ve Karaarslan Enis (2021). *Blokzincirinin Askerî Lojistik Takip Sistemlerinde Kullanılması*, Siber Güvenlik Ve Savunma: Blokzinciri Ve Kriptografi, Ankara, Nobel Yayınevi, S.223-226-227.

Küçükkıralı Zeynep Ve Afşar Kerim Eser (2022). Türkiye'de Merkez Bankası Dijital Parasının Potansiyel Etkileri: Swot Analiziyle Bir Değerlendirme. *Selçuk Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, (48), 142-158.

Lee Suhyeon Ve Kim Seungjoo (2021). Blockchain As A Cyber Defense: Opportunities, Applications, And Châllenges, *Ieee Access*, *10*, 2602-2618.

Lee Yangsun (2022). A Study On Intermediate Code Generation For Security Weakness Analysis Of Smart Contract Chaincode. Webology, 19:1.

Lı Dongcheng, Wong W. Eric, Guo Jincui (2020). ''A Survey On Blockchain For Enterprise Using Hyperledger Fabric And Composer.'' In: *2019 6th International Conference On Dependable Systems And Their Applications (Dsa)*. Ieee, P. 71-80.

Lılly Bilyana Ve Lılly Sale (2021). Weaponising Blockchain: Military Applications Of Blockchain Technology İn The Us, China And Russia, *The Rusı Journal*, *166*(3), 46-56.

Lukasık Stephen (2010). Why The Arpanet Was Built, *Ieee Annals Of The History Of Computing*, *33*(3), 4-21, S.12.

Mcabee Ashley, Tummala Murali Ve Mceachen John (2019). Military İntelligence Applications For Blockchain Technology, Proceedings Of The 52nd Hawaii International Conference On System Sciences, S.6031-6040.

Nakamoto Satoshi (2008). A Peer-To-Peer Electronic Cash System. *Bitcoin.–Url: Https://Bitcoin. Org/Bitcoin. Pdf*, *4*, 2.

Polcumpally Arun Teja (2022). Blockchain Technology And İts İmportance İn The Military Applications, Css, S.2.

Swan Melanie (2015). *Blockchain: Blueprint For A New Economy*, " O'reilly Media, Inc.", 1st Edition, S.83.

Şat Nur (2019). Blokzincir (Blockchain)'İn Kamu İdaresine Olası Etkileri Üzerine. *Amme İdaresi Dergisi*, *52*(4).

Taş Oğuzhan Ve Kiani Farzad (2018). Blok Zinciri Teknolojisine Yapılan Saldırılar Üzerine Bir İnceleme, *Bilişim Teknolojileri Dergisi*, *11*(4), 369-382, S.376.

Taylor Paul J. Et Al (2020). A Systematic Literature Review Of Blockchain Cyber Security *Digital Communications And Networks*, *6*(2), 147-156.

Törenli Nurcan (2004). *Enformasyon Toplumu Ve Küreselleşme Sürecinde Türkiye*, Bilim Ve Sanat Yayınları, Ankara, S.10-11.

Zhu Y. Et Al (2020). A Study Of Blockchain Technology Development And Military Application Prospects, In *Journal Of Physics: Conference Series* (Vol. 1507, No. 5, P. 052018), Iop Publishing.

İnternet Kaynakları

‘‘5th Generation Cyber Attacks Are Here And MostBusinesses Are Behind- A New Model For Assessing and Planning Security’’, http://www.infosecurityeurope.com erişim 07.06.2022.

‘‘Afghanistan’s Film Archives Were Saved from the Taliban Once Before. What Now?’’, https://www.indiewire.com/2021/10/afghan-film-archives-taliban-1234660410/, erişim 22.07.22.

‘‘Blokzincir’’, https://blokzincir.bilgem.tubitak.gov.tr/blok-zincir.html, erişim 08.06.2022.

‘‘Global Risks Report’’, https://www.weforum.org/reports/global-risks-report-2022/, erişim 07.06.2022.

‘‘Haiti Gov't Says 150K Bodies Recovered In Capital’’, https://www.wbur.org/news/2010/01/24/bc-cb-haiti-earthquake, erişim 22.07.22.

BAKİ Ozan, ‘‘Rusya, Küresel İnternet Ağıyla Bağlantısını Başarıyla Kesti’’, https://www.webtekno.com/rusya-kuresel-internet-agiyla-baglantisini-kesti-h82374.html, erişim 25.05.2022.

BROCK Billy, ‘‘The Pros and Cons of Hyperledger Fabric’’, https://www.verypossible.com/insights/the-pros-and-cons-of-Hyperledger-fabric, erişim 28.07.22.

Edward Snowden Interview ‘‘The NSA and Its Willing Helpers’’, https://www.spiegel.de/international/world/interview-with-whistleblower-edward-snowden-on-global-spying-a-910006.html, erişim 22.05.2022.

https://emn178.github.io/online-tools/sha256.html, erişim 09.06.2022.

https://Hyperledger-fabric.readthedocs.io/en/release-2.2/network/network.html, erişim 11.06.22.

https://Hyperledger-fabric.readthedocs.io/en/release-2.2/private-data/private-data.html, erişim 11.06.22.

https://www.aa.com.tr/tr/15-temmuz-darbe-girisimi/izmirdeki-askeri-casusluk-sorusturmasinda-kumpas-davasinda-karar/1904912 erişim 26.10.22

https://www.crowell.com/files/Potential-Uses-of-Blockchain-Technology-In-DoD.pdf, erişim 23.06.2022.

https://www.globalfirepower.com/countries-listing-nato-members.php, erişim 23.07.2022.

https://www.globalfirepower.com/countries-listing.php, erişim 23.07.2022.

https://www.Hyperledger.org/wp-content/uploads/2018/07/HL_Whitepaper_IntroductiontoHyperledger.pdf, erişim 10.06.22.

https://www.ibm.com/tr-tr/topics/Hyperledger, erişim 21.07.2022.

https://www.ig.com/en/trading-strategies/what-is-blockchain-technology--200710, verileri kullanılarak tarafımızca revize düzenlenmiştir, erişim 09.06.2022.

https://www.mckinsey.com/business-functions/risk-and-resilience/our-insights/cybersecurity/cybersecurity-trends-looking-over-the-horizon, erişim 24.07.2022.

https://www.msb.gov.tr/SlaytHaber/milli-savunma-bakani-sn-fikri-isik-ulastirma-denizcilik-ve-haberlesme-bakani-sn-ahmet-arslan-ile-siber-guvenlik-isbirligi-protokolunu-imzaladi, erişim 24.10.22

https://www.ntv.com.tr/turkiye/kozmik-oda-nedir,lqaMw53CdEq8SlGV-ASz_A erişim 28.10.22 ‘‘5th Generation Cyber Attacks Are Here And MostBusinesses Are Behind- A New Model For Assessing and Planning Security’’, http://www.infosecurityeurope.com erişim 07.06.2022.

https://www.trthaber.com/haber/gundem/kozmik-oda-casusu-bilgileri-harddiskle-feto-elebasina-goturmus-530949.html erişim 26.10.22

KILIÇ Hakan, ‘‘ABD'nin dev casus uçağı İran tarafından düşürüldü: Peki şimdi ne olacak?’’, https://www.yenisafak.com/gundem/iranin-abd-ucagini-dusurmesi-nasil-sonuclar-doguracak-3495626, erişim 23.05.2022.

SHARON Cocco and GARİ Singh, ‘‘Top 6 technical advantages of Hyperledger Fabric for blockchain networks’’, 2018, https://developer.ibm.com/articles/top-technical-advantages-of-Hyperledger-fabric-for-blockchain-networks/, erişim 09.06.2022.

T.C. Savunma Sanayii Başkanlığı, https://www.ssb.gov.tr/WebSite/contentlist.aspx?PageID=1083&LangID=1, erişim 03.06.2022.

T.C. Strateji ve Bütçe Başkanlığı, ‘‘2022 Yıllık Programı’’, s.371, https://www.sbb.gov.tr/wp-content/uploads/2021/10/2022-Yili-Cumhurbaskanligi-Yillik-Programi-26102021.pdf, erişim 07.06.2022.

USLU Sinan, ‘‘Türk ordusunun yeni "kuvveti" siber savunma’’, https://www.aa.com.tr/tr/turkiye/turk-ordusunun-yeni-kuvveti-siber-savunma/584061, erişim 01.06.2022.