Journal of Quantum Technologies and Informatics Research
JQTAIR

KUANTUM TEKNOLOJİLERİ VE ENFORMATİK ARAŞTIRMALARI
Volume / Cilt: 2, Issue / Sayı: 1, 2024, pp. 1-13
E - ISSN: 3023-4735
URL: https://journals.gen.tr/index.php/jqtair/
DOI: https://doi.org/10.70447/ktve.2339

Received / Geliş: 22.01.2024
Acccepted / Kabul: 04.03.2024

RESEARCH ARTICLE / ARAŞTIRMA MAKALESİ

Kolektif Siber Güvenliğin Önemi ve Türk Devletler Teşkilatı

The Importance of Collective Cybersecurity and the Organization of Turkic States

Cengiz Çalıkoğlu

Bilgi Üniversitesi, Türkiye, e-mail: ccalikoglu@hotmail.com

Öz

Dijitalleşen dünyada siber güvenliğin önemi her geçen gün artmaktadır. Bu bağlamda ülkeler ve topluluklar, konuyla ilgili gerekli yatırımları yapmakta, önlemler almaya çalışmakta, ulusal ve uluslararası düzeyde siber saldırılarla mücadele etmektedir. Bu çalışmada siber güvenlik, siber saldırılar, ortak siber güvenlik yapıları ve son yıllarda dünyada gerçekleşen siber saldırılarla ilgili bilgiler sunulmuştur. Ayrıca, Türk Devletleri Teşkilatına üye ülkelerin "Kolektif Siber Savunma Gücü" adı ile ortak siber savunma gücü oluşturulması konusunda önerilere de yer verilmiştir. Bu çalışma, devletler, araştırmacılar, bilim insanları ve bu alana ilgi duyan kişiler için önemli bilgiler içermekte ve bundan sonra yapılacak çalışmalara kaynak oluşturmaktadır.

Anahtar Kelimeler: Siber Güvenlik, Siber Savunma, Siber Tehditler, Türk Devletleri Teşkilatı, Kolektif Siber Savunma Gücü, TDT- Kolektif Siber Savunma Gücü, TDT- KSSG

Abstract

In the digitalized world, the significance of cybersecurity is progressively increasing. In this context, countries and communities are making necessary investments, attempting to take precautions, and collaborating to combat both national and international cyberattacks. This paper provides information on cybersecurity, cyberattacks, collaborative cybersecurity frameworks, and recent cyberattacks worldwide. Additionally, recommendations are made regarding the establishment of a joint cyber defense force under the name "Collective Cyber Defense Force" for member countries of the Turkic Council. This study contains valuable information for governments, researchers, scholars, and individuals interested in this field, serving as a resource for future research endeavors.

Keywords: Cybersecurity, Cyber Defense, Cyber Attacks, Organization of Turkic States, Collective Cyber Defense Force, OTS- Collective Cyber Security Force, OTS- CCFS

Citation/Atıf: ÇALIKOĞLU, C. (2024). Kolektif Siber Güvenliğin Önemi ve Türk Devletler Teşkilatı. *Kuantum Teknolojileri ve Enformatik Araştırmaları*. 2(1): 1-13, DOI: 10.70447/ktve.2339

Corresponding Author/ Sorumlu Yazar:
Cengiz Çalıkoğlu
E-mail: ccalikoglu@hotmail.com

GİRİŞ

Günümüzde, hızla dijitalleşen dünya düzeninde siber güvenlik, ulusal ve uluslararası güvenliğin temel bir bileşeni olarak ön plana çıkmaktadır. Siber alan, sadece bireysel kullanıcılar için değil, aynı zamanda devletler ve çok uluslu örgütler için de stratejik bir öneme sahiptir. Türk Devletleri Teşkilatı (TDT) kendi üye devletlerinin siber güvenlik alanında karşılaştığı tehditlere karşı koyma ve bölgesel iş birliğini güçlendirme yönünde önemli adımlar atmaktadır. Bu çalışma, TDT üyesi ülkeler arasında siber güvenlik entegrasyonunun güçlendirilmesi için yenilikçi önerileri ele almakta ve böylece siber tehditlere karşı birlikte mücadele etme kapasitesinin artırılmasını hedeflemektedir. Siber güvenlik, sadece teknolojik bir konu olmanın ötesinde ekonomik, sosyal ve politik boyutlarıyla da derinlemesine incelenmesi gereken bir alandır. Bu bağlamda TDT›nin siber güvenlik stratejisi, bölgesel ve küresel siber tehditlerin doğası ve bu tehditlere karşı alınabilecek tedbirler üzerine yoğunlaşmaktadır. Dijitalleşen dünyada, siber güvenlik entegrasyonu, üye ülkeler arasındaki bilgi paylaşımını, ortak eğitim programlarını, ortak siber tatbikatları, teknolojik iş birliğini ve hukuki düzenlemeleri içermelidir. Bu temeller çerçevesinde ortak siber güvenlik yapısı oluşturulmasıyla birlikte, gelecekteki değişen teknolojilere derin teknoloji odağının olması kritiktir. Bu entegrasyon, aynı zamanda, TDT ülkelerinin siber alanda karşılaştıkları ortak tehditlere karşı koymada daha etkili ve koordineli bir yaklaşım geliştirmelerini sağlayabilir.

Ülkeler bir araya gelerek siber saldırılara karşı yeni iş birlikleri gerçekleştirmekte veya ülkeler tarafından kurulmuş Kuzey Atlantik Anlaşma Teşkilatı (The North Atlantic Treaty Organization-NATO), Avrupa Birliği (AB) gibi organizasyonlarda siber güvenlik bölümleri oluşturmuşlardır. Bu çalışmada önerilen yapı vasıtasıyla TDT üye ülkelerinin mevcut siber güvenlik yapıları, karşılaştıkları zorluklar ve fırsatlar detaylı bir şekilde analiz edilebilecektir. Ayrıca, siber güvenlik politikalarının oluşturulmasında ve uygulanmasında üye ülkeler arasında daha iyi bir uyum ve koordinasyon sağlamayı hedeflemektedir. Etkili bir siber güvenlik entegrasyonu için, teknik kapasite geliştirme, ortak risk değerlendirme yöntemleri ve acil durum müdahale ekiplerinin oluşturulması gibi unsurların üzerinde durulmuştur.

TDT ülkeleri arasında "Kolektif Siber Savunma Gücü" adı ile bir yapı oluşturulması önerilmiştir. Kolektif Siber Savunma Gücü siber güvenlik konusunda birlikte çalışarak, TDT ülkelerinin siber alanda daha dirençli ve hazırlıklı olmalarını sağlamayı amaçlamaktadır. Siber tehditlerin ulusal sınırları aşan doğası göz önünde bulundurulduğunda, bu tür bir entegrasyonun, bölgesel ve küresel düzeyde siber güvenliği artırıcı etkisi olacağı düşünülmektedir. Bu makale, TDT ülkelerinin siber güvenlik alanında karşılaştıkları mevcut zorlukları tartışacak ve yenilikçi bir entegrasyon modeli önererek, bu zorlukların üstesinden gelmelerine yardımcı olacak stratejiler sunmaktadır.

SİBER GÜVENLİK, SİBER SALDIRILAR VE JEOPOLİTİK OLAYLAR

Siber güvenlik, elektronik ağlar ve sistemler üzerinden bireyler ve kuruluşlar arasında paylaşılan hassas ve gizli verileri korumak için benimsenen bir dizi önlem ve uygulama (Türk Dil Kurumu, 2024) olarak ifade edilebilir. Bilgilerin güvenli bir şekilde iletilmesini ve depolanmasını sağlamanın yanı sıra verilere yetkisiz erişim, kullanım, değişiklik veya imhanın önlenmesini içerir. Siber güvenliğin birincil amacı veri, yazılım ve donanım gibi dijital varlıkların bütünlüğünü, kullanılabilirliğini ve gizliliğini potansiyel siber tehditlere ve saldırılara karşı korumaktır.

Siber saldırı ise bir veya birden fazla bilgisayar sistemlerine veya ağlarına yetkisiz erişim sağlamak için saldırganlar tarafından gerçekleştirilen bir dizi kötü niyetli faaliyet (Türk Dil Kurumu, 2024) olarak açıklanabilir. Bu saldırılar verilerin çalınması, değiştirilmesi veya imha edilmesi gibi farklı şekillerde olabilir. Saldırganlar, hedef sistemdeki açıklardan faydalanmak ve kendi çıkarları için kullanabilecekleri hassas bilgilere erişim sağlamak için çeşitli teknikler kullanırlar. Siber saldırılar bireyler, işletmeler ve hükümetler için ciddi bir tehdit oluşturmaktadır ve bunlara karşı korunmak için önleyici tedbirler almak çok

önemlidir.

Siber güvenlikle ilgili literatüre baktığımızda her geçen gün bu konuda yapılan akademik çalışmaların arttığı görülmektedir. Son zamanda yapılan çalışmalara (Gündüz & Daş, 2022; Nezgitli & Benzer, 2020; Karasoy & Babaoğlu, 2021; Kurnaz & Önen, 2019; Altın, 2023; Köker, 2022; Atakan, 2021; Kişman & Güleç, 2021; Eldem, 2021; Paltacı, 2022) (Ada & Çakır, 2017; Acar & Pekcandanoğlu, 2020; Göçoğlu & Aydın, 2019; Renda, 2022; Gündoğdu, 2023; Yılmaz, 2018; Dolma, 2023; Çıtak, 2021; Güntay, 2018; Ünal, Kanat, & Gürkaynak, 2023) örnek gösterilebilir.

Bu çalışmada, koşullar, durumlar ve özelliklerin ortaya koyulması, mevcut olayların daha önceki benzer olay ve koşullarla ilişkileri dikkate alınarak açıklanmasını hedefleyen (Kaptan, 1991) betimleme yöntemi kullanılmıştır.

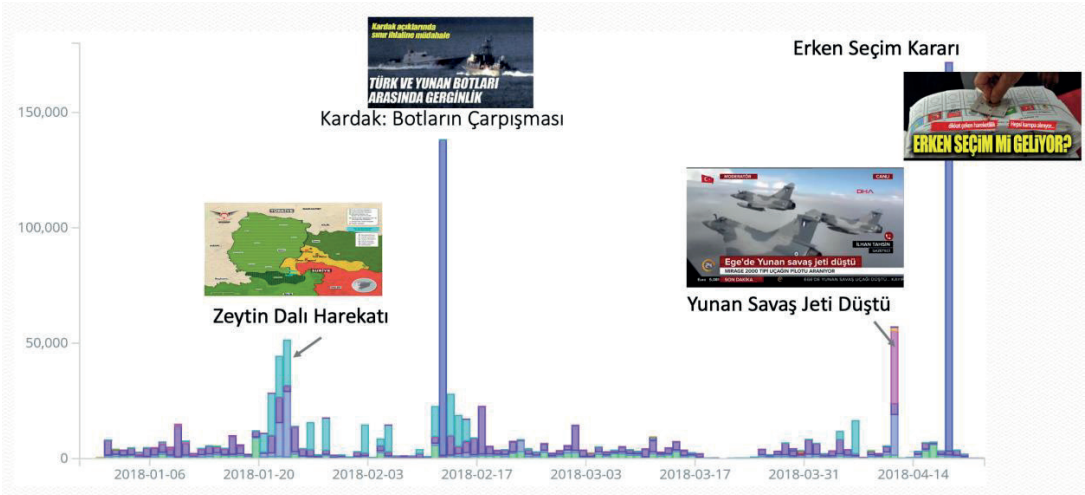
Siber saldırılar ülkelerin altyapılarını etkilemekte ve bu saldırılar genel olarak askeri, finansal ve kritik altyapılar olarak üç başlıkta ele alınabilir. Enerji üretim ve dağıtım, su ve gaz dağıtım altyapıları genel yapılara örnek gösterilebilirken, askeri komuta kontrol ve iletişim sistemler askeri yapılarak örnek gösterilebilir. Havalimanları, bankacılık ve ödeme sitemleri, Telekom ve iletişim altyapıları ise finansal altyapılara örnek gösterilebilir.

Jeopolitik olayların olduğu ülkelerdeki olaylar ile siber hareketlilikler arasında bir korelasyon olduğu söylenebilir. Siber saldırıların durumlarıyla ilgili bazı veriler Şekil 1-3 de sunulmuştur.

Jeopolitik olaylar ve siber saldırılar arasında bir korelasyon olduğu söylenebilir. Türkiye 20 Ocak 2018 tarihinde Zeytin Dalı Harekâtı (Milli Savunma Bakanlığı, 2018) gerçekleştirmiştir. Şekil 1. de görüldüğü üzere 6 Ocak 2018 tarihinde siber saldırılar 50.000'nin altındayken, Zeytin dalı harekatının başladığı 20 Ocak 2018 tarihinde siber hareketlilik günlük olarak 50.000'nin üzerine çıktığı görülmektedir. Türkiye Cumhurbaşkanı ve 57. dönem milletvekilliği seçimi 2018 yılında yapılmıştır (Yüksek Seçim Kurumu, 2019). Yine şekil 1 de görüldüğü üzere seçimler öncesinde Türkiye ile ilgili siber hareketlilik 50.000'nin altıdayken, seçimlerle ilgili haberlerle birlikte 14 Nisan 2018 tarihinde Türkiye ile ilgili siber hareketlilik günlük 150.000'nin üzerine çıkmıştır. Bu ve benzeri örneklerden yola çıkarak jeopolitik olayların başladığı zamanlarda siber hareketliliklerin arttığı görülmektedir.

Jeopolitik Olaylar ile Siber Hareketlilik arasında korelasyon bağı olduğunu gösteren ikinci bir örnek Şekil 2 de sunulmuştur. Türkiye'nin zeytin dalı operasyonuna devamı olarak, Afrin operasyonu süresince de siber hareketliliğin artarak devam ettiği görülmektedir. Suriye'de savaş ve operasyonlar sürecinde Amerika Birleşik Devletleri (ABD) başkanı Donalt Trump "hazır ol Rusya, füzelere gelecek" başlıklı bir açıklama yapmıştır (NTV , 2018). Bu açıklamayla birlikte şekil 2'de de görüldüğü üzere siber hareketliliğin artığı görülmektedir.

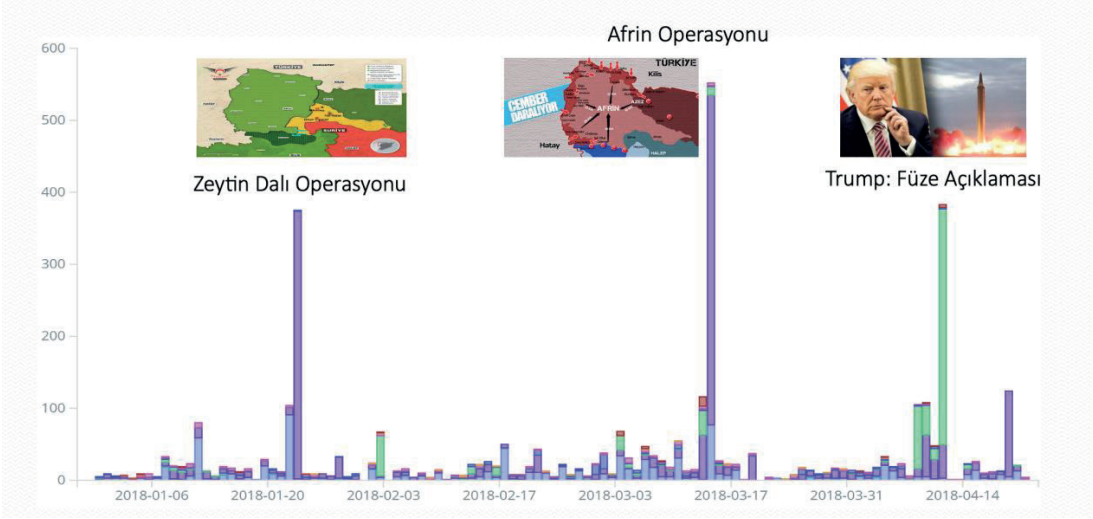
Şekil 1. Jeopolitik Olaylar ve Siber Hareketlilik *(Taş, 2017)*



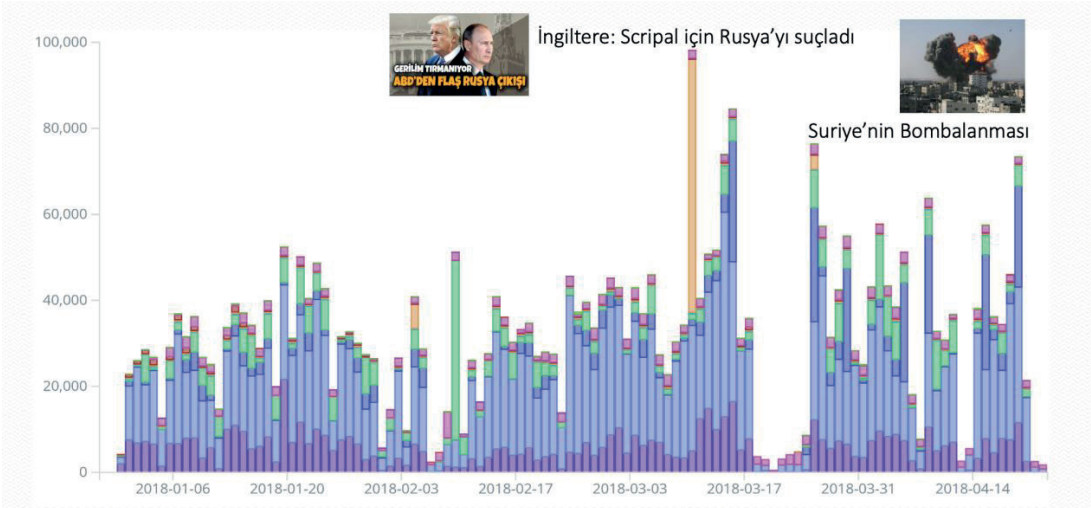
Jeopolitik olaylar ve siber hareketlilikle ilgili olarak son örnek ise Rusya ile İngiltere arasında casus krizi örnek verilebilir. 2018 yılında İngiltere ajan Sergey Skripal'ın Rus yapımı kimyayalar madde ile zehirlendiği iddia etmiştir (Anadolu Ajansı, 2018). Konuyla ilgili Şekil 3- 'te görüldüğü üzere 3 Mart 2018 tarihinde Rusya da siber hareketliliğin 100.000'in üzerine çıktığı görülmektedir. Tablo detaylı olarak incelendiğinde Ocak 2018 de en yüksek siber hareketlilik 55.000 civarındayken, ajan krizi ile birlikte Mart ayında yapılan açıklamalardan sonra siber hareketlilik % 82 artarak 100.000'in üzerine çıkmıştır.

Bu örneklerden yola çıkarak Siber saldırılar ile jeopolitik olaylar arasında karmaşık bir ilişki bulunduğu söylenebilir. Çağdaş dünya düzeninde, siber saldırılar sadece teknik birer ihlal değil, aynı zamanda devletler arası ilişkilerin bir parçası haline gelmiştir. Jeopolitik gerilimler, uluslararası sahnede meydana gelen siber saldırılarda artan bir rol oynamaktadır. Siber saldırıların potansiyel yıkıcılığı, geleneksel savaşlar kadar ciddi sonuçlar doğurmaktadır. Bu saldırılar, devletlerin kritik altyapılarına, askeri sistemlerine ve ekonomik yapılarına yönelik olarak gerçekleştiğinde, uluslararası arenada güç dengelerini etkilemektedir. Güçlü devletler, siber yeteneklerini ulusal güvenlik stratejilerinin bir parçası olarak kullanabilir. Bu devletler, casusluk, bilgi çalma ve diğer siber operasyonları yürüterek ulusal çıkarlarını koruma amacını taşıyabilir. Bazı durumlarda ise birden fazla devlet, ortak hareket ederek karmaşık ve

Şekil 2. Jeopolitik Olaylar ve Siber Hareketlilik *(Taş, 2017)*



Şekil 3. Jeopolitik Olaylar ve Siber Hareketlilik *(Taş, 2017)*



sofistike siber saldırılar düzenleyebilirler. Bu durum, uluslararası ilişkilerde yeni bir boyut kazandırarak, siber alanın giderek daha önemli bir stratejik unsura dönüşebilir.

SİBER GÜVENLİK VE İŞ BİRLİĞİ

Siber güvenlik kişilerin, firmaların, kamu kuruluşları ve diğer organizasyonların hassas verilerini, her türlü altyapılarını tehlikelere karşı korumak ve sürdürmek için önemlidir. Bu tehditlere karşı kişiler ve kurumlar tedbirleri almaya çalışırken yetersiz kalabilmektedir. Bu durumda ülke politikalarında ve stratejilerinde siber tehditlere karşı gerekli hukuksal ve teknolojik önlemler alınmaya çalışılmaktadır. Bu çalışmalar ülke bazında bazı durumlarda yeterli olmamakta, ülkeler arasında iş birliğini zorunlu kılmaktadır. Ayrıca, ülkelerin oluşturmuş NATO gibi ortak savunma güçleri içerisinde siber güvenlik konusunda bölümler oluşturulmakta ve iş birliği yapılmaktadır. Siyasi ve ekonomik örgütlenme örgütü olaraktan AB ülkeleri kendi aralarında siber güvenlik yapısıyla ilgili her türlü çalışmaları yapmakta ve gerekli önlemler konusunda iş birliğine gitmektedir. Bu çalışma kapsamında siber güvenlik ve iş birliği ile ilgili NATO ve AB'deki çalışmalara yer verilmiştir.

Avrupa Birliği Siber Güvenlik Ajansı (ENISA)

ENISA, 2004 yılında Yunanistan'ın başkenti Atina'da kurulmuştur. Bu oluşumun temel amacı, Avrupa'nın siber güvenlik kapasitesini güçlendirmektir. Bağımsız bir ajans olarak faaliyet gösteren ENISA, Avrupa Birliği üye devletleri arasında siber güvenlik iş birliğini artırmayı, kabiliyetleri güçlendirmeyi ve dirençli bir siber güvenlik ekosistemi oluşturmayı amaçlamaktadır. Saldırıya uğrayan ülkelere yardım sağlama, üye ülkelerin siber olaylara müdahale ekipleri ile iş birliği yapma ve ulusal kapasitelerin geliştirilmesine destek olma gibi görevlerle hareket eden ENISA, kolektif siber güvenliği artırmak adına bilgi paylaşımı, eğitim, iş birliği ve ortak tatbikatlar düzenlemektedir. Yönetim kurulu üyeleri her AB üye devletinden seçilirken, ajansın bağımsızlığını sağlamak ve görevlerini etkin bir şekilde yerine getirmek için İcra Direktörü tarafından yönetilmektedir. ENISA'nın kuruluşu, Avrupa genelindeki siber güvenlik endişelerine karşı bir yanıt olarak ortaya çıkmış olup, özellikle İngiltere, Almanya, Fransa gibi ülkelerde yaşanan ciddi siber güvenlik saldırılarından alınan derslerle şekillenmiştir (ENISA, 2024).

ENISA, AB ülkelerinde gerçek zamanlı olarak siber saldırı izlemeleri yapmamaktadır. Siber saldırıların anlık olarak izlenmesi ve yönetilmesi her bir AB üyesi devletinin sorumluluğundadır. Diğer taraftan saldırıya uğrayan bir AB üyesi talep etmesi durumunda destek vermektedir. Böylece kolektif siber güvenlik sağlanmakta ve iş birliği yapılmaktadır. ENISA'nın diğer önemli bir faaliyeti ise AB ülkeleri arasında bilgi paylaşımı ve olası siber saldırılarla ilgili tatbikatlar yapmaktır. Bu pratik uygulamalar olası saldırılara karşı ülkeleri hazır ve güvende tutmaktadır. ENISA, karasal olarak bir ordusu olmamasına rağmen, dijital olarak siber uzayda ortak ordu mantığıyla sahip olduğu söylenebilir

NATO Müşterek Siber Savunma Mükemmeliyet Merkezi (CCDCOE)

NATO, 4 Nisan 1949 tarihinde 12 ülke tarafından imzalanan Kuzey Atlantik Anlaşması ile kurulmuştur. 2024 yılı itibariyle bu ittifaka 31 ülke üyedir. NATO'nun amacı, insanları korumak, ortaklıkları geliştirmek, yeni tehditlerle savaşmak, barış ve istikrarı korumak olarak ifade edilebilir (NTV, 2023).

Dünyadaki en önemli ve kapsamlı oluşumlardan biri olan NATO siber güvenlik konusunda da gerekli çalışmaları yaparak Müşterek Siber Savunma Mükemmeliyet Merkezi'ni 14 Mayıs 2008 tarihinde kurmuştur. CCDCOE'nin amacı oldukça geniş kapsamlı ve stratejik bir rolü üstlenmektedir. 2008 yılında Estonya'nın başkenti Tallinn'de kurulan merkez, bilgi güvenliği konusunda NATO ülkelerini koruma ve savunma görevini üstlenmiştir. Merkezin yönetimine "Bilgi Güvenliği Baş Sorumlusu" başkanlık etmekte olup, NATO merkezlerini öncelikli olarak korumak, siber olaylara müdahale etmek ve saldırıları önlemek temel amaçlar arasında yer almaktadır. Ayrıca, üye ülkeler arasında bilgi paylaşımı, iş birliği ve ortak tatbikatlar düzenlemek de merkezin stratejik hedefleri arasında bulunmaktadır. Bu kapsamda, 2016 yılında Belçika'nın Mons şehrinde Siber Uzay Operasyon Merkezi'nin kurulması,

NATO'nun siber savunma kapasitelerini güçlendirmeye yönelik bir adım olarak öne çıkmaktadır. NATO CCDCOE, siber güvenlik alanında müttefikler arasında koordinasyonu ve dayanışmayı sağlayarak, siber tehditlere karşı etkili bir savunma mekanizması oluşturmayı amaçlamaktadır (CCDCOE, 2023).

2004 yılında NATO'ya katılan Estonya, bu süreçte ittifaka bir siber savunma merkezi kurulması önerisini ortaya atmıştır. Ancak, 2007 yılında Estonya'ya yönelik siyasi amaçlı ilk siber saldırılar, bölgesel ve uluslararası düzeyde büyük bir endişe yaratmış ve siber güvenlik konusundaki hassasiyeti artırmıştır. Bu olaylar, siber saldırıların sadece teknik bir mesele olmanın ötesinde, siyasi ve stratejik bir boyuta da sahip olduğunu göstermiştir (Dilek & Talih, 2023). Bu deneyimler, siber güvenlik konusundaki stratejik yaklaşımların geliştirilmesine ve güvenlik tedbirlerinin artırılmasına katkıda bulunmuştur.

CCDCOE tarafından yürütülen faaliyetler, müttefik ülkeler arasında siber güvenliği güçlendirmeyi hedefleyen önemli bir rolü yansıtmaktadır. Merkez, üye ülkelerin gerçek zamanlı izlenmesi sorumluluğunu taşımaz ve bu görevleri üye devletlere bırakır. Ancak, siber tehditlere karşı koordinasyonu sağlamak ve kolektif savunma çabalarını desteklemek amacıyla kolaylaştırıcı bir rol üstlenir. Merkez, üye devletlerin talepleri doğrultusunda yardım sağlama ve siber savunma kapasitelerini güçlendirmek üzere iş birliği yapma yeteneğine sahiptir. Bilgi paylaşımı, iş birliği ve ortak tatbikatlar düzenleme konusundaki faaliyetleri ile CCDCOE, müttefik ülkeler arasında siber güvenlik konusunda bilinçlenmeyi artırmak ve etkili bir kolektif savunma mekanizması oluşturmak adına önemli bir rol oynamaktadır (CCDCOE, 2023).

CCDOCOE ve ENISA amaç ve hedefleri olaraktan bir birilerine benzemekte ve dijitalleşen dünyada siber güvenlik konusunda örnek olabilecek çalışmalar, mevzuatlar, geleceğe yönelik olaraktan çalışmalar yaptığı görülmektedir.

TÜRK DEVLETLERİ TEŞKİLATI KOLEKTİF SİBER SAVUNMA GÜCÜ

Türk Devletleri Teşkilatı ve Siber Güvenlik

Türk Devletleri Teşkilatı, Türk Devletleri arasında kapsamlı iş birliğini teşvik etmek için uluslararası bir örgüt olarak 2009 yılında kurulmuştur. Teşkilatın kurucu üyeleri Azerbaycan, Kazakistan, Kırgızistan ve Türkiye`dir. Ekim 2019'da Bakü'de gerçekleştirilen 7. Zirve sırasında Özbekistan Teşkilata tam üye olarak katılmıştır. Macaristan ise Eylül 2018'de Kırgızistan'ın Cholpon-Ata şehrinde düzenlenen 6. Zirve sırasında, Türkmenistan Kasım 2021'de İstanbul'da düzenlenen 8. Zirvede, Kuzey Kıbrıs Türk Cumhuriyeti Semerkant'ta düzenlenen 9. Zirvede ve Ekonomik İş birliği Teşkilatı (EİT) 2023 yılında Astana'da düzenlenen 10. Zirve sırasında Teşkilat nezdinde gözlemci statüsü kazanmıştır. Nahcivan Anlaşmanın önsözünde üye devletler, Birleşmiş Milletler Anlaşması'nın amaç ve ilkelerine bağlılıklarını teyit ederek, TDT'nin genel amacını, Türk Devletleri arasında kapsamlı iş birliğini derinleştirmek, bölgesel ve küresel barış ile istikrara katkıda bulunmak olarak tanımlamışlardır. Üye ülkeler ayrıca, demokrasi, insan haklarına saygı, hukukun üstünlüğü ve iyi yönetişim gibi temel ilkelere bağlılıklarını ifade etmişlerdir. TDT kapsamındaki iş birliği, üye ülkeler arasındaki ortak tarih, kültür, kimlik ve Türk dili konuşan halkların dil birliğinden kaynaklanan özel dayanışma temelinde inşa edilmektedir (Türk Devletleri Teşkilatı, 2024). 2024 Ocak ayı itibariyle TDT asıl ve gözlemci üye ülkeler Şekil 4'te sunulmuştur.

Dijitalleşen dünyamızda siber güvenlik tanım, kavram ve konuya bakış açıları kökten değişmiş, siber tehdit ve saldırılar bireysellikten devletler arası düzeye çıkmıştır. Uzaydaki siber güç dengeleri, güvenlik stratejilerini ve ulusal kabiliyetlerin geliştirilmesini zorunlu kılmaktadır. Günümüzde ülkelerin fiziksel sınırlarını korumak kadar, ülkenin verisini ve dijital altyapısını korumak kaçınılmaz olmuştur. Siber güvenlik, devlet güvenliğiyle eşdeğer öneme sahip bir konu haline gelmiştir.

Bu çalışmanın ilgili bölümünde dünyada yaşananlar, jeopolitik olaylarla, siber olaylar arasında korelasyon olduğu verilerle detaylı

bir şekilde açıklanmıştır. Dünyada ortak siber güvenlik yapıları olarak ENISA ve CCDCOE'nin ortak siber güvenlik yapıları detaylı incelenmiştir. Bu bölümde de belirtildiği üzere AB'de de NATO'da da bazı ülkeler siber güvenlik saldırılarına maruz kalmış ve bu saldırılar ENISA ve CCDCOE kuruluşunu hızlandırmıştır. Bu iki organizasyonun ortak siber güvenlik yapılarında ortak amaç üye devletleri arasında siber güvenlik iş birliğini artırmayı, kabiliyetleri güçlendirmeyi ve dirençli bir siber güvenlik ekosistemi oluşturmayı amaçlamışlardır. Yine saldırıya uğrayan ülkelere yardım sağlama, üye ülkelerin siber olaylara müdahale ekipleri ile iş birliği yapma ve ulusal kapasitelerin geliştirilmesine destek olma gibi görevlerle hareket etmekteler ve kolektif siber güvenliği artırmak adına bilgi paylaşımı, eğitim, iş birliği ve ortak tatbikatlar düzenlemektedirler.

Dünyada artan siber hareketlilik konusunda Türkiye'ye yönelik olaraktan önemli siber olayların yaşandığı görülmüştür. Bu saldırılardan banklalar, Telekomünikasyon şirketleri, sektör bazı şirketler etkilenmiştir (TRT Haber, 2019), (BBC News Türkçe, 2015). Benzer şekilde TDT üye ülkelere yönelik siber olayların olduğu geçmiş yıllarda gözlenmiştir. TDT üye ülkelere yönelik birçok siber saldırılırsa bilinse de uluslararası yayınlara düşen şu örnekleri verebiliriz (The Hacker News, 2012; The Hacker News, 2012; The Hacker News, 2023; The Hacker News, 2012; The Hacker News, 2012; The Hacker News, 2023; The Hacker News, 2022; The Hacker News, 2019).

Tüm bu gelişmeleri dikkate aldığımızda, dijitalleşen ve kutuplaşan dünyada bireysellikten devletler arası düzeye çıkan siber güvenlikte Türk Devletleri Teşkilatı üye devletler olarak ortak hareket etmek bir zorunluluk ve çok kritik bir stratejik iş birliği gereksinimi ortaya çıkmıştır. Ayrıca, TDT üye devletlerine genel olarak bakıldığında bazı devletlerin teknolojik altyapı, insan kaynağı, mevzuat ve siber güvenlik altyapılarının iyileştirilmesinin kaçınılmaz olduğu söylenebilir. Türk dünyasının büyük düşünürü İsmail Gaspıralı bundan yaklaşık 110

Şekil 4. TDT üye ve gözlemci devletler

yıl önce «Dilde, işte, fikirde birlik» sözleriyle tüm Türk halklarını birlik ve dayanışmaya çağırmıştır. Türk topluluklarının gelişmesi için yol çizen, basın ve eğitim çalışmalarıyla iz bırakan Kırım Tatar Türk'ü İsmail Gaspıralı fikirleriyle Türk dünyasını etkilemeye devam etmektedir (Anadolu Ajansı, 2020).

Geçen 110 yılda dünyamızda çok büyük değişimler olmuş, sanayi devrimi, gelişen teknolojiler, Endüstri 4.0 ile dijitalleşen altyapıları, siber uzaydaki gelişmeler ve önümüzdeki yıllar yapay zekâ destekli siber saldırıları düşündüğümüzde "teknoloji ve siber güvenlik" her şeyin merkezinde olacağı söylenebilir. Bu bakışla Türk düşünürü İsmail Gaspıralı'nın sözüne atıfla "Dilde, fikirde, işte, **teknolojide** ve **güvenlikte** birlik" için iş birliği ve ortak çalışmalar yapılabilir. "Birlikte daha güvendeyiz" bakışıyla bu yapının kurulmasının Türk dünyası için tarihi bir sorumluluk olduğunu düşünülebilir. Bu kapsamda TDT üye devletleri için «TDT Kolektif Siber Güvenlik Gücü» kurulması önerilmektedir.

TDT Kolektif Siber Güvenlik Gücünün Gerekliliği

TDT üye ülkeler arasında ulusal güvenliğin ve kritik yapıların korunması, ulusal siber güvenlik olgunluk seviyesinin güçlendirilmesi, ulusal güvenlik politika ve stratejilerinin desteklenmesi, devletler, kurumlar ve sektörler arasında köprüler kurulması, uluslararası iş birliğinin teşvik edilmesi ve kapasite geliştirme konusunda iş birliği yapılması kaçınılmazdır.

TDT üye devletleri arasında siber güvenlik iş birliğini artırmak, kabiliyetleri güçlendirmek, güçlü bir siber güvenlik ekosistemi oluşturmak önem arz etmektedir. TDT üye ülkelerimizden birine olası siber saldırı olduğunda yardım sağlamak, üye ülkelerin siber olaylara müdahale ekipleri ile iş birliği yapmak ve ulusal kapasitelerin geliştirilmesine destek olmanın yanında kolektif siber güvenliği artırmak adına bilgi paylaşımı, eğitim, iş birliği ve ortak tatbikatlar düzenlenmesi ülkelerimizi siber saldırılarının korumanın yanında daha güvende hissettirecektir.

TDT Kolektif Siber Güvenlik Gücünün Amacı ve Hedefi

İstihbarat paylaşımı, kolektif hareket, önleme, zarar toplama, etkin caydırmayı amaçlayan TDT Kolektif Siber Güvenlik Gücünün hedeflerini kısaca aşağıda özetlenebilir:

- Gizliliği korumak ve teşvik etmek,
- Kapasite geliştirme konusunda iş birliği yapmak,
- Uluslararası kuruluşlar ve kilit oyuncular/ ortaklar ile stratejik ortaklıklar kurmak,
- Ulusal siber güvenlik olgunluk seviyesinin güçlendirilmesi için ilgili ulusal politikaların, stratejilerin oluşturulmasını desteklemek,
- Kamu sektörü, özel sektör, akademik kurumlar arasında köprüler kurmak,
- Belirli siber istişareler için ikili veya ortak komisyonlar oluşturmak,
- Eğitim & ARGE faaliyetleri ile sürekli iyileştirmelerde bulunmak,
- Ekosisteme özgü zorlukları periyodik olarak ele almak,
- En iyi uygulamaları geliştirmek ve teşvik etmek.

TDT Kolektif Siber Güvenlik Gücünün Organizasyon Yapısı:

Bir oluşumun başarılı olabilmesi için; planlama, örgütlenme, yönetme, denetim gibi unsurları yürüten yönetim organizasyon yapısının oluşturulması son derece önemlidir. Bu kapsamda TDT Kolektif Siber Güvenlik Gücünün ilk oluşumu aşamasında yönetim komitesi ve alt komiteler Şekil 5 ve 6 da sunulmuştur.

Şekil 5'te görüldüğü üzere TDT Kolektif Siber Güvenlik Gücü iş sürekliliği ve kriz yönetim, yasal ve uyum, teknoloji ve inovasyon, bilgi güvenliği ve yönetim komitesi olmak üzere dört komiteden oluşması önerilmektedir. Gelişen teknolojiler ve günün ihtiyaçlarına göre yönetim komitesinin sayısı artırılabilir.

Şekil 6'te görüldüğü üzere TDT Kolektif Siber Güvenlik Gücü, İş Sürekliliği ve Kriz Yönetimi, Program Yönetişimi, Operasyonel Model Tasarımı, Eğitim & ARGE, Denetim & Risk & Yasal ve Uyum, Siber Güvenlik Yönetimi Ekibi olmak üzere altı ekipten oluşması önerilmektedir.

TDT Kolektif Siber Güvenlik Gücünün Faaliyet Alanları

TDT Kolektif Siber Güvenlik Gücü, kritik altyapının korunması, ulusal güvenliğin korunması, vatandaşların mahremiyetinin ve verilerinin korunması, ekonomik büyümenin desteklenmesi, uluslararası iş birliğinin teşvik edilmesi gibi konularda faaliyet gösterebilir.

▪ *Kritik altyapının korunması:* Siber güvenlik tehditleri elektrik şebekeleri, ulaşım sistemleri ve finans kurumları gibi kritik altyapılar için önemli bir risk oluşturmaktadır. Kritik altyapıya yönelik bir siber saldırı, temel hizmetleri aksatarak ve yaygın ekonomik hasara yol açarak yıkıcı sonuçlar doğurabilir. Ülkeler ve ittifak güçleri siber güvenlik yapıları kurarak kritik altyapılarını siber saldırılardan koruyabilir ve temel hizmetlerin devamlılığını sağlayabilirler.

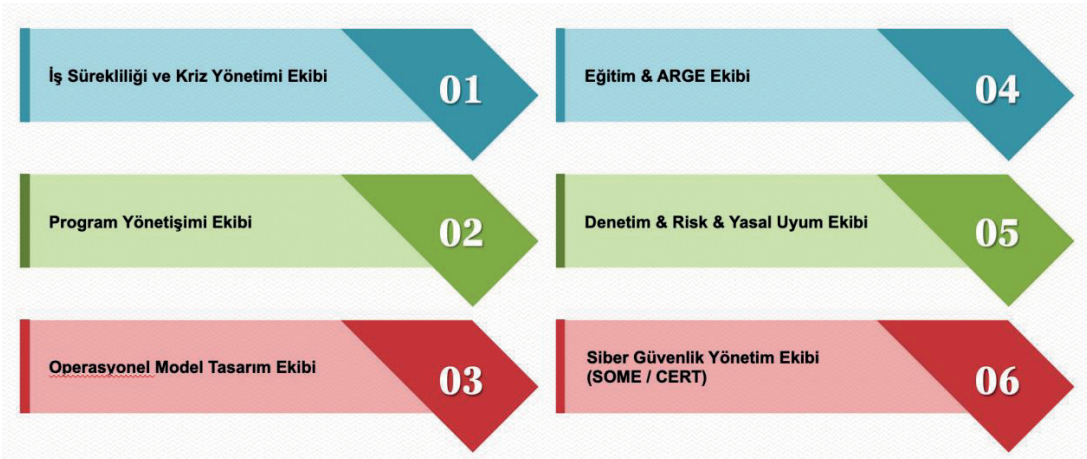
▪ *Ulusal güvenliğin korunması:* Siber saldırılar hassas bilgileri çalmak, askeri operasyonları sekteye uğratmak ve hatta halk arasında nifak tohumları ekmek için kullanılabilir. Ülkeler ve ittifak güçleri siber güvenlik yapıları kurarak ulusal güvenliklerini siber saldırılara karşı koruyabilir ve düşmanlarına karşı stratejik bir avantaj sağlayabilirler.

▪ *Vatandaşların mahremiyetinin ve verilerinin korunması:* Siber suçlular, kişisel bilgileri ve finansal verileri çalmak için bireyleri giderek daha fazla hedef almaktadır. Ülkeler ve ittifak güçleri siber güvenlik yapıları kurarak vatandaşlarının gizliliğini ve verilerini siber saldırılardan koruyabilir ve vatandaşlarının çevrimiçi hizmetleri kullanırken kendilerini güvende hissetmelerini sağlayabilir.

▪ *Ekonomik büyümenin desteklenmesi:* Siber güvenlik günümüzün dijital ekonomisinde ekonomik büyüme için vazgeçilmezdir. Her büyüklükteki işletme faaliyetlerini sürdürmek için internete güvenmektedir. Siber saldırılar

Şekil 5. TDT Kolektif Siber Güvenlik Gücü Yönetim Komitesi

Şekil 6. Kolektif Siber Güvenlik Gücü Çalışma Ekipleri



şirketlerin operasyonları aksatabilir, itibara zarar verebilir ve mali kayıplara yol açabilir. Ülkeler ve ittifak güçleri siber güvenlik yapıları kurarak işletmelerin gelişmesi için daha güvenli ve istikrarlı bir ortam yaratabilir. Bu durum ekonomik büyüme ve istihdam yaratılmasına katkı sağlar.

▪ *Uluslararası iş birliğinin teşvik edilmesi:* Siber güvenlik, etkin bir şekilde ele alınması için uluslararası iş birliği gerektiren küresel bir sorundur. Ülkeler ve ittifak güçleri, siber güvenlik yapıları kurarak bilgi paylaşmak, tehdit istihbaratı geliştirmek ve siber saldırılara karşı müdahalelerini koordine etmek için birlikte çalışabilirler. Bu iş birliği genel siber saldırı riskini azaltmaya ve küresel toplumu daha güvenli hale getirmeye yardımcı olabilir.

TDT Kolektif Siber Güvenlik Gücünün Kritik Başarı Faktörleri

TDT Kolektif Siber Güvenlik Gücünün başarı kriterlerini yönetim, mevzuat ve finansal olmak üzere üç başlıkta incelenebilir.

▪ *Yönetim Yapısı:* Önerilen yapının TDT çatısı altında kurulması ve projeye tam destek verilmesi, siber güvenlik stratejisinin başarılı bir şekilde uygulanması açısından kritik bir rol oynar. Bu destek, projenin sürdürülebilirliğini sağlamak, hedeflere ulaşmak ve ulusal siber güvenlik kapasitesini güçlendirmek adına önemlidir. Sahiplik olmadan, her bir kurumun kendi önceliklerine odaklanması, projenin bütünlüğünü ve etkisini azaltabilir. Önerilen yapının başkanının, belirlenen komitelerden seçilen uzman bir ekip olması, projenin yönetiminde etkinlik ve odaklanma sağlayacaktır. Özellikle Yönetim Komitesinde, bu yapının baş yöneticisinin ve her ülkeyi temsilen sabit üyelerin olması önem arz etmektedir. Yine kurucu ekibin hedeflenen kurulum süresi boyunca sabit kalması projenin başarısı açısında önemli olacaktır. Bu komitelerde yer alacak üyelerin tek görevlerinin siber güvenlik işine odaklanması, uzmanlık ve derinlemesine bilgi sağlayarak projenin başarısına katkıda bulunacaktır. Bu sayede, hızla evrilen siber tehditlere karşı etkili bir mücadele stratejisi oluşturmak mümkün olacaktır. Projenin başarılı olabilmesi için sadık siber güvenlik uzmanlarının yetiştirilmesi ve korunması önemlidir. Bu uzmanlar, projenin teknik gereksinimlerini karşılamak ve güvenlik önlemlerini güncel tutmak adına kritik bir rol oynarlar. Ayrıca, personel sirkülasyonlarına karşı alternatif çözümler belirlenmesi, bilgi birikiminin korunmasını sağlayarak projenin uzun vadeli etkinliğini artırabilir.

▪ *Ülke Mevzuatları:* Önerilen yapının başarılı bir şekilde kurulabilmesi için, ülkeler arasındaki siber güvenlik mevzuatlarının uyumlu hale getirilmesi kritik bir öneme sahiptir. Bu uyum, siber güvenlikle ilgili iş birliğini güçlendirmek, veri koruma standartlarını belirlemek ve projenin etkili bir şekilde yönetilmesini sağlamak için gereklidir. Ayrıca, genel veri koruma yönetmeliği (General Data Protection Regulation- GDPR) gibi mevzuatlar göz önünde bulundurularak toplanacak veriye dair eksiksiz ve hatasız bir mevzuat oluşturulmalıdır. Bu mevzuat, kullanıcıların gizliliğini koruma, veri güvenliğini sağlama ve siber saldırılara karşı koruma sağlamak üzere tasarlanmalıdır. Önerilen yapının amacına uygun olarak işlevselliğini yerine getirebilmesi için, ülkeler arasında siber istihbarat amaçlı veri paylaşımı büyük bir önem taşır. Bu, hızlı ve etkili bir şekilde siber tehditlere karşı mücadele edebilmek adına kritiktir. Bu bağlamda, ülke ülke siber istihbarat verilerinin paylaşılabilmesi için mevzuat düzenlemelerinin yapılması ve değişikliklerin devlet nezdinde desteklenmesi gerekmektedir. Veri paylaşımını destekleyen bir mevzuat çerçevesi, siber güvenlikle ilgili bilgilerin güvenli bir şekilde paylaşılmasını sağlayarak projenin etkinliğini artırabilir ve ülkeler arası iş birliğini güçlendirebilir. Bu noktada, siber güvenlik mevzuatının oluşturulması ve düzenlenmesi sürecinde paydaşların, uzmanların ve sivil toplum kuruluşlarının katılımı önemlidir. Şeffaf, güçlü ve katılımcı bir süreç, mevzuatın etkili bir şekilde uygulanmasını ve siber güvenlik alanında başarılı bir yapı oluşturulmasını destekleyecektir.

▪ *Bütçe Oluşturulması:* Önerilen yapının kurulması için, gerekli bileşenlerin alınması, ortamların kurulması, yönetilmesi, maliyetlerin karşılanması, kaynakların temin edilmesi ve belirlenen şartların yerine getirilmesi için yatırım mekanizmasının oluşturulması gerekmektedir.

SONUÇ VE DEĞERLENDİRME

TDT Kolektif Siber Güvenlik Gücünün kuruluşu, günümüzde karşılaşılan karmaşık ve artan siber tehditlerle başa çıkabilmek ve ulusal güvenliği sağlamak adına ülkeler arasında güçlü bir iş birliği ve koordinasyonun gerekliliğini vurgulamaktadır. Bu ortak yapı, siber tehditlere etkin bir şekilde karşı koymayı amaçlayarak bilgi paylaşımını artırır ve ortak savunma stratejileri geliştirir. Koordineli bir şekilde hareket etmek, siber saldırılara hızlı ve etkili yanıtlar verme kapasitesini artırır. Bu yapı, ülkelerin siber güvenlik kapasitelerini güçlendirerek, ulusal sistemlerini daha dirençli hale getirmeyi hedefler.

TDT Kolektif Siber Güvenlik Gücünün kurulmasıyla birlikte, üye ülkeler arasında siber güvenlik konusunda iş birliği ve koordinasyonun güçlenmesi, bölgesel ve küresel düzeyde güvenliği artırır. Ayrıca, ortak bir siber güvenlik politikası oluşturarak uyum ve standartlar bütünlüğünü sağlar. Bilgi ve deneyim paylaşımının artması, ülkelerin siber tehditlere karşı daha hazır ve bilgili olmalarını sağlar. Ortak tehditlere karşı kolektif önlemler alabilme yeteneği, üye ülkelerin daha etkili bir şekilde güvenliklerini sağlamalarına olanak tanır. Bu yapı aynı zamanda dijital ekonominin gelişimine destek olacak standartların belirlenmesine katkı sağlar, bireylerin ve kurumların dijital verilerinin güvenliği ve gizliliği korunur.

Uluslararası Siber Güvenlik Yapılarına katılmamanın beraberinde getirdiği riskler, modern dünyanın karmaşık siber tehdit ortamında bir ülkeyi önemli zorluklarla karşı karşıya bırakabilir. Savunma zayıflığı, ulusal bilgi ve veri güvenliğini tehdit edebilir, ekonomik ilişkileri ve dış politika stratejilerini olumsuz etkileyebilir. Ayrıca, gelişen siber tehditlere hazırlıksız olma olasılığı artar ve ülkeyi beklenmedik siber saldırılara karşı savunmasız bırakabilir. Bu bağlamda, uluslararası siber güvenlik yapılarına katılmak, bir ülkenin siber güvenlik kapasitesini artırarak, küresel düzeyde daha güvenli ve dirençli bir dijital ortam oluşturmasına katkı sağlayabilir.

TDT Kolektif Siber Güvenlik Gücünün kuruluşu, kutuplaşan dünya düzeni, artan siber saldırılar, uzaydaki değişen siber güç dengeleri gibi faktörlerle şekillenen modern dünyanın gerçeklerine uygun olarak ortak bir siber güvenlik teşkilatı kurma ihtiyacını vurgular. Bu oluşum, üye ülkeler arasında güç birliği oluşturarak siber tehditlere karşı etkili bir savunma sağlamayı amaçlar. Aynı zamanda, bireysellikten devletler arası düzeye çıkan siber tehditlerle başa çıkabilmek adına ulusal güvenlik stratejilerini ve kabiliyetlerini revize etmeyi hedefler.

TDT Kolektif Siber Güvenlik Gücünün kuruluşuyla birlikte üye ülkeler, ortak bir siber güvenlik teşkilatının avantajlarından faydalanarak siber tehditlere etkili bir mücadele verme kapasitesini artırır. Bu çaba, ülkeler arasında güç birliği, caydırıcılık, siber tehditlere ortak müdahale, istihbarat paylaşımı, kolektif hareket, önleme ve toparlama stratejilerinin birlikte oluşturulması gibi hedefleri içerir. Bu sayede, ülkelerin verileri ve dijital altyapıları daha güvenli bir şekilde korunurken, bölgesel dayanışma ve siber güvenlikte liderlik güçlenir.

TDT Kolektif Siber Güvenlik Gücünün kuruluşu, üye ülkeler için sağlayacağı katma değerli hizmetlerle dijital güvenliğin güçlendirilmesine yönelik kapsamlı bir strateji sunar. Ortak siber savunma gücü oluşturulması, TDT üye ülkelerini siber tehditlere karşı güç birliği içinde ortak müdahale etme imkanıyla donatır. Bu yapı, siber saldırılardan korunmak adına kapsamlı bir ekosistem oluşturulmasına katkı sağlar. Aynı zamanda, olası finansal kayıpların engellenmesi amacıyla zamanında siber saldırıları fark etme ve önleme yetenekleri güçlendirilir.

Bilgi ve altyapı eşitlenmesi, TDT üye ülkelerinin kendi içlerindeki siber güvenlik açıklarını merkezi bir düzeyde koruma altına almasını sağlar. Bu sayede, ülkeler siber saldırı sonrasında en az hasarla toparlanma yeteneklerini artırır ve dijital güvenliklerini daha etkin bir şekilde yönetir. Ayrıca, teknoloji ve güvenlik altyapılarında standardizasyon sağlanarak ülkeler arasında siber güvenlikte bir uyum ve iş birliği ortamı oluşturulur.

TDT Kolektif Siber Güvenlik Gücünün kuruluşu, sadece TDT üye ülkelerine değil, tüm dünyada siber saldırılara karşı etkili önlemler

alınmasına katkı sağlayacak ve dijital güvenliği güçlendirecektir. Bu yapı, bölgesel güvenliği artırmanın yanı sıra benzer siber güvenlik oluşumlarına örnek teşkil edebilir. Bölgesel güvenlik için sağladığı avantajlar, TDT'nin dijital dünyadaki liderliğini pekiştirir ve küresel düzeyde siber güvenliği artırmaya yönelik bir çabanın önemli bir parçası olur.

Yukarıda belirtilen unsurların hepsi bir araya geldiğinde, TDT Kolektif Siber Güvenlik Gücünün kurulması, üye ülkelerin siber güvenlik kapasitelerini güçlendirerek, siber tehditlere karşı daha etkin bir savunma mekanizması oluşturmayı amaçlamaktadır. Bu çabaların sonucunda, dijital dünya daha güvenli bir geleceğe doğru adım atmayı hedeflemekte ve ulusal güvenliği güçlendirmektedir.

Kaynakça

Çıtak, E. (2021). Siber Terörizm: Potansiyelin Gerçekçi Tehdidi. *Turkuaz Uluslararası Sosyo-Ekonomik Stratejik Araştırmalar Dergisi*, , Cilt 3, Sayı 1, Sayfalar 1 - 16.

Acar, H., & Pekcandanoğlu, M. (2020). Rusya'nın Siber Güvenlik ve Siber Espiyonaj Politikalarının Analizi. *Türkiye Rusya Araştırmaları Dergisi*, , Sayı 3, Sayfalar 167 - 189.

Ada, M., & Çakır, H. (2017). Kuzey Atlantik Antlaşma Örgütü'nün (NATO) Siber Güvenlik Stratejisinin İncelenmesi. *Düzce Üniversitesi Bilim ve Teknoloji Dergisi*, Cilt 5, Sayı 2, Sayfalar 632 - 656.

Ajansı, A. (2020, 09 24). *Türk dünyasının büyük düşünce adamı: Gaspıralı İsmail*. Ocak 2024 tarihinde https://www.aa.com.tr/tr/portre/turk-dunyasinin-buyuk-dusunce-adami-gaspirali-ismail/1982859 adresinden alındı

Altın, O. (2023). AB'nin Siber Güvenlik Alanındaki Politikalarının ve Uygulamalarının Etkinliği: Bir Siber Güvenlik Temsilcisi Olarak AB'nin Yeterliliği. *Çankırı Karatekin Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi*,, Cilt 13, Sayı 2, Sayfalar 482 - 507.

Anadolu Ajansı. (2018, Mart 14). *İngiltere ilke Rusya arasında casus krici tırmanıyor*. Aralık 2023 tarihinde https://www.aa.com.tr/tr/dunya/ingiltere-ile-rusya-arasinda-casus-krizi-tirmaniyor-/1088291 adresinden alındı

Anadolu Ajansı. (2020, 09 23). *Türk dünyasının büyük düşünce adamı: Gaspıralı İsmail*. Ocak 2024 tarihinde https://www.aa.com.tr/tr/portre/turk-dunyasinin-buyuk-dusunce-adami-gaspirali-ismail/1982859 adresinden alındı

Atakan, M. (2021). Siber Güvenlik Ve Covid 19 Salgının Uzaktan Denetim Üzerinde Etkileri. *Denetişim*, , Cilt 0, Sayı 22, Sayfalar 27 - 39.

BBC News Türkçe. (2015, 12 24). Ocak 2024 tarihinde Türkiye'ye siber saldırının 10 günü: Ne oldu?: https://www.bbc.com/turkce/haberler/2015/12/151224_siber_saldiri_arslan adresinden alındı

CCDCOE. (2023). *About us*. Ocak 2024 tarihinde https://ccdcoe.org/about-us/ adresinden alındı

Dilek, E., & Talih, Ö. (2023). Estonya 2007 siber saldırılarının incelenmesi ve ülkelerin ulusal siber güvenlik politikalarına etkileri. *Bilgi yönetimi dergisi, 6*(2), 332 - 347.

Dolma, Ö. (2023). Siber Güvenlik İhbarcılarının Korunması Açısından ABD ve AB Yaklaşımlarının Karşılaştırılması. *Pamukkale Üniversitesi İşletme Araştırmaları Dergisi*,, Cilt 10, Sayı 2, Sayfalar 615 - 631.

Eldem, T. (2021). Uluslararası Siber Güvenlik Normları ve Sorumlu Siber Egemenlik. *İstanbul Hukuk Mecmuası*, Cilt 79, Sayı 1, Sayfalar 345 - 376.

ENISA. (2024). *Stracture and organization*. Ocak 2024 tarihinde https://www.enisa.europa.eu/about-enisa/structure-organization adresinden alındı

Göçoğlu, V., & Aydın, M. D. (2019). Siber Güvenlik Politikası: Abd, Rusya Ve Çin Üzerine Karşılaştırmalı Bir Analiz. *Güvenlik Bilimleri Dergisi*, , Cilt 8, Sayı 2, Sayfalar 229 - 252.

Gündüz, M. Z., & Daş, R. (2022). Kişisel Siber Güvenlik Yaklaşımlarının Değerlendirilmesi. *Dicle Üniversitesi Mühendislik Fakültesi Mühendislik Dergisi*,, *13*(3), 429-438.

Gündoğdu, S. (2023). Uluslararası Politikada Bir Etki Aracı Olarak Siber Güvenlik Ve Türkiye'nin Siber Güvenlik Politikası Uygulaması: Ulusal Siber Olaylara Müdahale Merkezi (Usom). *Fırat Üniversitesi Sosyal Bilimler Dergisi*,, Cilt 33, Sayı 3, Sayfalar 1325 - 1337.

Güngöe, U., & Güney, O. (2017). Uluslararası İlişkilerde Güvenliğin Dönüşümü Çerçevesinde Bilgi Güvenliği Ve Siber Savaş. *Karadeniz Araştırmaları*, Cilt 14, Sayı 55, Sayfalar 131 - 146.

Güntay, V. (2018). Siber Güvenliğin Uluslararası Politikada Etki Aracına Dönüşmesi ve Uluslararası Aktörler. *Güvenlik Stratejileri Dergisi*, Cilt 14, Sayı 27, Sayfalar 79 - 111.

Ünal, E., Kanat, S., & Gürkaynak, M. (2023). Hibrit Tehditler Ve Avrupa Birliği . *Süleyman Demirel Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, Cilt 1, Sayı 45, Sayfalar 391 - 412.

Köker, A. E. (2022). Avrupa Birliği'nin Gelişen ve

Değişen Tehdit Algısı: Siber Güvenlik. *EURO Politika,* , Sayı 14, Sayfalar 48 - 77.

Köksal, F. (2020). Avrupa Birliği'nin Siber Güvenlik Politikası: Kurumsalcılık mı Tutarlılık mı? *Güvenlik Stratejileri Dergisi*, Cilt 16, Sayı 35, Sayfalar 635 - 674.

Kaptan, S. (1991). *Bilimsel araştırma ve istatistik teknikleri.* Ankara: Tekışık Web Ofset Tesisleri.

Karasoy, H. A., & Babaoğlu, P. (2021). Türkiye'de Siber Güvenlik: Yasal Ve Kurumsal Altyapı. *Yasama Dergisi*, Sayı 44, Saylar 123-155.

Kişman, Z. A., & Güleç, Ö. (2021). Uluslararası İlişkiler Açısından Siber Güvenlik ve NATO'nun Siber Güvenlik Stratejileri. *Akademik Açı*, Cilt 1, Sayı 1, Sayfalar 127 - 154.

Kurnaz, S., & Önen, S. (2019). Avrupa Birliğine Uyum Sürecinde Türkiye'nin Siber Güvenlik Stratejileri. *International Journal of Politics and Security*, Cilt 1, Sayı 2, Sayfalar 82-13.

Milli Savunma Bakanlığı. (2018). *Zeytin dalı harekatı*. Aralık 2023 tarihinde https://www.msb.gov.tr/ZeytinDaliHarekati adresinden alındı

Nezgitli, S., & Benzer, R. (2020). Avrupa Birliği Siber Güvenlik Kanunu. *Journal of Information Systems and Management Research*, Cilt 2, Sayı 1.

NTV . (2018, Nisan 11). *Turmp:Hazır ol Rusya, füzelere gelecek*. Aralık 2023 tarihinde https://www.ntv.com.tr/dunya/trump-hazir-ol-rusya-fuzeler-gelecek,IiARdXk_xEq7aq0I8tgplw adresinden alındı

NTV. (2023, 4 4). *NATO nedir, ne demek? NATO ne zaman kuruldu?* Ocak 2024 tarihinde https://www.ntv.com.tr/dunya/nato-nedir-ne-demek-nato-ne-zaman-kuruldu,kZ0uYGG3GEG9NYJ3rz4A1Q# adresinden alındı

Paltacı, B. M. (2022). Ukrayna-Rusya Savaşı Bağlamında Siber Güvenlik Ekosistemi'Nde Yaşanan Gelişmeler Ve Değerlendirmeler. *Orta Doğu ve Orta Asya-Kafkaslar Araştırma ve Uygulama Merkezi Dergisi*, Cilt 2, Sayı 2, Sayfalar 1 - 19.

Renda, K. K. (2022). Avrupa Siber Güvenlik Politikasının Gelişimi: Eşgüdümcü Rol'den Siber Güce? *Ankara Avrupa Çalışmaları Dergisi,* , Cilt 21, Sayı 2, Sayfalar 469 - 495.

Türk Devletleri Teşkilatı. (2024). *Türk Devletleri Teşkilatı*. Ocak 2024 tarihinde https://www.turkicstates.org/tr/turk-konseyi-hakkinda#:~:text=T%C3%BCrk%20Devletleri%20Te%C5%9Fkilat%C4%B1%20(eski%20ad%C4%B1yla,%C3%B6rg%C3%BCt%20olarak%202009%20y%C4%B1l%C4%B1nda%20kurulmu%C5%9Ftur. adresinden alındı

Türk Dil Kurumu. (2024, Ocak 02). *Güncel Türkçe sözlük*. Türk Dil Kurumu Sözlükler: https://sozluk.gov.tr/ adresinden alındı

Taş, E. (2017, Eylül 9). *Siber Guvenlik 2030.* Ocak 2024 tarihinde DigitalAge TechSummit: https://digitalagesummit.com/en/schedule/vivamus-vitae-quam-dui/ adresinden alındı

The Hacker News. (2012, 3 29). *Apple Azerbaijan got hacked by Team Nuts*. Ocak 2024 tarihinde https://thehackernews.com/2012/03/apple-azerbaijan-got-hacked-by-team.html adresinden alındı

The Hacker News. (2012, 2 23). *Azerbaijan Arrests Iranian terror group, Iranian Hackers hit Azerbaijan Sites*. Ocak 2024 tarihinde https://thehackernews.com/2012/02/azerbaijan-arrests-iranian-terror-group.html adresinden alındı

The Hacker News. (2012, 1 30). *Embassy of Kazakhstan hacked by Anonymous Supporters*. 1 2024 tarihinde https://thehackernews.com/2012/01/embassy-of-kazakhstan-hacked-by.html adresinden alındı

The Hacker News. (2012, 2 24). *Iran Cyber Army in Action, Azerbaijani TV Down !* Ocak 2024 tarihinde https://thehackernews.com/2012/02/iran-cyber-army-in-action-azerbaijani.html adresinden alındı

The Hacker News. (2019, 8 21). *Russian Hacking Group Targeting Banks Worldwide With Evolving Tactics*. 1 2024 tarihinde https://thehackernews.com/2019/08/silence-apt-russian-hackers.html adresinden alındı

The Hacker News. (2022, 6 17). *Researchers Uncover 'Hermit' Android Spyware Used in Kazakhstan, Syria, and Italy*. 1 2024 tarihinde https://thehackernews.com/2022/06/researchers-uncover-hermit-android.html?m=1 adresinden alındı

The Hacker News. (2023, 1 12). *Chinese Hackers Using SugarGh0st RAT to Target South Korea and Uzbekistan*. 1 2024 tarihinde https://thehackernews.com/2023/12/chinese-hackers-using-sugargh0st-rat-to.html adresinden alındı

The Hacker News. (2023, 10 19). *Operation Rusty Flag: Azerbaijan Targeted in New Rust-Based Malware Campaign*. 1 2024 tarihinde https://thehackernews.com/2023/09/operation-rusty-flag-azerbaijan.html adresinden alındı

TRT Haber. (2019, 10 28). Ocak 2024 tarihinde Türkiye'ye yönelik siber saldırılar bertaraf edildi: https://www.trthaber.com/haber/turkiye/turkiyeye-yonelik-siber-saldirilar-bertaraf-edildi-437841.html adresinden alındı

Yüksek Seçim Kurumu. (2019). *Cumhurbaşkanı seçimi ve 27. dönem milletvekili genel seçimi*. Aralık 2023 tarihinde https://www.ysk.gov.tr/tr/24-haziran-2018-secimleri/77536 adresinden alındı

Yılmaz, O. (2018). Küreselleşme Sürecinde Dönüşen Güvenlik Algısı Ve Siber Güvenlik. *Cyberpolitik Journal*, Cilt 2, Sayı 4, Sayfalar 22 - 43.