YENİ DÜNYA DÜZENİNDE SİBER EGEMENLİK.

Türk Dünyası İçin Stratejik Uyarı, Zaafiyet Analizi ve Yol Haritası

21. yüzyılın ikinci çeyreğine girilirken güç mücadelesi artık yalnızca kara, deniz, hava ve uzay alanlarında yürümemektedir; dijital alan, bu güç mücadelesinin hem görünmeyen hem de en belirleyici cephesi haline gelmiştir. Siber güvenlik bugün teknik bir bilişim meselesi olmaktan çıkmış; milli güvenlik, ekonomik bağımsızlık, toplumsal istikrar, kritik altyapı güvenliği, istihbarat üstünlüğü ve siyasal egemenlik meselesine dönüşmüştür. ENISA'nın 2025 Tehdit Manzarası raporuna göre operasyonel teknoloji tehditleri toplam tehditlerin yüzde 18,2'sini, tedarik zinciri riskleri ise yüzde 10,6'sını oluşturmaktadır; bu tablo, saldırganların artık yalnızca kurumları değil, sanayi, enerji ve bağımlı ekosistemleri hedeflediğini göstermektedir.[1] Bu bağlamda mesele, "siber saldırı olur mu?" sorusu değildir. Esas soru şudur: devletler, toplumlar ve medeniyet havzaları dijital bağımlılık, veri sömürüsü, platform manipülasyonu ve hibrit etki operasyonları karşısında ne kadar dirençlidir? Sosyal medya platformlarının yabancı etki operasyonlarında ana yayılım alanına dönüşmesi, yapay zekâ destekli dezenformasyonun hızla büyümesi ve 5G'ye geçişin beraberinde yeni yüzeyler açması, Türk dünyası için siber güvenliğin artık ertelenebilir bir gündem olmadığını ortaya koymaktadır. Avrupa Dış İlişkiler Servisi'nin 2025 tarihli tehdit raporu, sosyal medya platformlarının yabancı bilgi manipülasyonu ve müdahalesinin başlıca "hotbed" alanı olmaya devam ettiğini vurgulamaktadır. ABD Adalet Bakanlığı ise 2024'te Rusya bağlantılı bir etki operasyonunun yapay zekâ üretimli içerik, sahte profiller, ücretli sosyal medya reklamları ve influencer ağları üzerinden yürütüldüğünü açıklamıştır.[2]

Bu makalenin temel tezi şudur: Türk dünyası siber güvenlikte henüz geri dönülmez bir kırılma yaşamamış olsa da, parçalı yapılanma, dış teknoloji bağımlılığı, kurumsal kapasite dengesizliği ve ortak dijital savunma mimarisinin eksikliği nedeniyle stratejik risk alanına girmiştir. Bu nedenle Türk dünyası için "kırmızı alarm" ifadesi, panik değil; yüksek öncelikli, kurumsal ve eşgüdümlü bir seferberlik çağrısı olarak değerlendirilmelidir.

1. Yeni dünya düzeni neden siber alanda kuruluyor?

Geleneksel jeopolitik düşünce, gücü sınırlar, boğazlar, enerji hatları ve askeri üsler üzerinden okurdu. Bugün bunların tamamı hâlâ önemlidir; ancak bunları yöneten sinir sistemi dijital ağlara taşınmıştır. Elektrik şebekeleri, bankacılık sistemleri, gümrük hatları, hava trafik ağları, kamu veri tabanları, haberleşme omurgaları ve hatta toplumsal kanaat üretimi, artık ağ-toplum mantığı içinde çalışmaktadır. Bu yüzden siber güvenlik, savunmanın teknik alt başlığı değil, devlet aklının çekirdeğidir.

Kanada'nın 2025–2026 Ulusal Siber Tehdit Değerlendirmesi, siber tehdit ortamını yalnızca suç ekonomisi üzerinden değil, devlet destekli ve stratejik etki doğuran faaliyetler üzerinden değerlendirmektedir. Aynı dönemde birçok Batılı güvenlik kurumu, hibrit kampanyaların siber sabotaj ile dezenformasyonu birleştirdiğini vurgulamıştır.[3] Bu durum bize iki kritik sonuç verir. Birincisi, saldırı artık sadece sisteme sızmak değildir; toplumu yönlendirmek, güveni aşındırmak, karar alma süreçlerini bozmak ve devleti reaksiyona zorlamak da saldırının parçasıdır. İkincisi, savunma yalnızca firewall ve antivirüs yatırımıyla kurulamaz; istihbarat, iletişim, hukuk, eğitim, diplomasi ve sanayi politikasıyla birlikte ele alınmalıdır.

2. Dünyada istihbarat ve güvenlik yapıları siber alanda nasıl kontrol kuruyor?

Modern istihbarat yapılarının siber alandaki kontrol mekanizmaları birkaç ana kanal üzerinde yükselir.

-İlk kanal veri akışıdır. Kim hangi platformu kullanıyor, hangi veriyi nerede depoluyor, hangi uygulama hangi izinleri topluyor, hangi reklam teknolojisi hangi davranış modelini çıkarıyor; bunların tamamı modern istihbaratın pasif ve aktif çalışma alanıdır.

-İkinci kanal platform ekosistemidir. Sosyal medya, arama motorları, bulut servisleri, mobil işletim sistemleri ve uygulama mağazaları, yalnızca ticari araçlar değil; davranış haritalama ve etki alanı üretme imkânı sağlayan dijital ekosistemlerdir.

-Üçüncü kanal tedarik zinciridir. ENISA'nın 2025 raporunda tedarik zinciri risklerinin kayda değer paya ulaşması, üçüncü taraf sağlayıcılar ve bağımlı yazılım-bileşen yapısının stratejik bir zafiyet ürettiğini teyit etmektedir.[4]

-Dördüncü kanal ise etki operasyonlarıdır. ABD Adalet Bakanlığı'nın 2024 açıklamasında ortaya koyduğu örnekte, yabancı etki operasyonunun influencer'lar, yapay zekâ içerikleri, ücretli reklamlar, sosyal medya hesapları ve sahte alan adları üzerinden yürütüldüğü belirtilmiştir. Bu, klasik propaganda döneminden farklı olarak, merkezi bir yayın yerine çok katmanlı ve algoritmik yayılım modeline geçildiğini göstermektedir.[5]

Dolayısıyla kontrol artık yalnızca "dinlemek" değildir; görmek, modellemek, yönlendirmek, görünürlüğü artırmak veya azaltmak, gündemi saptırmak ve güven krizleri üretmektir. Bu nedenle siber güvenlik ile bilgi güvenliği, medya okuryazarlığı ve ulusal stratejik iletişim birbirinden ayrı düşünülemez.

3. Sosyal medya bu denklemin neresinde?

Sosyal medya artık bir iletişim kanalı değil; toplumsal algı, siyasal davranış, kriz psikolojisi ve kamusal meşruiyetin üretildiği ana mücadele zeminidir. EEAS'ın 2025 raporunda sosyal medya platformlarının yabancı bilgi manipülasyonu için temel alan olmaya devam ettiği belirtilmektedir. FBI da yabancı aktörlerin siyasal süreçleri etkilemek için siber saldırılar, örtülü etki operasyonları ve sosyal medya dezenformasyonunu birlikte kullandığını uzun süredir vurgulamaktadır.[6]

Burada asıl risk, yanlış bilginin varlığı değil; organize biçimde yayılması, algoritmaların aşırı duygusal ve kutuplaştırıcı içeriği öne çıkarması ve toplumun güven refleksinin aşındırılmasıdır. Yani saldırı bazen sunucuya değil, zihne yapılır. Seçim dönemlerinde, etnik hassasiyetlerde, kriz anlarında veya dış politika kırılmalarında sosyal medya; devlet-toplum bağını gevşetmek, karar vericilere baskı oluşturmak ve hedef ülkede dağınık bir "algı cephesi" kurmak için kullanılabilir.

Algoritmaların çalışma mantığı:

Duygusal içerik → daha fazla yayılım

Kutuplaştırıcı içerik → daha fazla etkileşim

Hızlı içerik → daha fazla görünürlük

Bu yapı, şu riski doğurur:

Gerçeklik değil, algı kazanan taraf belirleyici olur.

Türk dünyası için bu durum kritik bir zafiyet üretir:

Ortak tarih → kolay manipülasyon

Ortak kimlik → hızlı mobilizasyon

Duygusal bağ → yüksek kırılganlık

4. 4G'den 5G'ye geçiş nasıl oldu, 4.5G neydi?

5G teknolojisi çoğu zaman belirli bir ülke veya şirket ile özdeşleştirilmektedir. Özellikle Çin merkezli Huawei'nin küresel pazardaki güçlü konumu, bu algının oluşmasına neden olmuştur. Ancak 5G, tek bir ülkeye ait bir teknoloji değil; uluslararası standartlar çerçevesinde gelişen çok aktörlü bir ekosistemdir. Bu tartışmanın özünde yer alan mesele, doğrudan bir "teknoloji riski"nden ziyade, stratejik bağımlılık riskidir. Çünkü 5G altyapısı yalnızca iletişimi değil; veri akışını, kritik hizmetleri ve dijital ekonomiyi yöneten temel omurgayı oluşturmaktadır.

Türkiye'de 4.5G olarak adlandırılan LTE-Advanced teknik bir standart değil, Türkiye'ye özgü bir pazarlama+politika dilidir. Bu geçiş, çoğu zaman yalnızca teknik bir altyapı güncellemesi olarak değerlendirilmiştir. Ancak bu süreç, daha geniş bir perspektiften bakıldığında, dijital dönüşümün kontrollü ve kademeli ilerletilmesine imkân tanıyan bir ara evre işlevi görmüştür.[7]

Türkiye'nin 4.5G süreci de bu bağlamda değerlendirildiğinde:

altyapı olgunlaşması

kullanıcı adaptasyonu

regülasyonların gelişimi

güvenlik farkındalığının artışı gibi alanlarda önemli bir hazırlık dönemi sağlamıştır. Bu durum, Türkiye'nin dijital dönüşümde dolaylı olarak "kademeli geçiş ve risk yayma stratejisi" uyguladığını göstermektedir. Dolayısıyla 4.5G süreci, yalnızca teknolojik bir ara basamak değil; aynı zamanda daha kompleks bir dijital geleceğe hazırlık evresi olarak okunmalıdır.

5. 5G neden sadece hız değil, egemenlik meselesidir?

5G tartışması çoğu zaman internet hızına indirgeniyor. Oysa asıl mesele, kritik hizmetlerin gerçek zamanlı, düşük gecikmeli, çok bağlantılı ve yazılım tanımlı ağ mantığıyla çalışacak olmasıdır. Bu; akıllı şehirlerden enerji şebekelerine, savunma sanayiinden lojistiğe, limanlardan insansız sistemlere kadar geniş bir alanı etkiler.

Azerbaycan için hazırlanan EU4Digital yol haritası da 5G özel ağlarının tarım, petrol-gaz, madencilik, enerji ve su yönetimi gibi sektörlerde dönüşüm potansiyeline işaret ediyor. Fakat 5G'nin getirdiği geniş yüzey, yeni zafiyetler de üretir. Özellikle IoT cihazları, özel ağlar, bulut bağımlılığı ve yazılım güncelleme zinciri, saldırı yüzeyini büyütür. Özbekistan CERT'in 2025 tehdit öngörüsü, 5G ve IoT cihazlarına yönelik saldırıları açıkça başlıca riskler arasında saymaktadır.[8] Bu nedenle 5G'ye hazırlık; sadece baz istasyonu kurmak değil, güvenli çekirdek şebeke, ulusal test laboratuvarı, tedarik zinciri denetimi, sertifikasyon, veri yerelliği ve milli kripto/kimlik altyapısı kurmaktır.

6. Türk dünyası buna hazır mı?

Cevap tek kelimeyle şudur: KISMEN

Türkiye'nin 2024–2028 Ulusal Siber Güvenlik Stratejisi;

siber dayanıklılık

proaktif çalışma

İnsan odaklı yaklaşım

Teknolojinin güvenli kullanımı

yerli ve milli teknolojiler

Uluslararası iş birliği

Bu 6 ana hedefe dayanıyor.

ITU GCI 2024 bağlamında Türkiye'nin 100 puan alan ülkeler arasında gösterilmesi, kurumsal iradenin ve olgunluk seviyesinin yüksek olduğunu gösteriyor.[9]

Azerbaycan da 93,76 puanla "advanced" grupta yer almakta; ancak kendi kurumlarının değerlendirmesine göre kapasite geliştirme, teknik ve organizasyonel alanlarda ilave çabaya ihtiyaç duymaktadır. 2025 sonunda Cumhurbaşkanı Aliyev, siber güvenlik stratejisinin ulusal güvenlik mimarisinin temeli olduğunu açıkça vurgulamıştır. Aynı dönemde hükümet düzeyinde sektörel SOC'lar ve CERT yapılarının kurulması ihtiyacı da dile getirilmiştir.[10]

Kazakistan 94,04 puanla Tier 2'de yer almakta ve resmi hedef olarak 5G yayılımını 2025 sonuna kadar tamamlama yönünde ilerlemektedir; Haziran 2024 itibarıyla 20 şehirde 1.144 baz istasyonu kurulmuştu. Bu, dijitalleşme iradesinin yüksek olduğunu gösterir; fakat yüksek bağlantı, otomatik olarak yüksek dayanıklılık anlamına gelmez.[11]

Özbekistan son yıllarda siber güvenlik konumunu güçlendirmiştir; ITU'nun 2024 değerlendirmesine göre Azerbaycan ve Kazakistan ile birlikte ikinci gruba yükselmiştir. Ancak ülkenin CERT kurumu 2025 için phishing, deepfake, mobil cihaz saldırıları, ransomware, 5G/IoT saldırıları, içeriden tehditler ve kritik altyapı saldırılarını başlıca riskler olarak tanımlamaktadır.[12]

Kırgızistan ise kurumsal yapı oluşturmuş olsa da ITU değerlendirmesinde "establishing" grubundadır. Ülkede Koordinasyon Merkezi 2020'den beri faaliyettedir ve 2025'te ulusal siber tatbikat düzenlenmiştir; ancak kapasite derinliği ve sistemik direnç bakımından daha erken aşamadadır.[13]

Bu tablo bize şunu söyler:

Türkiye → ileri seviyede kurumsallaşma

Azerbaycan & Kazakistan → gelişmiş yapı

Özbekistan → yükselen kapasite

Kırgızistan → gelişim aşaması

Bütün bu değerlendirmeler zayıflıktan çok asimetri ve koordinasyon eksikliği sorununu ortaya koymaktadır.

Tek-tek güçlü olmak, birlikte güvenli olmak anlamına gelmez.

7. Başlıca zaafiyetler nelerdir?

7.1. En büyük zaafiyet parçalı mimaridir. Ortak savunma mekanizmasının eksikliği.

Yapılması gerekenler

ortak siber tatbikat,

ortak olay müdahale protokolü,

ortak tehdit istihbaratı havuzu

ortak tedarik güvenliği standardı oluşturulmalıdır.

7.2. Teknolojik dış bağımlılık.

Telekom çekirdeği,

bulut altyapısı,

işletim sistemleri,

mobil uygulama ekosistemi

reklam-teknoloji katmanı büyük ölçüde dış merkezli kaldıkça, egemenlik yalnızca hukuki metinlerle korunamaz.

7.3. İnsan faktörü. Özbekistan CERT'in de vurguladığı gibi phishing, sosyal mühendislik ve deepfake tehditleri teknik açıklardan çok insan reflekslerini hedeflemektedir. Toplum, kamu kurumları e özel işletmeler ardıcıl olarak bilgilendirilmeli, eğitimler, seminerler, yarışmalar düzenlenmelidir.

7.4. Kritik altyapıların artan bağlantılılığıdır. ENISA'nın operasyonel teknoloji tehdidini yüzde 18,2 seviyesinde göstermesi, enerji, sanayi ve ulaştırma alanlarının giderek daha kırılgan hale geldiğini ortaya koymaktadır.

7.5. Algoritmik manipülasyon, bilgi alanıdır. Sosyal medya üzerinden yürüyen yabancı etki operasyonları, özellikle Türk dünyası gibi kimlik, tarih ve dış politika başlıklarının duygusal yoğunluk taşıdığı coğrafyalarda çok daha yüksek stratejik sonuç üretebilir.

8. Türk dünyası kırmızı alarm vermeli mi?

Bu soruya verilecek cevap nettir: EVET - bu alarm panik değil, stratejik farkındalık alarmıdır.

Bugün için "kırmızı alarm" demek, yarın tüm sistemlerin çökeceğini söylemek değildir. Bunun anlamı şudur: tehdit, münferit olmaktan çıkmış; yapısal hale gelmiştir. Siber alan artık yalnızca bilişim uzmanlarının teknik masası değil, devletin beka masasıdır. Türk dünyası için mesele tek tek siber saldırılar değil; dijital bağımlılık, ortak savunma eksikliği, algoritmik nüfuz, dış platform hegemonyası ve kritik altyapıların kırılganlığıdır.

Bu nedenle asıl soru “tehlike var mı?” değil, “tehlikeyi medeniyet ölçeğinde okuyabiliyor muyuz?” sorusudur.

9. Düşük Teknoloji Paradoksu

En İleri Güvenlik Bazen En Basit Olandır. Son dönemde özellikle Orta Doğu sahasında yürütülen istihbarat faaliyetlerine dair analizlerde dikkat çekici bir yaklaşım öne çıkmaktadır: yüksek teknoloji yerine düşük teknoloji kullanımı.

İsrail’in İran içerisindeki bazı operasyonlarda, saha elemanlarıyla iletişim kurmak amacıyla dijital ve izlenebilir sistemler yerine analog radyo frekansları ve basit şifreleme yöntemleri kullandığına dair çeşitli analizler ve iddialar bulunmaktadır. Bu tür yöntemler, ilk bakışta ilkel olarak değerlendirilebilir; ancak istihbarat perspektifinden bakıldığında bu yaklaşım son derece rasyoneldir.

Modern dijital sistemler; izlenebilirlik, kayıt altına alınabilirlik ve siber müdahaleye açıklık gibi riskler taşımaktadır. Buna karşılık analog iletişim sistemleri:

merkezi altyapıya bağlı değildir

dijital iz bırakmaz

siber saldırıya maruz kalmaz

doğal sinyal karmaşası içinde tespit edilmesi zorlaşır

Bu durum, istihbarat literatüründe giderek daha fazla karşılaşılan bir gerçeği ortaya koymaktadır:

En güvenli sistem, çoğu zaman en gelişmiş olan değil, en az iz bırakan sistemdir.

Türk dünyası açısından bu çıkarım son derece kritiktir. Çünkü dijitalleşme süreci hızlanırken, tüm güvenliğin yalnızca ileri teknolojiye bağlanması, alternatif ve düşük görünürlüklü iletişim yöntemlerinin göz ardı edilmesine yol açabilir.

Dolayısıyla siber güvenlik stratejileri: yalnızca yüksek teknolojiye değil, aynı zamanda düşük izli, alternatif ve bağımsız iletişim yöntemlerine dayandırılmalıdır. Bu bir zafiyet değil, tam tersi ileri seviye istihbarat doktrinidir.

Bu yaklaşım, geleceğin güvenlik mimarisinde “hibrit güvenlik modeli”nin kaçınılmaz olduğunu göstermektedir.

EN GÜVENLİ AĞ = HİÇ OLMAYAN AĞ

10. Ne yapmalıyız? Stratejik yol haritası

10.1. Türk dünyası öncelikle müşterek bir siber güvenlik konsepti üretmelidir. Bu konsept, sadece iyi niyet bildirgesi değil; tehdit sınıflandırması, olay müdahale prosedürü, kritik altyapı listesi, ortak eğitim modülü ve kriz iletişim protokolü içermelidir.

10.2. Türk Devletleri Teşkilatı veya benzeri bir mekanizma altında "Türk Dünyası Siber Koordinasyon Ağı" kurulmalıdır. Bu ağ; CERT'ler, savunma kurumları, telekom otoriteleri ve stratejik iletişim birimlerini bir araya getirmelidir.

10.3. Ortak siber tatbikatlar yılda en az bir kez yapılmalıdır. Kırgızistan'daki 2025 tatbikatı gibi örnekler, ulusal seviyede değerlidir; fakat bunların bölgesel sürümü kurulmadıkça müşterek refleks oluşmaz.

10.4. 5G ve sonrasına yönelik telekom güvenliği bir sanayi politikası olarak görülmelidir. Yerli çekirdek ağ bileşenleri, güvenlik sertifikasyonu, kaynak kod denetimi ve tedarik zinciri incelemesi olmadan gerçek siber egemenlik kurulamaz.

10.5. Sosyal medya ve dijital etki operasyonlarına karşı ortak stratejik iletişim ve doğrulama mekanizması oluşturulmalıdır. Dezenformasyonla mücadele, sansür mantığıyla değil; hızlı teyit, kaynak analizi, ağ davranışı tespiti ve toplumsal dijital okuryazarlıkla yürütülmelidir.

10.6. Siber güvenlik eğitimi elit bir uzmanlık alanı olmaktan çıkarılıp milli kapasite programına dönüştürülmelidir. Lise, üniversite, kamu personeli ve kritik sektör çalışanları için katmanlı eğitim sistemi zorunlu hale gelmelidir.

10.7. Veri egemenliği başlığı netleştirilmelidir. Verinin nerede tutulduğu, hangi yargı alanına tabi olduğu, hangi bulut servislerinin hangi kritik sektörlerde kullanılabileceği, artık ekonomik değil doğrudan güvenlik sorusudur.

SONUÇ

Yeni dünya düzeni yalnızca başkentlerde, zirvelerde ve askeri doktrinlerde şekillenmiyor; veri merkezlerinde, fiber omurgalarda, baz istasyonlarında, platform algoritmalarında ve istihbaratın dijital uzantılarında inşa ediliyor. Bu nedenle siber güvenlik artık teknik savunma değil, milli egemenliğin dijital suretidir.

Türk dünyası bugün tamamen hazırlıksız değildir. Türkiye, Azerbaycan, Kazakistan ve Özbekistan'ın son yıllardaki kurumsal ilerlemeleri bunu göstermektedir; Kırgızistan da kurumsal zemin oluşturmaktadır. Ancak asıl açık, tekil ilerleme ile müşterek savunma arasındaki boşluktadır. Geleceğin mücadelesi, sadece kimin daha çok bağlandığıyla değil, kimin daha güvenli, daha yerli, daha koordineli ve daha dirençli bağlandığıyla belirlenecektir.

KAYNAKLAR

enisa.europa.eu ENISA THREAT LANDSCAPE, october 2025, sayfa 28-35

3rd EEAS REPORT, 31 Mart 2025, sayfa 12-13

NAATIONAL CYBER THEART ASSESMENT 2025-2026 / CANADIAN CENTER FOR SYBER SECURITY

ENISTA THREAT LANDSCAPE, october 2025, sayfa 49-54

ABD ADALET BAKANLIĞI Bülteni, 4 Eylül 2024

3rd EEAS REPORT, 31 Mart 2025, sayfa 18-24

TÜRKCELL RAPORU 31 aralık 2022

UZCERT XİZMETİ RAPORU 2025, 4. Bölüm

cyberartspro.com ULUSAL SIBER GÜVENLİK STRATEJİSİ 2024-2028 EYLEM PLANI

akta.az ULUSLARAARASI TELEKOMUNİKASYON BİRLİĞİ "KÜRESEL SİBER GÜVENLİK ENDEKSİ 2024 - AZERBAYCAN"

astanatimes.com İNTERNATİONAL TELEKOMMUNİCATİON UNİON " GLOBAL CYBERSECURIY İNDEX 2024 - KAZAKHSTAN

itu.int SİBER GÜVENLİK VE KİŞİSEL VERİ KORUNMASI, 14 ocak 2024

cert.gov.kg BÜLTENLER