

Zafer Bozyer¹İskenderun Teknik Üniversitesi
Yönetim Bilişim Sistemleri Bölümü
Dr. Öğretim Üyesi**MERKEZİ OLMAYAN FİZİKSEL ALTYAPILAR: MİLLİ GÜVENLİK AÇISINDAN BİR TEHDİT OLABİLİR Mİ?****GİRİŞ**

Günümüzde dijitalleşme, yalnızca teknolojik bir trend olmaktan çıkarak yaşamın her alanına nüfuz eden kapsamlı bir dönüşümü beraberinde getirmektedir. Blokzincir teknolojisi merkezi olmayan uygulamaları yaygınlaştırırken Artırılmış Gerçeklik (AR), Sanal Gerçeklik (VR) gibi teknolojiler fiziksel ve dijital dünyalar arasındaki sınırları giderek daha da belirsizleştirmekte; yapay zekâ destekli sistemler ve gelişmiş görüntü işleme teknikleri ise görsel algının sınırlarını ve görsel verilerin kullanım alanlarını genişletmektedir. Dijitalleşmenin bir parçası olan bu yeni nesil teknolojiler eğitimden sağlığa, mimariden eğlenceye, sanayiden turizme kadar pek çok sektöre nüfuz ederken insan-makine etkileşimini daha doğal, sezgisel ve etkili hâle getirmektedir.

Bu hızlı dönüşüm, sadece teknik gelişmeleri değil, aynı zamanda toplumsal ve kültürel dinamikleri de derinden etkileyen bir paradigma kaymasına da neden olmaktadır. Örneğin Artırılmış Gerçeklik ile gerçek dünya üzerinde kurgulanan, yerleşim alanları başta olmak üzere coğrafi olarak herhangi bir koordinatta beliren sanal canlıların yakalandığı ve oyuncular arasında turnuvalar düzenlendiği Pokemon Go gibi oyunlar geniş kitleler tarafından oynanmaktadır. Zira Mayıs 2025 itibarıyla dünya genelinde yaklaşık 127 milyon kişi bu oyunu aktif olarak oynamaktadır². Pokemon Go'nun yaygın kullanımı sayesinde oyunun geliştiricisi olan Niantic, farklı uygulamalarda kullanabilecek gerçek dünyadan içerikler elde etmektedir. Dijitalleşmenin kültürel etkilerine dair bir başka örnek ise sosyal medyada kullanıcıların gezip gördükleri yerleri paylaşma eğilimidir.

¹ Bu çalışmada ifade edilen bulgular, yorumlar, sonuçlar, öneriler ve görüşler tamamen yazar(lar)ına aittir. TEPAV'ın resmi görüşü değildir. © TEPAV, aksi belirtilmedikçe her hakkı saklıdır.

² <https://www.dexerto.com/pokemon/how-many-people-play-pokemon-go-pokemon-go-player-count-2132719/>

Sosyal medya hesaplarından turistlerin ziyaret ettikleri tüm yapıların, bölgelerin ve şehirlerin fotoğraflarına ve video kayıtlarına rahatlıkla ulaşılabilir. Öte yandan blokzincir ile hayatımıza giren kriptoparalar ve blokzincir madenciliği gelir modeli ise bir kısım insanı sürekli olarak kolay para kazanmanın yollarını aramaya sevk etmektedir. Böylece bu notta ele alınacak olan DEPIN (Decentralized Physical Infrastructure Network-Merkezi olmayan Fiziksel Altyapı Ağları) projeleri geniş kitleler arasında oldukça hızlı bir biçimde yayılabilir.

Ancak bu notun amacı dijitalleşmenin toplumsal ve kültürel etkilerini tartışmaktan ziyade ortaya çıkan dönüşümün birtakım potansiyel güvenlik risklerini de beraberinde getirebileceğine dikkat çekmektir. Önceki paragrafta bahsedilen örnekler, dijitalleşme ile toplumsal ve kültürel olarak ortaya çıkan olumsuz etkileri tartışmak veya bireylerin davranışlarını yargılamaktan ziyade ilerleyen paragraflarda anlatılacak olan potansiyel güvenlik risklerinin kapsamının ve yeni risklerin ne kadar hızlı ortaya çıkabileceğinin daha net anlaşılması için verilmiştir.

Merkezi Olmayan Fiziksel Altyapı Ağları

Merkezi olmayan fiziksel altyapı ağlarının milli güvenlik açısından oluşturabileceği risklere geçmeden önce, bu teknolojiye kısaca bahsedelim. DEPIN, fiziksel (donanım içeren) dijital altyapı hizmetlerinin tek bir merkezî otorite (örneğin bir devlet kurumu) tarafından değil, bireyler, topluluklar ya da otonom sistemler tarafından dağıtık şekilde sağlandığı ve yönetildiği projeler bütünüdür. Bu projeler genellikle blokzincir (blockchain), dağıtık ağlar ve akıllı sözleşmeler gibi teknolojiler üzerine inşa edilmektedir. Bu projelerde altyapı kelimesi sadece dijital değil, fiziksel unsurları da kapsamaktadır. Yani, blokzincir denilince ilk akla gelen kriptopara çözümlerinden oldukça farklıdır. Merkeziyetsizlik ise, bu hizmetlerin tek bir kurum ya da devlet tarafından değil, ağdaki katılımcıların (bazen kullanıcıların) karşılıklı fayda sağlamak amacıyla kolektif katkısı ve hareket etmesi ile gerçekleşmektedir.

Örneğin, bir telekomünikasyon altyapısının bireyler tarafından kurulması ilk bakışta imkânsız görünebilir. Çünkü bu tür bir altyapı; sunucular, alıcı-verici cihazlar, ağ bileşenleri ve teknik personel gibi yüksek maliyetli ve bilgi yoğun bileşenler gerektirir. Ancak teorik olarak, bu maliyet on binlerce bireyin finansal ve teknik katkısıyla karşılanabilir. Buradaki temel sorun ise birbirini tanımayan bu insanların güven ortamı içinde nasıl birlikte hareket edeceğidir. İşte bu noktada blokzincir uygulamaları devreye girmektedir. Blokzincir teknolojisi, merkezi olmayan ağların güvenli ve şeffaf şekilde kurulmasına olanak tanıyan bir altyapı sunar. Kriptopara sistemleri sayesinde bu güven mekanizması zaten pratikte kendini kanıtlamıştır. Milyonlarca insan, herhangi bir devlet otoritesine bağlı kalmaksızın, istedikleri kriptopara birimlerine yatırım yapabilmekte ve bunları küresel ölçekte kendi aralarında transfer edebilmektedirler. Ancak burada önemli bir noktaya dikkat çekmek gerekir. Kullanıcıları bu sistemlere çeken ana motivasyon genellikle "merkezi otoriteden rahatsızlık" değil, finansal kazanç beklentisidir. Kriptoparalar çoğunlukla yatırım ya da madencilik yoluyla gelir elde etmenin bir yolu olarak görülmektedir. DEPIN projeleri de tam olarak bu motivasyondan yararlanmaktadır.

Normal şartlar altında bireylerden kendi bütçeleriyle bir altyapı projesine yatırım yapmaları beklenemez. Ancak bir DEPIN projesi, "500 dolara sattığımız bu cihazı satın al, evinin çatısına ya da balkonuna kur, topladığın verileri bizimle paylaş ve karşılığında kriptopara kazanarak pasif gelir elde et" şeklinde bir teklifle geldiğinde, birçok insan bu ağa katılmayı mantıklı bulabilmektedir. Günümüzde, bu iş modeliyle çalışan ve bireylerin/kullanıcıların kendilerinin finanse ettiği onlarca DEPIN projesi mevcuttur. Katılımcılar, sisteme sundukları katkılar karşılığında kriptopara veya token ile ödüllendirilmekte; böylece ağ, kullanıcılar tarafından hem yaygınlaştırılmakta hem de sürdürülebilir hâle getirilmektedir. DEPIN projelerine birkaç örnek vermek gerekirse:

- **Helium**, kullanıcıların kurduğu LoraWAN protokolünü kullanan hotspot cihazlarıyla kablosuz ağ altyapısı sağlayarak merkezi olmayan bir IoT ve GSM ağı oluşturur³.
- **WeatherXM**, kullanıcıların kendi hava istasyonlarını kurarak gerçek zamanlı, hiper-lokal hava verisi topladığı bir hava durumu takip ağıdır⁴.
- **Wingbits**, kullanıcıların ADS-B alıcıları kurarak bölgelerinden geçen uçakların gerçek zamanlı verilerini topladığı ve paylaştığı merkezi olmayan bir hava izleme ağı sunar⁵.
- **Bee Maps**, özellikle kuryeler, taksiciler, servisler, dolmuş, otobüs gibi ulaşım araçlarını kullanan sürücülerin araçlarına yerleştirdikleri kameralar aracılığıyla sokak görüntüleri toplayıp paylaştıkları merkezi olmayan haritalama ve navigasyon ağı projesidir⁶.
- **GeodNet**, kullanıcıların çatılarında kurdukları istasyonlarla küresel bir eş zamanlı kinematik (Real-Time Kinematics, RTK) ağı oluşturur. Bu sayede GPS sinyallerinin iyileştirilmesinin hedeflendiği bir konumlandırma projesidir⁷.
- **Spexi**, drone pilotlarının otonom görevler ile uçarak yüksek çözünürlüklü görüntüleri topladığı ve bu verileri LayerDrone ağına yükledikleri DEPIN benzeri bir blokzincir projesidir⁸.
- **Over the Reality**, cep telefonları ile yer seviyesinden (şehirler, binalar vb.) görüntülerin toplanarak 3D modellere dönüştürüldüğü, DePIN benzeri başka bir projedir⁹.

Verilen örneklerin dışında farklı birçok konuda (sanal özel ağ oluşturan, merkezi olmayan bulut hizmeti veren, otomobillerin OBD portlarına bağlanarak araç kullanım verilerini toplayan, sürdürülebilir su ve kaynak yönetim hizmeti sunan, vs.) merkezi olmayan şekilde komüniteler tarafından geliştirilmiş DEPIN projeleri¹⁰ bulunmaktadır.

DEPIN Projelerinin Potansiyel Güvenlik Riskleri

Elbette, DEPIN projelerinin doğrudan bir güvenlik zafiyeti oluşturmak amacıyla geliştirildiğini söylemek doğru olmaz. Bu notta bahsi geçen projeler de dâhil olmak üzere, her bir DEPIN projesi; dijital dönüşümle birlikte ortaya çıkan altyapı ihtiyaçlarını daha verimli ve düşük maliyetli bir şekilde karşılamayı hedefleyen girişimlerdir. Ancak, özellikle istihbarat örgütlerinin faaliyet yelpazesi dikkate alındığında, bu örgütler kendilerine avantaj sağlayabilecek her tür teknolojiyi kullanmaktan çekinmemektedirler. Yalnızca son birkaç yıl içinde medyada yer alan haberler incelendiğinde, istihbarat örgütlerinin hedef aldıkları ülkelerin kritik askeri ve sivil tesislerine ait fotoğraf ve video verilerini saha ajanları aracılığıyla topladıkları¹¹; tehdit olarak değerlendirdikleri kişileri izleyerek haklarında ayrıntılı bilgi edindikleri ve gerekli gördüklerinde bu kişilere suikast düzenledikleri görülebilir. Güvenlik güçlerimiz tarafından 2024 yılının Ocak, Mart ve Nisan aylarında düzenlenen Köstebek-1¹², Köstebek-2¹³ ve Köstebek-3¹⁴

³ <https://www.helium.com>

⁴ <https://weatherxm.com>

⁵ <https://wingbits.com>

⁶ <https://beemaps.com>

⁷ <https://geodnet.com>

⁸ <https://www.spexi.com>

⁹ <https://www.overthereality.ai/tr>

¹⁰ Diğer DEPIN projeleri <https://depinhub.io/projects>

¹¹ <https://www.trthaber.com/haber/gundem/iran-adina-casusluk-yapan-5-zanli-yakalandi-900787.html>

¹² <https://www.icisleri.gov.tr/kostebek-operasyonu-ile-8-ilde-33-supheli-yakalandi>

¹³ <https://www.icisleri.gov.tr/kostebek-2-operasyonunda-7-supheli-yakalandi>

¹⁴ <https://www.icisleri.gov.tr/kostebek-3-operasyonu-ile-israil-istihbarat-servisi-icin-bilgi-toplayan-8-supheli-yakalandi>

operasyonlarında İsrail istihbarat servisi ile ilişkili, Türkiye’de bulunan şahıslar ile şirketler hakkında bilgi derleyen ve topladığı bilgi ve belgeleri İsrail istihbarat unsurlarına aktardığı tespit edilen toplam 48 kişinin gözaltına alındığı açıklanmıştır. Yine medyada söz konusu ajanlık faaliyetleri kapsamında bilgi toplama, araştırma, hedeflerin fotoğraf/video ile görüntülenmesi, takip, hedef araçlara GPS cihazı yerleştirme, darp/yaralama, kundaklama, tehdit ve şantaj gibi eylemlerin gerçekleştirildiği paylaşılmıştır¹⁵. Ayrıca yakın zamanda hem İsrail-İran hem de Rusya-Ukrayna savaşlarında patlayıcı yüklenmiş dronelar rakip ülkenin topraklarından kaldırılarak hassas hedeflere operasyonlar düzenlenmiştir. Savaşlarda drone ve İHA’lar başta olmak üzere otonom kara ve su altı araçları, akıllı mühimmatlar ve elektronik harp teknolojileri gittikçe artan bir oranda kullanılmaktadırlar.

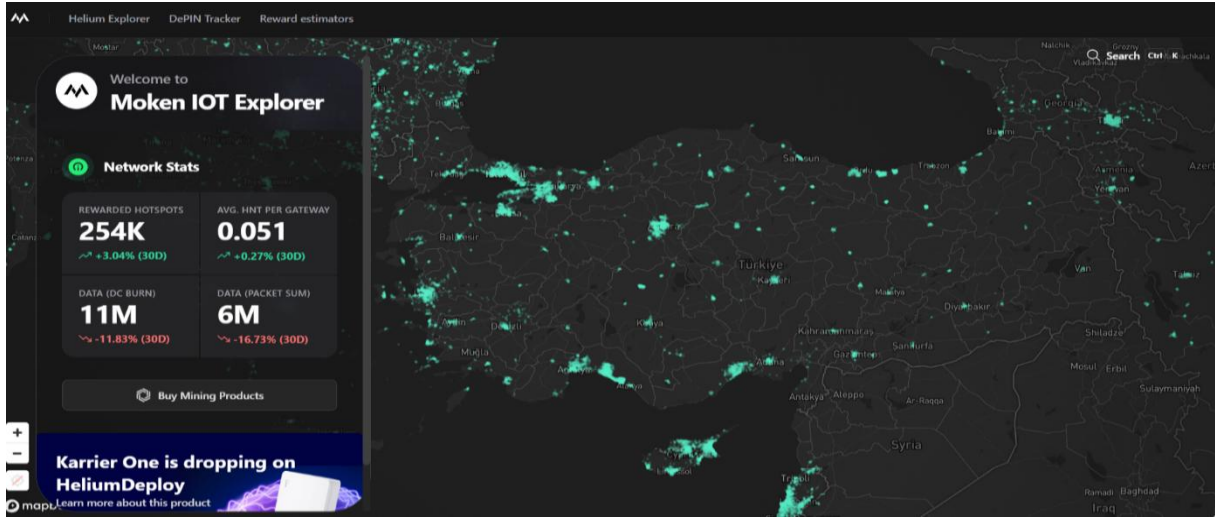
Peki, DEPIN projeleri casusluk faaliyetlerinde ya da savaşlarda kullanılabilir mi? Bu soruya “kesinlikle evet” diyebilmek için daha fazla araştırma ve teknik inceleme gereklidir. Ancak potansiyel bir risk barındırdıkları da göz ardı edilmemelidir. Örneğin, merkezi olmayan bir IoT altyapısı oluşturmak amacıyla geliştirilen *Helium* projesi; evcil hayvanların, araçların, çocukların ve yaşlıların takibinden lojistik süreçlerdeki soğuk zincirin korunup korunmadığını izlemeye, tarım uygulamalarından doğal afet sensörlerine kadar çok sayıda alanda veri toplamak için kullanılabilir. *Helium*, LoRaWAN protokolü üzerinden çalışmaktadır. Bu protokol, yüksek veri hacimlerini iletmek için uygun değildir. Ancak düşük frekanslı çalışması sayesinde duvarları geçebilir, çok düşük enerji tüketir ve bu sayede özellikle enerji verimliliği gereken senaryolarda avantaj sağlar. LORA teknolojisiyle çalışan bir cihaz, şehir içinde 2 ila 5 kilometre; açık arazide ve uygun coğrafi koşullarda ise onlarca kilometre uzağa sinyal iletebilmektedir. Elbette bu tür takip ve iletişim çözümleri, klasik GSM altyapılarıyla da sağlanabilir. Ancak GSM sistemleri yüksek bant genişliğine ve yüksek elektrik tüketimine sahiptir. Ayrıca bir GSM hattına sahip olmak genellikle kimlik doğrulaması gerektirir; yani doğrudan ya da dolaylı olarak kullanıcının kimliğini açığa çıkarır. İşte tam bu noktada DEPIN projeleri, düşük maliyetli, kimliksiz, anonim ve enerji tasarruflu alternatifler sunarak istihbarat ya da askeri amaçlarla kullanılabilecek açıklar yaratabilir. Bu doğrudan hedeflenmemiş olsa bile, teknolojinin niteliği bu tür senaryolara elverişli bir zemin sunmaktadır.

Öte yandan, biraz kodlama bilgisi olan bir uzman, kimliğini açık etmeden *Helium Console* üzerinden herhangi bir sensör cihazını bu ağa dahil edebilir. Bu durum, potansiyel casusluk senaryolarını akla getirmektedir. Örneğin, küçük bir takip cihazı hedef kişinin üzerine ya da aracına yerleştirilerek, *Helium* ağının kapsama alanında kaldığı sürece cihaz, aylarca pil değiştirmeye gerek kalmadan konum bilgisi aktarabilir. Benzer şekilde, bir eve ya da işyerine yerleştirilecek basit bir doluluk (occupancy) sensörü ile, kişinin hangi saatlerde eve girip çıktığı, hangi günler işyerinde bulunduğu gibi bilgiler otomatik olarak izlenebilir. Üstelik bu işlemler, GSM şebekesi gibi kimlik doğrulaması gerektiren altyapılardan tamamen bağımsız şekilde yapılabilir. Bu da eylemi gerçekleştirenlerin kimliğinin gizli kalmasını mümkün kılar.

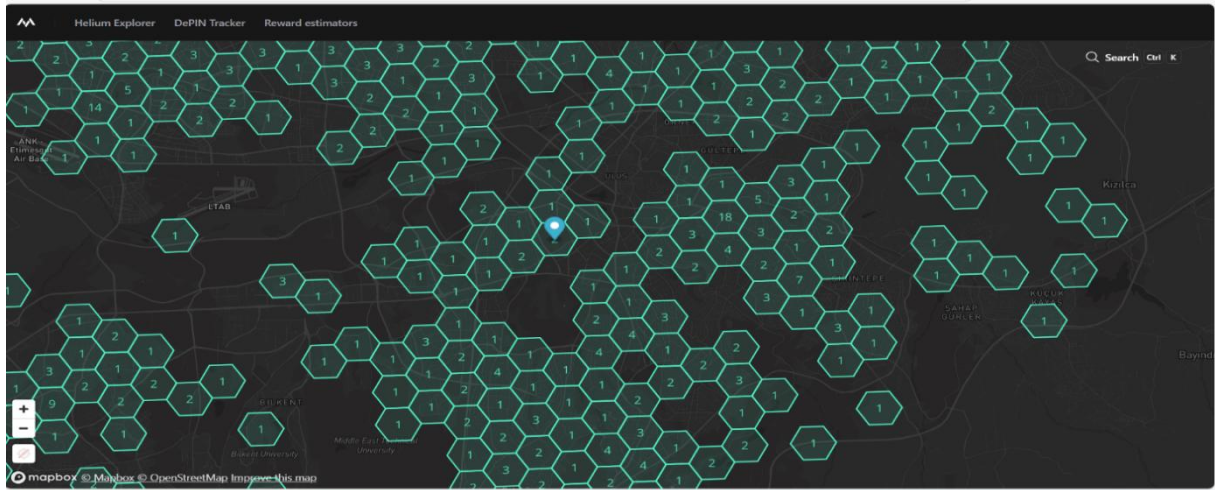
“Peki, Helium ağının kapsama alanı ne kadar olabilir ki?” diye düşünebilirsiniz. Veriler, küresel ölçekte bu ağın özellikle şehir merkezlerinde oldukça yaygınlaştığını göstermektedir. Resim 1, Helium ağının Türkiye genelinde kapsadığı şehirleri; Resim 2 ve Resim 3 ise Ankara ve İstanbul’un bazı bölgelerinde kurulu olan *Helium* cihazlarının konumlarını ve sayılarını göstermektedir. Resimlerdeki altıgen peteklerin her bir kenarı yaklaşık 700 metre uzunluğundadır. Buna göre, özellikle büyük şehir merkezlerinde *Helium* ağının kapsama alanı dışında kalan bölgeler yok denecek kadar azdır.

¹⁵ <https://www.aa.com.tr/tr/gundem/israil-istihbaratina-yonelik-2021den-bu-yana-4uncu-operasyon/3098379>

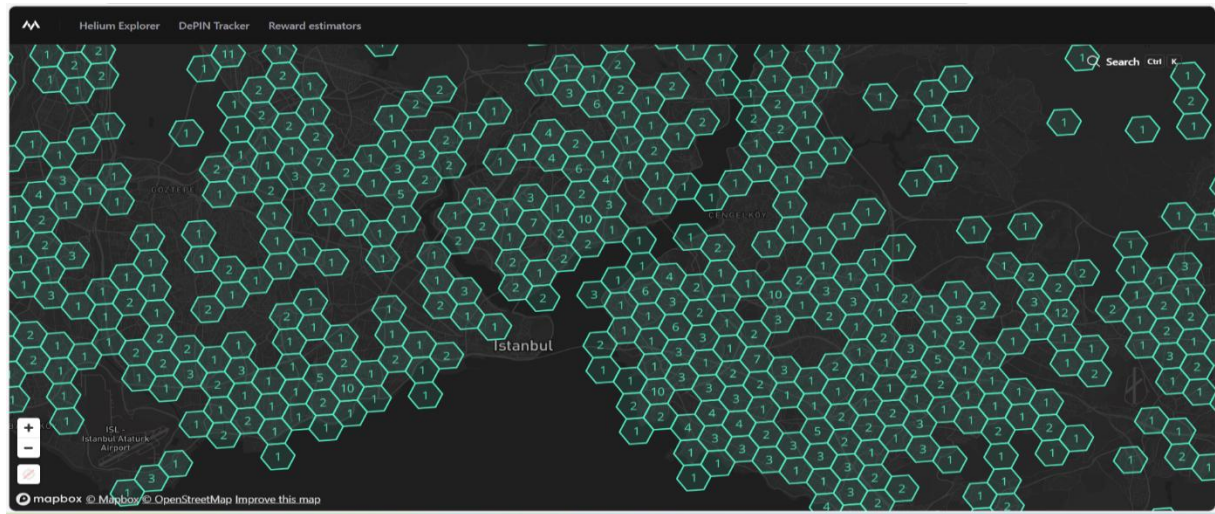
MERKEZİ OLMAYAN FİZİKSEL ALTYAPILAR: MİLLİ GÜVENLİK AÇISINDAN BİR TEHDİT OLABİLİR Mİ?



Resim 1. Helium projesine ait Türkiye’de kurulu olan cihazların dağılımı



Resim 2. Ankara’nın bir bölgesinde kurulu olan Helium cihazlarının yerleri ve sayıları

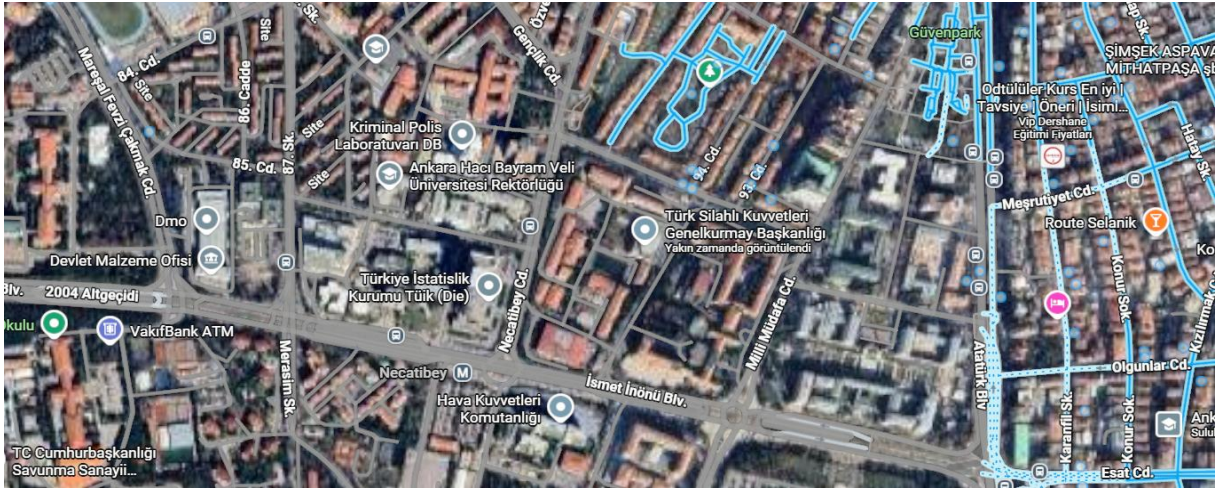


Resim 3. İstanbul’un bir bölgesinde kurulu olan Helium cihazlarının yerleri ve sayıları

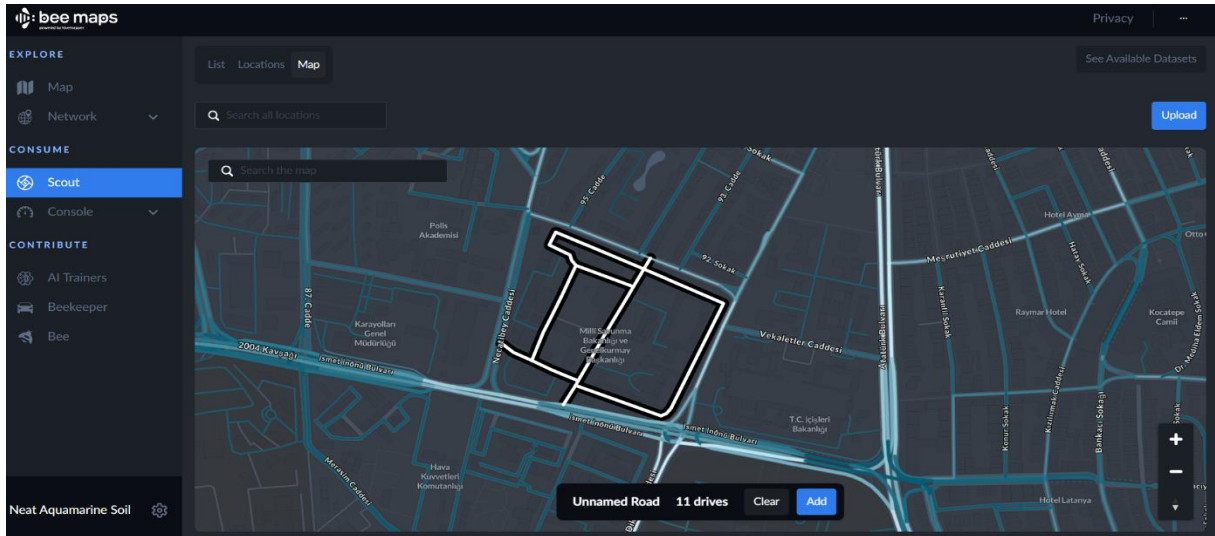
Bee Map (önceki adıyla *Hivemapper*) çözümleri, merkezi olmayan haritalama ve navigasyon hizmetleri sunmayı amaçlamaktadır. Temel prensip, *Googlemaps* ile sunulan hizmetlere benzer şekilde cadde ve sokakların üç boyutlu (3D) görünümünün ve şehir haritalarının

oluşturulmasıdır. Ancak en büyük fark, bu sistemde ağdaki her katılımcının birer "Google sokak görüntüleme aracı" gibi çalışıyor olmasıdır. *Bee Map* ağına katılan bireyler, araçlarına yerleştirdikleri ön panel (dashboard) kameraları sayesinde bulundukları bölgelerin görüntülerini sisteme yükler. Bu sayede, haritalar ve sokak görünümü sürekli ve anlık olarak güncellenebilir. Firmanın internet sitesinde yer alan "Dünyayı şu anda olduğu gibi görün, bir zamanlar olduğu gibi değil" sloganı da bu avantajını vurgulamaktadır.

Googlemaps gibi bir şirket tarafından sunulan hizmetlerin içerikleriyle ilgili bir sorun olması halinde devletler karşılarında bir muhatap bulabilmektedirler. Bir ülke, güvenlik gerekçesi ile hassas gördüğü bölgelere ait görüntülerin kaldırılmasını veya kısıtlanmasını talep edebilir; bu talepler yerine getirilmediği takdirde diplomatik ya da hukuki yaptırım mekanizmaları devreye sokulabilir. Ancak *Bee Map* gibi merkezi olmayan ve blokzincir tabanlı bir yapıda durum çok daha farklıdır. Uygulamayı destekleyen kuruluşlara çeşitli talepler iletilse bile, merkezi bir otorite olmadığından veya merkezi yapı olsa bile blokzincirin merkezi olmayan mimarisi nedeniyle bu talepler büyük ölçüde karşılanamayabilir.



Resim 4. Ankara'da Bakanlıklar bölgesinde kapalı olan *Googlemaps* hizmeti



Resim 5. Genelkurmay Başkanlığı çevresinden *Bee Map* cihazları ile alınan kayıtlar

Resim 4'te, Ankara'daki devlet kurumlarının yoğun olduğu Bakanlıklar bölgesinde, *Googlemaps* sokak görünümü hizmetinin devre dışı bırakıldığı görülmektedir. Ancak Resim 5'teki *Bee Map* platformuna ait verilerde, Genelkurmay Başkanlığı çevresindeki sokaklardan

tam 11 kez görsel verinin (fotoğraf/video) sisteme yüklendiği tespit edilmektedir. Bedeli ödenerek bu güncel verileri içeren harita servislerinden isteyen herkes yararlanabilir.

Yüksek çözünürlüklü fotoğraflar ve video kayıtları kullanan DEPIN projeleri birlikte değerlendirildiğinde, *Spexi*, *Over* ve yazının başında değinilen Niantic firmasına ait *Pokemon Go* gibi uygulamalar, gerçek dünyadan üç boyutlu (3D) modeller üretmeye imkân tanıyan görsel veriler toplamaktadırlar. Örneğin *Spexi* uygulaması, birçok ülkede yasal olarak izin gerektirmeyen 250 gramdan hafif dronelar ile çekim yapan kullanıcılara, sisteme yükledikleri görüntüler karşılığında ödeme yapmaktadır. Bu görüntüler, çeşitli platformlarda 3D modellemelerde kullanılarak geniş çapta dağıtılabılır hâle getirilebilir. Türkiye'de drone uçurmak için Sivil Havacılık Genel Müdürlüğü'nden izin alınması zorunludur ve izinsiz uçuşlara yüksek para cezaları uygulanmaktadır. Ancak, ajanlık ya da keşif amacıyla bir bölgenin görüntülenmesi söz konusu olduğunda, bu cezalarının yeterince caydırıcı olmayabileceği de unutulmamalıdır.

Öte yandan mini ve mikro insansız hava aracı (İHA) tehditleri için Aselsan tarafından İHTAR¹⁶ ve Boğaziçi Savunma tarafından İLTER¹⁷ sistemleri geliştirilmiş olsa da bu sistemler stratejik noktalar ve önemli askeri ve kamu kurumlarının korunmasına yöneliktir. Önemli bir kişinin takip edilerek suikast düzenlenmesi veya kaçırılması için operasyon yapılabilecek herhangi bir lokasyonun yerden alınan görüntülerde üç boyutlu olarak modellenmesi hala mümkündür. Hatta *Over* uygulaması ile şu anda dünyanın farklı bölgelerinden haritalanmış alanlar üç boyutlu olarak gezilebilmektedir (Resim 6). Taksim Meydanı yönünden İstiklal Caddesine giriş bölgesini 3D olarak keşfederken cep telefonu ekranımdan aldığım video kaydını dipnotta verdiğim bağlantı¹⁸ üzerinden izleyebilirsiniz.



Resim 6. *Over the Reality* projesinin anasayfasına ait ekran görüntüsü

Benzer şekilde, Meta Quest 3 ve 3S sanal gerçeklik gözlükleriyle "Into the Scaniverse" uygulaması aracılığıyla dünya genelindeki kullanıcılar tarafından yüklenen modeller sayesinde pek çok bölge dünyanın öteki ucuna gitmeden sanal olarak keşfedilebilmektedir. Tüm bu sistemler, başlangıçta masum görünen veya turistik, eğlence ya da haritalama amaçlı

¹⁶ İHTAR Savunma Sistemi, https://www.wcdn.aselsan.com/api/file/SST_IHTAR_100_TR.pdf

¹⁷ İLTER Savunma Sistemi, https://www.bogazicisavunma.com/uploads/docs/1716913722_ilter-j350.pdf

¹⁸ <https://drive.google.com/file/d/1-zFTGesi2KqUGi-3jTNv5robs8c0K-YJ/view?usp=sharing>

tasarlanmış olabilir. Ancak toplanan veriler yeterince detaylı ise, bir bölgenin detaylı biçimde analiz edilmesi, hassas kişilerin takibi, hatta suikast ya da kaçırma gibi eylemlerin planlanmasında kötü niyetli kullanım riski taşımaktadır.

Fotoğraf ve video gibi iki boyutlu görsel verilerden, gerçekçi üç boyutlu (3D) sahneler oluşturmak artık oldukça kolaylaşmıştır. Bu alanda en çok kullanılan yöntem ise, yapay zekâ tabanlı algoritmalarından biri olan nöral parlaklık alanlarıdır (Neural Radiance Fields- NeRF). Bu algoritmayı içeren yazılımlar sayesinde, yalnızca 30-40 farklı açıdan çekilmiş fotoğrafla, bir nesne ya da binanın hacimsel modeli çıkarılabilmektedir. Genellikle bu görseller, modellenmesi yapılmak istenen nesne veya yapının çevresinden çekilen kısa video kayıtlarından elde edilir. Bir dakikalık video kaydından, modelleme için uygun 40 ila 100 arasında kare (fotoğraf) üretmek mümkündür. Daha hassas ve ölçüye dayalı modelleme için ise lazer tarayıcılar kullanılmaktadır. Bu yöntemle, hedef yapının boyutları gerçeğe çok yakın şekilde modellenenebilir ve buna dijital ikiz adı verilir. Üretilen bu dijital ikizler sayesinde, bir binanın ya da bölgenin içini ve çevresini sanal olarak dolaşmak, detaylı şekilde keşfetmek mümkündür. Örneğin, Resim 7'de, İskenderun Teknik Üniversitesi'nin dijital ikizinin oluşturulması sırasında elde edilen kütüphane binasının gerçekçi 3D modeli¹⁹ verilmiştir. Bu tür modeller; mimari analizden eğitim simülasyonlarına kadar çeşitli amaçlarla kullanılabilirken kötü niyetli kişilerce keşif ve planlama faaliyetlerinde de kritik bir zafiyet doğurabilir.

“Nöral parlaklık alanı” (NeRF) algoritmalarının sadece sivil değil, askerî uygulamalar için de kullanılmasına yönelik araştırmalar halihazırda yürütülmektedir. Bu kapsamda, ABD Ordusu Savaş Geliştirme Komutanlığı bünyesindeki Ordu Araştırma Laboratuvarı ile Pennsylvania Üniversitesi'ndeki GRASP (Algılama ve Kavrama) Laboratuvarı tarafından ortaklaşa gerçekleştirilen bir çalışmada, Philadelphia ve New York şehirlerinin dijital temsili modelleri oluşturulmuştur²⁰. Çalışmada geliştirilen bu 3D şehir modellerinin, şehir içindeki bilinmeyen bölgeleri keşfetmek ve hedef takibi yapmak gibi amaçlarla kullanılabileceği belirtilmiştir. Yapılan simülasyonlarda, bu yöntemle yaklaşık 300 hedefin tespit edilip takip edilebildiği gösterilmiştir. Modellemeler, açık sokak haritası verilerinden (OpenStreetMap) alınan RGB ve derinlik görüntüleriyle eğitilmiş bir simülatör yardımıyla gerçekleştirilmiştir. Araştırmacılar, sahnelerin yeniden yapılandırma kalitesinin, özellikle izleme ve operasyonel görevler açısından kritik bir faktör olduğunu da vurgulamıştır. Bu araştırma, yeterli sayıda fotoğraf ve video verisinin toplanması durumunda, şehirlerin dijital temsilleriyle askerî operasyonlara - özellikle de meskûn mahal çatışmalarına- destek verilmesinin mümkün olduğunu açıkça ortaya koymaktadır. Ayrıca 3D modeller görsel konumlandırma amacıyla (Visual Positioning Systems-VPS) da kullanılabilmektedir. DEVCOM, GPS sinyalinin kaybedilmesi durumunda devreye giren VPS sistemini 2023 yılında test etmiştir²¹.

¹⁹ İskenderun Teknik Üniversitesi Dijital İkiz çalışmasını deneyimlemek için bağlantı:

https://live.arrival.space/12194264_1584

²⁰ Christopher D. Hsu ve Pratik Chaudhari (2024). Active Scout: Multi-Target Tracking Using Neural Radiance Fields in Dense Urban Environments. <https://arxiv.org/html/2406.07431v1>

²¹ https://www.army.mil/article/268390/aviation_missile_center_tests_new_visual_navigational_technology

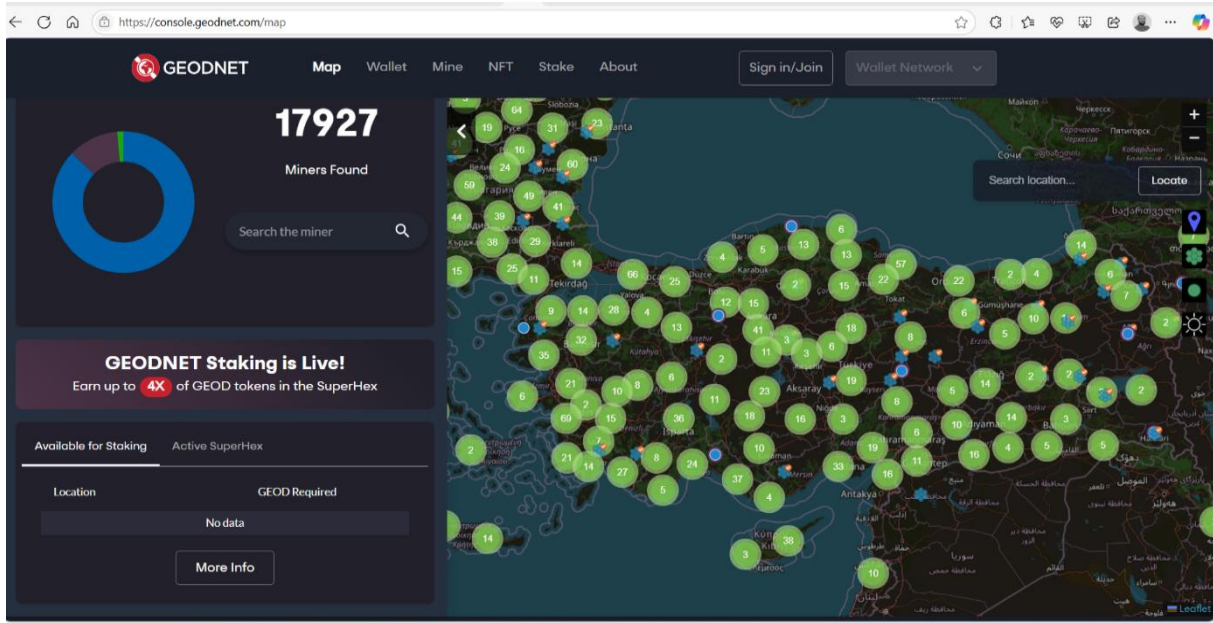


Resim 7. İskenderun Teknik Üniversitesi, Dijital İkiz projesi kapsamında üretilen 3D model

GeodNet, sabit konumlara yerleştirilen istasyonlar aracılığıyla oluşturulan Gerçek Zamanlı Kinematik (RTK) ağlar sayesinde, geleneksel GPS sinyallerini santimetre düzeyinde hassasiyete ulaştıran bir projedir. Resim 8, Türkiye’de kurulu RTK yer istasyonlarının konumlarını ve sayılarını; Resim 9 ise bu istasyonların kapsama alanlarını göstermektedir. Resim 9’da verilen haritada yer alan renkli bölgeler, GPS sinyallerinin düzeltme hassasiyetine göre sınıflandırılmıştır. Koyu yeşil alanlar, kapsama alanı dışında kalan ya da yeterli düzeltmenin yapılamadığı bölgeleri, açık yeşil alanlar, yaklaşık 10 cm hassasiyete, parlak yeşil alanlar ise 2 cm hassasiyete kadar GPS iyileştirmesinin yapılabildiği bölgeleri göstermektedir.

GeodNet’in sağladığı bu ultra hassas konumlama kabiliyeti, öncelikle tarım ve lojistik sektörlerinde kullanılan dronelar, otonom kara araçları (sürücüsüz traktörler, robotlar, otonom otomobiller) gibi sistemlerin daha verimli ve güvenli şekilde çalıştırılması amacıyla geliştirilmiştir. Ancak bu altyapının yalnızca sivil amaçlarla sınırlı kalmayabileceği de göz önünde bulundurulmalıdır. RTK ağları, askerî ve istihbarat faaliyetlerinde kullanılabilecek herhangi bir aracın konumlarının daha hassas şekilde belirlenmesi ve yönetilmesi açısından da kritik bir potansiyel taşımaktadır. Örneğin; *Helium* ağına bağlı bir GPS izleyici taşıyan bir hedef, RTK destekli *GeodNet* sistemleri ile santimetre hassasiyetinde takip edilebilir. Bu hassas konum verileri, İran’daki üst düzey bilim insanlarına veya askeri liderlere yönelik suikast saldırılarında olduğu gibi, hedeflerin evleri veya bulundukları noktalar esas alınarak son derece başarılı operasyonlar düzenlenmesine imkân tanıyabilir. Kısacası, sivil kullanım amacıyla geliştirilen konum iyileştirme sistemleri, kötü niyetli aktörlerin elinde yüksek hassasiyetli hedefleme altyapılarına dönüşebilir.

GeodNet ve *Helium* gibi DEPIN projelerinde kullanılan fiziksel cihazlar yalnızca topladıkları verilerle değil, aynı zamanda siber saldırılara açık yapılarıyla da güvenlik riski oluşturmaktadır. Bu cihazlar, temel olarak kripto para madenciliği ve veri aktarımı için tasarlanmış olsalar da yeterince korunmadıkları takdirde kötü niyetli kişiler tarafından uzaktan erişilerek manipüle edilebilirler. Örneğin, *Helium* cihazlarında bulunan LoRaWAN modülü, farklı LoRa ağlarına bağlanma yeteneğine sahiptir. Bu durum, cihazın sadece *Helium* ağıyla sınırlı kalmayıp başka ağlarla da iletişim kurabilmesi anlamına gelir. Ayrıca bu cihazların birçoğunda, küçük ama güçlü bir bilgisayar olan Raspberry Pi gibi donanımlar yer almakta ve bu donanımlar dışarıdan erişim sağlandığında farklı yazılımların çalıştırılmasına olanak tanımaktadır. Yani teoride, bir *Helium* cihazı ele geçirilerek arka planda paralel bir casus yazılımın çalıştırılması mümkündür. Bu sayede, cihazın orijinal işlevi devam ederken aynı zamanda başka ağlara veri gönderebilir veya başka bir cihazla koordineli şekilde hareket edebilir.



Resim 8. GeodNet projesine ait Türkiye’de kurulu olan RTK cihazların dağılımı ve sayıları



Resim 9. GeodNet RTK cihazlarının Türkiye’deki doğruluk seviyelerine göre kapsama alanları

Değerlendirme ve Öneriler

Merkezi olmayan fiziksel altyapı ağları (DEPIN) projelerinin doğrudan milli güvenliğe tehdit oluşturmak üzere geliştirildiği şeklinde bir genelleme yapmak doğru değildir. Aslında bu projelerin büyük kısmı, hayatımızı kolaylaştırmak, iş süreçlerini daha verimli ve kaliteli hâle getirmek amacıyla geliştirilmiştir. Ancak her teknolojik ürün gibi DEPIN projeleri de öngörülemez kullanım senaryoları nedeniyle askeri, stratejik veya istihbari riskler barındırabilmektedir. Bu notun temel amacı, özellikle son yıllarda hızla yaygınlaşan DEPIN projelerinin, milli güvenlik perspektifinden taşıyabileceği potansiyel risklere dikkat çekmektir. Verilen örnekler, herhangi bir projeyi karalamak ya da kullanıcılarını zor durumda bırakmak amacıyla değil, güvenliğimize ilişkin olası tehditleri tartışmaya açmak için paylaşılmıştır.

Şüphesiz ki bu projeler tamamen yasaklanarak da güvenlik sağlanabilir; ancak bu yaklaşım, Web 3.0 teknolojilerinin ülkemizde gelişmesini engelleyecek ve Türkiye'nin küresel dijital dönüşüm yarışında geride kalmasına neden olabilecektir. Unutulmamalıdır ki burada adı geçen *Helium*, *GeodNet*, *Over*, *Bee Map* gibi projeler, ülkemize büyük teknolojik ve ekonomik katkılar sağlayabilecek potansiyele sahiptir. Bu nedenle, yasaklayıcı değil, denetleyici ve yönlendirici bir yaklaşımla hareket edilmesi daha uygun olacaktır. Bu doğrultuda hayata geçirilebilecek bazı politika önerileri aşağıda sunulmuştur:

- DEPIN altyapılarının izlenmesi ve denetlenmesi gerekmektedir. Ülke sınırları içerisinde kurulan DEPIN ağları düzenli olarak takip edilmeli, güvenlik riski taşıyan projeler için gerekli önlemler alınmalıdır. Cihaz sahiplerinden kayıt ve lisans talep edilerek cihazlara uzaktan erişimle müdahale imkânı sağlayan yazılımlar zorunlu kılınabilir. Yüksek risk taşıyan projeler içinse yasaklama ya da sıkı denetim uygulanabilir.
- Diğer devletlerin DEPIN projelerine ilişkin tutumları ve stratejileri izlenmelidir. Örneğin, *Helium* ve *Bee Map* projeleri İsrail'de oldukça yaygınken neden *GeodNet* ağına ait tek bir RTK cihazının dahi bu ülkede bulunmadığı araştırılmalıdır. Farklı ülkelerin bu teknolojilere karşı gösterdikleri yaklaşımlar stratejik planlama açısından yol gösterici olabilir.
- DEPIN donanımlarının tedarik zinciri kontrol altına alınmalıdır. Bu cihazları yurt içinde üreten veya yurt dışından ithal eden firmalar kayıt altına alınmalı, gerekirse ithalat ve satış süreçleri özel izinlere tabi tutulmalıdır.
- Kullanıcı farkındalığı artırılmalıdır. DEPIN cihazlarını gelir amacıyla satın alan bireyler, cihazlarının yönetimi ve potansiyel güvenlik riskleri konusunda bilinçlendirilmelidir. Bu amaçla eğitim, bilgilendirme ve kontrol mekanizmaları kurulmalıdır.
- Mini ve mikro İHA tehditlerini engellemek amacıyla geliştirilen savunma sistemleri sürekli güncellenmeli ve yaygınlaştırılmalıdır. Ancak yapay zekâ destekli, VPS (Görsel Konumlandırma Sistemleri) ile çalışan insansız araçların, radyo ve GNSS karıştırıcı sistemlerden etkilenmediği unutulmamalıdır. Artık bina içlerinde dahi GPS olmadan konumlandırma yapılabilmektedir.
- Kritik bölgelerin konumu stratejik olarak yeniden değerlendirilmelidir. Sokak ve şehir görsellerinin yüksek çözünürlüklü kaydının önüne geçmek artık mümkün değildir. Bu yüzden, stratejik noktalara/kurumlara ait görsellerin (video ve/veya fotoğraf) alınarak modellenmesi ve potansiyel senaryolar ile çalışılmasının önüne geçilebilmesi için bunlar şehir dışına veya yer altına taşınmalıdır. İsrail'in savaş anında tüm operasyonları sürdürebilmek için yer altına inşa ettiği Zion Kalesi, bu yaklaşıma bir örnektir.
- Türkiye DEPIN projelerini aktif olarak değerlendirmelidir. Sadece savunma değil, gerektiğinde istihbarat ve güvenlik amaçlı olarak bu altyapıların nasıl kullanılabileceği araştırılmalı, yerli DEPIN çözümleri teşvik edilmelidir.