COVID-19 SALGINI SONRASI DÖNEMİN DİJİTAL KODLARI VE SİBER GÜVENLİK

Oğuz YILMAZ

Yeni tip koronavirüsü nedeniyle dünyanın çalkantı içine girdiği 2020 sonrasında dünyanın gelişimi büyük kırılmalara gebe görünmektedir. Dünya ekonomisi Nisan-Mayıs itibarıyla %20'den fazla yavaşlamış, birçok ülkede üretim ciddi derecede azalmıştır. Ulaşım durma noktasına gelmiş, ülkeler giriş ve çıkışlara kapanmıştır. İnsanlar evlerden çıkmamakta ve buna rağmen iş ve hayatlarının gereği olan faaliyetleri yapmaya çalışmaktadır. Evlerden ya da ofislerden, ama biraraya gelmeden, uzaktan yürütülen birlikte iş yapma eğilimi artmaktadır. Kamu faaliyetleri ve vatandaş ile iletişim de yine uzaktan yerine getirilmektedir.

Yeni tip koronavirüsün hayatımızı nasıl etkilediği ve teknolojiyi hayatımızda nereye koyduğu bu salgın sonrası incelenmeye muhtaçtır. Bu inceleme; siyaset, iş, finans, devlet-vatandaş ilişkisi, güvenlik, sağlık, bilişim, sanayi, ticaret boyutlarıyla yapılmalıdır.

Teknoloji ve Sağlık

Hastanelere gitmenin gittikçe ötelendiği dönem, insanları hastalık belirteçlerinin neler olduğuna ve bunları kendinde yoklamaya yönlendirdi. Elbette sadece belirteçler ile spesifik bir hastalık tanımlamak mümkün değildi. Diğer yandan, örneğin Covid-19 belirteçlerinden bir kısmı olanlar dahi hastanelere gitmekten imtina ettiler. Bununla beraber diğer sağlık sorunları nedeniyle de hastaneye gidişlerin önü kesilmiş oldu. Bu aslında her salgın döneminin bir karakteri olarak algılanmalıdır.

Hastanelere gitmenin geciktirilmesi ile insanlar bu teşhisleri kendi kendilerine yapmalarına imkân verecek aygıt talebi oluşturdular. Akıllı aygıt ve giyilebilir teknolojilerin tasarımları da hemen yönlerini bu talebe çevirdiler. Bundan önce hastanelerde göreve özel aletler olarak karşımıza çıkan EKG gibi cihazlar, saatlerin içine bir fonksiyon olarak girmeye başladı. Sadece bu da değil. Örneğin termometre, kalp atış ölçeri ve hatta kandaki oksijen satürasyonunu ölçen saatler dahi piyasaya giriyor. Bu arz ve karşısındaki talep, artık insanların kendi sağlıklarını kendilerinin analiz ettiklerini, erken teşhis imkânlarını hastaneye gitmeden sağlamak istediklerini ifade ediyor.

Bu durum, tele-teşhis (*tele-health*) kitlerinin kabullenilmesini de hızlandırıyor. Özellikle yaşlıların kullanımı öngörülerek bir süredir geliştirilen bu kitler, en temel teşhis araçları olan tansiyon, ateş, nabız, şeker seviyesi gibi ölçümleri bireyin evde yapmasına olanak veriyor. Teşhislerin muhatap doktora çevrimiçi iletilmesiyle de teşhis ve tedavi netleşiyor (*tele-medicine*). İşte bu kitlerin gittikçe daha yaygınlaştığı bir sürece giriyoruz. Her ailenin evinde bulunan ve aile hekimine irtibatlı sistemler çok uzak ihtimaller değiller.

Nesnelerin interneti teknolojisi ile sağlık alanı da kesişmektedir. Ölçüm cihazlarının verileri merkezî bir bulut sistemine iletmesi ile her kişi ve onu takip edenler bu ölçümleri görebiliyor. Bu sayede büyük bir faydanın daha önü açılıyor. Tek bir yerden tüm ülkedeki insanların ölçtüğü ateş değerlerini görebildiğinizde ateş belirtili bir salgının yayılımını ve odak coğrafî alanı da görme imkânı doğmuş oluyor. İşte sağlıkta büyük veri analizi diyebileceğimiz bu yöntem ile sadece ateş değil, tüm sağlık başvuru ve teşhis bilgileri işlendiğinde elde edilebilecek bilgilerin, tüm ülke çapında, anomalinin ve anomali kaynaklarının tespiti için ne kadar kıymetli olacağı görülebilir. Güncel salgın sürecinde dahi sokak bazına inen coğrafî analizler ile salgın kaynaklarının ve süper taşıyıcıların bulunması mümkün olduğu kadar, filyasyon ve tarama ekiplerinin bir alana odaklanması da mümkün olabilmektedir.

Diğer yandan yapay zekâ da büyük bir genişleme alanı sunmaktadır. Örneğin, radyoloji görüntülerine göre temiz, müspet, menfi görüntülerin öğretilmesi ile eğitilen bir yapay zekâya herhangi bir radyoloji görüntüsü verildiğinde bunun niteliği anında alarmlanabilecek, hatta radyoloji raporları otomatik şekilde yazılabilecektir. Çinli dev *Alibaba* şirketi de bu alanda yatırım yaptığını belirtmektedir. Alibaba, güncel çalışmasında tıbbî tahlil verileri ve akciğer taramaları verilen bir yapay zekâ ile Covid-19 teşhisi yapabilmektedir. Bir diğer örnekte de ABD'de bulunan MIT Üniversitesi, insan sesinden yeni koronavirüs etkilerini seçip yalnızca bir ses kaydından teşhis üzerinde çalıştığını belirtmektedir.

Yapay zekânın kullanılabileceği alanlar bunlarla da sınırlı değildir. Bir ilacın bir tür patojen üzerinde etkisinin olasılığı, geçmiş ilaç ve etken maddelere göre eğitilmiş bir yapay zekâ ile çok daha hızlı tahmin edilebilecektir. Daha hızlıca hayvan ve insan testlerine ilerlenebilecektir.

Bunlarla beraber biyoteknolojinin de geleceğin millî güvenlik alanı olduğunu görmek gerekir. KBRN olarak tabir edilen kimyasal, biyolojik, radyolojik, nükleer silahlar arasında belki de en sinsi olanının biyolojik silahlar olduğu fark edilmelidir. Bunlara karşı savunmada olduğu kadar, hastalıkların tedavisinde de biyoteknolojinin önemi bundan sonraki dönemde gecikmesiz kavranacaktır.

Bu anlamda, üzerinde çalışılması gereken başlık önerilerinden birkaçı şu şekilde listelenebilecektir:

1- Biyolojik ve biyoteknolojik amaçlarla, genetik materyal değiştirme teknolojisi üzerinde çalışan bir laboratuvarın "yanlışlıkla" ya da "yönlendirilmiş hatayla" bir biyolojik tehdide ön ayak olması olasılığı dünya çapında yönetilmelidir. Nasıl uluslararası nükleer materyal üretimi sıkı bir şekilde denetleniyorsa, tüm biyoteknoloji çalışma-

larının da yeterli seviyede denetime tabi olacağı, ulusal ve uluslararası bir model güçlendirilmelidir.

2- Yakın tarihte Türk vatandaşlarının genetik materyallerinin topluca ele geçirilme çabalarına rastlanmış, bunların bir kısmı başarılı da olmuştur. Bu nedenle yurtdışından edinilen, aşı ve benzeri, tüm halka uygulanması muhtemel uygulamalarda bir "biyoteknolojik/genetik tehdit analizi" şarttır.

3- Sağlık en az gıda kadar kendine yeter bir alan olmalıdır. Sadece bilinen pratiklerin iyi uygulandığı hastanelerle değil, hastalığı önleme aracı aşılar, tedavi ilaç ve teknolojileri gibi alanlarda da kendine yeterlik hedeflenmelidir.

4- Patent ve diğer fikrî mülkiyet hakları, ülkelerin sağlık üzerinde münferit gelişmelerini engellemektedir. ABD'de metotlar dâhil olmak üzere fikrî mülkiyet için liberal bir yaklaşım varken, Avrupa'da tıbbî metotlar doğrudan patentlenebilir değildir.[1] Ancak Avrupa'da da metotlar, ilaçlar ve ürünler için dahi patentleme için, daha önce tıbbî amaçla kullanılmayan bir ürünün "ilk tıbbî kullanımı" ya da amaç-limitli-ürün-iddiası gibi çok geniş arka kapılar bulunmaktadır. Önümüzdeki dönemde, aşı, ilaç, tedavi yöntem ve teknolojilerinin patentlenebilirliği konusu tartışmaya açılmalıdır.

5- Ülkemiz kısa süre içinde solunum cihazı üreterek önemli bir başarı sergilemiştir. Ancak, solunum cihazlarının tıbbî teknolojiler arasında alt-orta teknoloji alanında olduğu unutulmamalıdır. Orta ve yüksek sağlık teknolojisi alanında çalışmaların ilerletilmesine hâlen büyük ihtiyaç vardır. Ülkemizde bu çalışmaların devlet güdümünde Aselsan gibi daha önce savunma alanında başarı hikâyesine sahip şirketler tarafından yapılması ile ilgili bir irade oluştuğu görülmektedir. Bu noktada doğru politika, tek bir şirketin desteklenmesi yerine rekabetçi, yani hedefe doğru eş zamanlı koşan alternatiflerle desteklenmesi şeklinde olacaktır. Rekabet, hem yüksek kalite hem de yedeklilik getirecektir. Dünya pazarı birden fazla Türk alternatife fazlasıyla açıktır.

Teknoloji ve Devlet-Vatandaş İlişkisi

Covid-19 salgını ile beraber halk evlere sığınmıştır. Kamu işlevleri için kamu kurumlarına gitmek yerine uzaktan bu işleri halledebilme talep edilmektedir. Türkiye Cumhuriyet e-Devlet Kapısı bu noktada en mahir araç olmaktadır. Tüm vatandaşların girebildiği sistemde bundan sonra çok daha geniş yelpazede uygulamalar bulunabilecektir.

Vatandaşların evlerde olması, kendilerine interneti ve sosyal medyayı bir arabirim yapmalarını getirmiştir. Bu anlamda sosyal medya, bir iç kamu diplomasisi aracı olarak bundan önce olmadığı kadar öne çıkacaktır.

Sosyal medyanın ana mecra hâline gelmiş olması, sadece vatandaş ve devlet tarafında değil, bunlara tehdit unsurlar tarafında da gerçekleşmiştir. Sosyal medya, bölücü, yıkı-

1 Patentability of Medical Methods in Europe | European IP Blog", Finnegan | Leading Intellectual Property Law Firm, 2020. [Çevrimiçi]. Adres: https://www.finnegan.com/en/insights/blogs/european-ip-blog/patentability-of-medical-methods-in-Europe.html. [Erişim: 13 Mayıs 2020].

cı, sinsi terör örgütleri tarafından da yoğun şekilde kullanılmaktadır. Gerek PKK gerekse FETÖ terör örgütlerine ait sosyal medya hesapları Atatürk, TC, adalet gibi maskelerle sosyal medyada kendilerini gizlemekte, psikolojilere hitap eden mesajlarla bu örgütlerin görüşlerini yaymaktadır. Bundan sonraki dönemde de bu çaba ve yöntemlerin güçleneceği görülmelidir.

Devletlerin vatandaşlarının aşılanması noktasında hassasiyeti güçlenecektir. Özellikle son dönemlerde yaygın olan, ailelerin aşı yaptırmama seçimlerine karşı devletler daha zorlayıcı olacaktır. Bu anlamda üzerinde çalışılması gereken başlık önerilerinden birkaçı şu şekilde listelenebilecektir:

1- İnternet mecralarındaki terör tehditlerine karşı duruş yine sosyal medya üzerinden olacaktır. Ancak bu çalışmanın siyasî partiler ya da vatandaşlar yanında devlet aygıtları tarafından da yürütülmesi gerektiği açıktır. Devlet aygıtları bundan önceki dönemde ağırlıklı olarak bu hesapların arkasındakilere ulaşarak, polisiye ve adlî yöntemlerle bertaraf etme yoluna gitmiştir. Artık bu yeterli değildir. Tehditkâr hesapların arkalarındaki unsurlar bulunana dek, bizzat devlet kurumları açacakları sayfalar ile karşı algı yönetimi yapmalıdır.

2- Sosyal medya mecralarının Türkiye Cumhuriyeti Devleti ve mahkemelerine muhataplıkları çevreleyici şekilde sağlanmalıdır.

3- Kişilerin kimlik tespiti ve aşı takibi gibi amaçlarla yonga (çip) uygulamalarının önerileceği teorileri ciddiye alınmalı, bunlara karşı insan onuru, özgürlüğü ve diğer anayasal haklarını koruyacak bir duruş oluşturulmalıdır. Bu noktada sadece vücut yongaları değil, yüz tanıma, parmak izi, avuç izi, retina izi gibi biyometrik kimliklendirme araçlarının durumu da analiz edilmelidir.

4- Çin'de renk yelpazesi uygulaması ile salgın hastalık durumuna göre bir renk kodu alan vatandaşların hangi ortama girip girmeyecekleri denetlenmektedir. Şu an için ülkemizde bu durumu gerektirecek bir acil durum oluşmamışsa da, gelecekteki daha büyük salgın olasılıkları göz önünde tutularak salgın eylem planları güncellenmeli ve ilgili kurumların büyük bir ahenkle yapabilecekleri şekilde organlara aktarılmalıdır.

Teknoloji ve İş, Finans, Sanayi, Ticaret

İş dünyası yeni koronavirüs salgını ile çok hızlı şekilde adapte olarak muhtelif uzaktan çalışma yöntemlerini kullanmaya başladı. Bu pratikler şu şekilde özetlenebilir:

- *Bilgi depoları*: Evlerden ya da belli bir mesafeyle çalışan şirketler, daha önce muhtelif kağıt evraklarda bulunan bilgilerin ortak ulaşılabilir olması için çevrimiçi diskler ve doküman yönetimi sistemleri kullanılmaya başladı.

- *Uzaktan toplantılar*: Hem birkaç kişilik toplantılar hem de birebir görüşmeler de olduğu kadar konferanslar için dahi çevrimiçi platformlar yoğun şekilde kullanılmaya başlandı. Bu gelişimin daha hızlanacağını öngörmek mümkündür.

- *Uzaktan çalışma*: Bu süreç ile beraber işi elverenler anında uzaktan çalışmaya geçtiler. Uzaktan çalışma doğası gereği etkileşimin daha az olduğu bir çalışma tipi olsa da bu bir yandan da verimlilik anlamına gelebilir. Etkileşim de gerektiği kadar bilişim iletişim araçları ile yapılabilmektedir.

Bir coğrafî konuma bağlı olmaksızın da çalışabildiğini gösteren bu reel dönem ile yabancı iş gücünün uzaktan istihdamının önü daha açılmış olacak, iş piyasasının coğrafî sınırları daha belirsizleşmiş olacaktır. Bu işsizliğin artışını destekleyebilecek, ancak diğer yandan şirketlerin rekabetçiliğini de destekleyecektir.

Bununla beraber özellikle ortak kullanılan teknolojik aygıt ve araçlar için dokunmadan işletim önem kazanmaktadır. Bu anlamda temassız ödeme sistemleri, ses ile komut verilen kiosk ve benzeri ortak kullanım araçları, göz ya da vücut hareketleri ile yönlendirilen makine-vizyon (*machine vision*) arabirimlerin öne çıkacağı söylenebilir.

Evden çalışma ve evde kalma deneyimleri elektronik ticarette de bir dönüşüm getirmiştir. Bu dönüşümde özellikle market alışverişlerinin de evden yapılmasıyla beraber e-ticarette yeni bir segment doğmuştur denilebilir.

Her ne kadar bilgisayar ve telefon tabanlı iş yapan kurumlar için uzaktan çalışma mümkün olsa da, fabrikasyon üretim yapan ya da malzeme ile çalışması gerekilen işlerde bu mümkün olmamıştır. Fabrikaların çalışma ortamları imkânlar dâhilinde salgın önlemlerine göre düzenlenmeye ve vardiya sistemleri işletilmeye başlansa bile, durum bir arz sorununa yol açmıştır. Bu arz sorunu gelecekte olası durumlarda insana daha az bağımlı çalışan fabrikalar fikrini güçlendirmektedir.

İnsansız ve karanlık fabrikalar olarak da tanımlanan fabrikaların çalışması için tezgâh, makine ya da bantlarda insana neredeyse ihtiyaç duymamaktadır. Üretim, ışıklandırma ya da iklimlendirme de gerekmeyen ortamda, robot kollar, makineler, tezgâhlar ve bantlar aracılığı ile yapılmakta, her bir sistem, tezgâh, fabrikadaki sensörler, nesnelerin interneti ile tam iletişim hâlindedir. Bu fabrikalar yalnızca kendi içinde değil dışarı ile de iletişim hâlinde olarak, örneğin tedarik zinciri üzerinde hammadde siparişlerini verebilmekte, fabrikaya geliş zamanlarını takip ederek üretimi planlayabilmektedir. İşte her fiziksel sistemin "siber" özellik kazandığı bu yapılar, "siber fiziksel sistemler" olarak isimlendirilmektedir.

Sanayi 4.0 akımı için 3 boyutlu yazıcılar da ana unsurlardandır. Yeni bir ürün üretimi için 3 boyutlu yazıcıların kullanımı ile prototipleme çok hızlı yapılabilmekte, yeni bir ürünün üretiminin benzetimi de yalnızca bilgisayarda çalıştırılacak bir yazılım aracılığı ile yapılabilmektedir. Böyle bir fabrikasyonda, fabrikaların insansız hâle gelmesi elbette iş gücü piyasasında devrim niteliğinde etkilere de yol açacaktır.

Bu anlamda üzerinde çalışılması gereken başlık önerilerinden birkaçı şu şekilde listelenebilecektir:

1- İnsansız fabrikalarla beraber işçilerin geleceğini düşünmek gerekmektedir. Öngörülebilir bir meslekî dönüşüm gerçekleşecektir. Bu anlamda işsizlik fonu, bu hareket için hazır tutulmalıdır.

2- 4'üncü sanayi devrimi ile beraber bazı yeni mesleklerin de oluşması beklenmektedir. Veri bilimciliği, robot koordinatörlüğü, endüstriyel programcılık, 3 boyutlu yazıcı uzmanlığı, kullanıcı arayüzü tasarımcılığı, her alanda bilişim uzmanlıkları, robot ve kontrol mühendisliği, e-ticaret uzmanlığı, siber güvenlik uzmanlığı gibi bu dönemle yükselecek meslekler için yönlendirilmiş politika çalışmalarına hız verilmelidir.

3- Sanayi 4.0 buna erken geçen ülkelerde verimlilik yükselişi ve maliyetlerin düşmesi sayesinde çok daha rekabetçi fiyatlar olarak bizi de etkilemeye başlamıştır. Kaçınılmaz şekilde, çok daha ucuz mal sağlayabilen küresel tedarikçilere karşı yerli üreticilerin tutunabilmesi, ancak akıllı fabrikalara doğru ilerleme ve çeşitli gümrük bariyerleri ile olabilecektir. Her iki eylem için de politika çalışmaları gerekmektedir.

4- Üretim sürecinin tedarik zinciri incelenmelidir. Tedarik zincirindeki olası yurt dışı kaynaklı bozulmalar hâlindeki durum analiz edilmeli ve ilgili başlıklardaki malzeme, hammadde üretiminin ülkede yapılması için politikalar yönlendirilmelidir.

5- 1 milyon istihdam projesi gibi projelerle atılan adımlarla gerekli kalitede teknik personel yetiştirilebilirse, yabancı şirketlerde maaşlı ya da bağımsız çalışacak bu personeller, Türkiye için bir döviz kaynağı hâline gelebilecektir.

6- Salgın döneminde sağlığın gereği olarak karar almayı engelleyen unsurlardan birisi haklı olarak ekonomik gerekçeler olmuştur. Benzer durumlar için ülkemizin işsizlik ve acil durum fonları güçlendirilmelidir.

7- Kullanımı çok artan e-postalar ve çevrimiçi diskler (*drive*) nedeniyle birçok şirket ve kurumun verisi bu platformlar üzerine taşınmaktadır. En hızlı şekilde yerli platformların oluşması ve güçlenmesi için rekabetçi ortam sağlanmalıdır. Mevzuatlarla yalnız kamu değil tüm vatandaşların verileri yurtiçinde tutulmalıdır.

8- Çoğunluğu Çin ve Amerika menşeli sesli ve görüntülü görüşme platformları üzerinden geçebilecek ses verilerinin belirlenmiş anahtar kelimelerle izlenebildiği teknolojiler olduğu düşünüldüğünde, bu platformların yerli olmaması büyük sorun oluşturacak görünmektedir. Bu platformların şu amaçlarla yerli olması için ortam oluşturulmalıdır: Birincisi, görüşmenin noktadan noktaya akışında, trafik hiçbir şekilde yurt dışına çıkmamalıdır. Tüm sunucu sistemler de yurt içinde olmalıdır. İkincisi, bu uygulamaların yazılımları burada geliştirilmeli, istenirse Türkiye'de güvenlik anlamında sertifikasyona tabi tutulabilmelidir. Üçüncüsü de, bu iş için Türkiye'de tüketiciler bir para harcayacaksa, bu TL olmalı ve Türkiye'de kalmalıdır.

9- Türkiye'de uygulanmakta olan e-ticaret müşterilerini koruma mevzuatının uzaktan market alışverişlerinde de müşterileri koruyup korumadığı analiz edilmelidir.

10- Yapay zekâ kullanan sistemlerin yaygınlaşması ile beraber bu sistemlerin aldığı eylem kararlarının sonuçlarının yol açtığı hukukî durumların analiz edilmesi ve kanunların bunları da kapsayacak hâle gelmesi gerekmektedir.

11- Kripto para olarak tabir edilen, sınırlı bir algoritma ve kriptoloji kaynağına dayanan

para birimleri hakkında, vatandaşların kullanımı, mali suçların engellenmesi, kripto para üretimi, kripto para regülasyonu başlıklarında çalışmalar yürütülmelidir.

12- Nakit kullanımının azalacak olması ve tüm harcamaların kayıt içi sistemlere doğru kaymasıyla beraber vergilendirme modellerinde değişiklikler beklenebilecektir. Bu rüzgârın da kullanılmasıyla beraber, teşvik edici vergilendirme şemaları ile halk kayıt içi harcama yöntemlerini kullanmaya teşvik edilmelidir.

13- Halkın imkânları dâhilinde kendi ve yöresinin ihtiyaçları için yerelde bitki yetiştirmesi ve gıda üretimi için modeller geliştirilmelidir. Herhangi bir salgın anında kapanan bir ilde, özellikle ana gıdalar olmak üzere kendine yeter bir üretim-tüketim dengesi önemlidir. Seracılık politikaları da bölgesel değil, tüm ülkeyi kapsayacak şekilde tasarlanmalıdır.

14- İnsandan bağımsız yenilenebilir enerji ile ülke coğrafyası içinde olabildiğince eşit dağılmış bir enerji üretim kapasitesinin oluşturulması gereklidir.

15- Ülkemiz, arz istikrarını sağlamaya odaklanmalıdır. Her bir ihtiyaç kaleminde "ulusal stok" kavramı ve "yerli üretim" ilkesi güçlenmelidir.

Teknoloji ve İnsansız Savunma

Bu başlık iki ana şey vaat etmektedir. Bunlar, geleceğin salgınları sırasında olabilecek savaşlara hazır olmak ve insansız savunma ile can kayıplarının en aza indirgenmesidir. Günümüzde fiziksel mesafenin ana korunma önlemi olduğu bu salgında, bu önlem askeriyenin birlikte yaşama kültüründe çok kolay uygulanamayacaktır.

Günümüzde, robotik, gömülü sistemler, güvenilir haberleşme, yapay zekâ, optik ve sensör teknolojilerinin gelişmesi insansız çalışan araçların gelişimine imkân sağlamıştır. Uzaktan kontrollü ya da otonom olan bu sistemler hem sivil hem de askerî alanlarda yer bulmuşlardır.

Sınır güvenliği noktasında da oldukça geniş sınırlara sahip olan ülkemiz, yıllardır sürdürdüğü insanlı sınır güvenliğinin ötesinde bir başarı için duvarları tercih edilmiştir. Duvarlara ek olarak tesis edilecek insansız gözlem kulesi projeleri yürütülmektedir. Bu projelerin bundan sonra hızlanacağını görmek mümkündür.

Bu anlamda üzerinde çalışılması gereken başlık önerilerinden birkaçı şu şekilde listelenebilecektir.

1- Yalnızca hava değil, su ve kara araçlarında da insansız sistemlerin geliştirilmesi için politikalar oluşturulmalıdır.

2- Tüm dünya için korona sonrası dönem ekonomik krizle beraber anılmaktadır. Bu noktada teknolojinin yardımıyla insana en az bağlı ve kalıcı sistemlerin oluşturulması yönünde politikalar gereklidir.

3- Benzer ve daha güçlü salgınlar halinde yaşanabilecekler, tatbikatlar halinde ele alınarak, savunma, sivil savunma ve kolluk kuvvetleri için protokoller gözden geçirilmelidir.

Dijitalleşme ve Uzaktan Siyasî İletişim

El sıkışma ve insana dokunarak siyaset zaten bir dönüşüm içerisindeydi. Bu dönüşüm teknoloji ile itekleniyor gibi görünse de, aslında siyasetin dönüşümü için zorlayıcı etken teknolojinin kendisi değildir. Siyasetin tarafı olan ve yeni doğumlarla daha da değişen nesil için vitrin, iletişim mecrası ve itibar tartısı gittikçe sayısal ortamlar halinde gelmeye zaten başlamıştı.

Yeni tip koronavirüs salgını da, gençler ve erken yetişkinler için internet, dijital tv ve sosyal medya kullanımını artırmıştır. Bununla beraber orta yaşlı ve yaşlı kesim de sosyal medya ile tanışmak için evde kalma sürecini bir zorunlu fırsata çevirmiştir. Dolayısıyla dijital göçmen diye tarif edilen, dijitalleşmemiş dünyada doğup, sonradan dijital dünyaya gelenlerin sayısı da artmıştır. Sosyal medya eskiden olduğundan daha farklı şekilde, orta yaşlı ve yaşlılar için de bir mecra hâline dönüşmektedir. Salgın iletişimi için Sağlık Bakanlığı'nın infodemi (info+pandemi, salgın bilgilendirmesi) mecrası olarak internet ve sosyal medyayı kullanması da dijital göçü hızlandırmıştır.

Salgın süresinde sosyal medya platformlarının birbirlerine göre ayrışmaları da dikkat çekicidir. Tartışmanın içinde olmak isteyenler *Twitter*'ı tercih ederken, hastalık duymak istemeyen ve eğlenceli ve magazin içerikleri tercih edenler için mecra *Instagram* olmuştur. *Facebook* ise tartışmadan ziyade geniş bilginin yayımı için tercih edilen ortamlar olmuştur.

Covid-19 salgını ve bu salgının öngörülen sonraki aşamaları düşünüldüğünde insan davranışlarında kalıcı etkisi olacağı açıktır. Bundan önce opsiyonel görülen sosyal medya ve dijital iletişim, korona sonrası dönemde zorunlu hâle gelmiştir. Eskiden "çalışmaların sosyal medyadan duyurulması" diye özetleyebileceğim siyasette dijitalin kullanımına "Dijital Siyaset 1.0" dersek, bugünden sonra göreceğimize "Dijital Siyaset 2.0" diyebiliriz.

Sadece sosyal medyaya özgü yapılan propaganda çalışmaları artacaktır. Bu çalışmalar uzaktan iletişimin getirdiği etki ile daha katılımcı ve belki de daha açık sözlü olacaktır. Bu kampanyalar etiketlerle yapılan ve birkaç güne yayılan zincir kampanyalar olabileceği gibi, etki-tepki içeren kampanyalar da gerçekleşmeye başlayacaktır.

Dijital kampanyalarda kampanyaya muhatap olanlar yalnızca bir alıcı değil, aynı zamanda da kampanyanın bir konuşanı hâline gelebilmektedir. Savunulan konularla ilgili kısa, etkili, okunduğunda ya da izlendiğinde anlaşılabilen gönüllülerin yayacağı içerikler önemli hâle gelmektedir.

Bununla beraber siyasî iletişime uzak duran kişiler için de durum değişmektedir. Sosyal medyada bir siyasî mesaj, ansızın siyasî iletişime kapalı kişileri bulabilmekte, mesajın içe-

riğine ve mesajların tekrarına bağlı olarak siyasî katılımı artırmaktadır.

Alışılagelen kampanyaların mitingleri, parti parti birbirini takip eden, dolayısıyla sonrakilere, önceki mitingi yapana cevap hazırlaması için bir süre veren şekilde gerçekleşirken, yeni dijital siyaset iletişimi ile bir dijital kampanya başladığında etkileşim anında oluşmaya başlamaktadır. Dolayısıyla etki-tepki çok hızlı oluşacaktır. Bu etkiye tepkinin hazır şekilde mesajı sunmak isteyen tarafından verilmemesi hâlinde karşı mesaj ileten baskın gelebilecektir.

İnternet kampanyalarında kitleyi büyük gösterme ve etki-tepkide baskın çıkma güdüsü, yazılım robotlarının (*chatbot*) kullanımını da artıracaktır. Geçmiş ABD seçimlerindeki kullanımına baktığımızda Türkiye için de sosyal medya robotlarının yoğundan öte baskın bir şekilde kullanılacağını öngörmek mümkündür.

Diğer yandan sosyal medya kampanyalarında yaş ayrımı da yapılabilmektedir. Bundan önce tüm kitleye önerilerle giden kampanyanlar yerine farklı cinsiyet, ilgi ve yaş dilimlerine göre farklı kampanyalar tasarlanabilecektir.

Dijital siyaset 2.0'da alışılagelen televizyon platformlarındaki etki gücünün bir kısmının sosyal medyaya ve dijital tv platformlarına kayacağı değerlendirilmelidir. Bu kapsamdaki medya mecraları yeni medya olarak da tabir edilmektedir.

Ölçümleme anlamında düşündüğümüzde de yeni dijital siyaset avantajlar sunmaktadır. Sosyal medya mecralarının analitik platformları gibi karmaşık reklam etki değerlendirmeleri çok hızlı şekilde alınabilecek, her bir etkinlikte etki-tepki mesajlarının ve etiketlerin izlenmesi ile dahi kampanyanın başarısı ve bu başarının kalıcılığı nicel olarak ve anında ölçülebilecektir.

Bu anlamda üzerinde çalışılması gereken başlık önerilerinden birkaçı şu şekilde listelenebilecektir:

1- Sosyal medya robotlarının kullanımına izin verilip verilmeyeceği ile beraber, bu robotların, sosyal medya mecralarında mecra işletmecilerince hızlı şekilde engellenmesi üzerinde çalışılmalıdır.

2- Siyasî partilerin internet ve sosyal medya reklamları kullanımında ücretlendirme ve vergilendirme konuları çalışılmalıdır.

3- İnternetin insanları özgürlüğe sevk eden tasarımı ve bu şekilde geçirdiği 20 yıl üzerine sinmiştir. Bu platformlar üzerinde engelleyici politikalar bu platformların ağırlıklı kullanıcıları olan gençler ve erken yetişkinler tarafından olumsuz olarak algılanabilecektir. Bu nedenle engellemelerde, engellerin nihaî sonuçlarının beklentiyi sağlaması iyi irdelenmeli, engel-fayda dengesi gözetilmelidir.

4- İnternet bazlı engeller yerine herhangi bir olay anında buna hızlı müdahale edilebilmesi için, yabancı sosyal medya mecrası şirketlerinin devlet emrine en hızlı şekilde uymasının sağlayacak araçlar geliştirilmelidir. Maddî vergilendirme ve maddî cezalandırma gibi yan yöntemler Türkiye'de para kazanan sosyal medya şirketlerine karşı

güçlü birer araç olarak kullanılmalıdır.

5- Bunların yanında, algı çalışmalarına, algının hızında, karşı algı ile mukabele yöntemleri çalışılmalıdır. Bu anlamda sosyal medya ofisleri ile 7/24 esasında çalışılmalıdır.

6- Siyasî mesajların görselle zenginleştirilmiş, çok kısa dijital mesajlar hâline getirecek medya fabrikaları gündeme gelmelidir. Siyasî mesajlar alışılagelen ve zaten destekleyen siyasî kitlenin kolayca kabul edeceği, desteklemeyenler için ise sıradan kabul edilip kolayca reddedecekleri mesajlar yerine, münazara teknikleri henüz mesajı dağıtan partiyi desteklemeyenleri de hedefleyebilmelidir.

7- Salgının devamı ya da olası diğer salgınlar karşısında "dijital oylama" yöntemleri üzerine tartışmalar gündeme mutlaka gelebilecektir. Bu anlamda öncül çalışmalar gereklidir.

8- Siyasetçi ve politikacılar için de uzaktan toplantı yöntemleri ile kendi kitlelerine ulaşmaları yöntemi kullanılmalıdır. Bu seçmenler için siyasetçi-seçmen etkileşimli sosyal medya toplantıları olabileceği gibi, bölgesel derneklerle toplantıların uzaktan yapılabilmesi gibi siyasetçi-kurum etkileşimli toplantılar da olabilecektir.

Dijital Dönüşüm

Covid-19 salgını ile beraber tüm dünyada dijital dönüşüm hızlanmıştır. Sanal gerçeklik ve artırılmış gerçeklik ile beraber, ortam ve alet olmaksızın eğitimler düzenlenebilecek, eğlence sektörü için de sinemanın verdiği büyüklük ve üç boyut bu teknolojilerle sağlanabilecektir. Bu teknolojilerin tamamlayanı ise hologram teknolojisi olacaktır. Bugün dahi örneklerini gördüğümüz bu teknolojideki ivmelenmenin hızlanacağı ve uzak görüşmelerin üç boyutlu hologramla yapılacağı bir dünya daha da yakındır.

1850'lerdeki kolera salgını şehirler için yeni kanalizasyon sistemlerinin gerçekleştirilmesine yol açmıştı. Kirli suyun temiz sudan uzak şekilde atılabilmesi problemi çözülmüştü. Bu salgın da şehirlerde birçok etkiye yol açabilme potansiyeline sahiptir. Örneğin, şehrin göbeğinde kalabalık ile beraber olmak yerine, şehirden uzak, daha ucuz, ama kaliteli hayatlar bir tercih sebebi hâline gelebilecektir. Güneş enerjisinin kullanımı bu anlamdaki ulaşım maliyetlerini azaltacaktır. Yine benzeri şekilde sokaklarda ücretsiz kullanılabilecek ateş ölçerler ile erken teşhise imkân verilebilecektir. Akıllı şehir teknolojileri ile hastalık yoğunlaşma bölgelerinin tespiti de sağlanabilecektir.

Salgın sırasında alınan istatistiklere göre elektronik oyunlar zirve yapmaktadır. Durum bu iken, futbol oyunları da uzun süre oynanamamıştır. Bilgisayar oyunlarının bir lig kapsamında oynandığı e-spor olarak tabir edilen sporun fanlarının sayısı da gittikçe artacaktır.

Ülkelerin mevcut verileri ve siber hâkimiyet alanları o ülkelerin dijital topraklarıdır, dijital vatandır.[2] Siber güvenlik ise dijital vatanın olmazsa olmazıdır. Toprağın üstünde görünen-

2 O. Yılmaz, "Dijital vatan, dijital sınırlar, dijital hukuk ve dijital münhasır ekonomik bölgeler", Türkgün, 2020. [Çevrimiçi]. Adres: https://www.turkgun.com/dijital-vatan-dijital-sinirlar-dijital-hukuk-ve-diji-

ler, her türlü bilişim sistemi, yazılımlar ve bunların bağlı olduğu ağlardır. Toprağın altında ise milyonlarca vatandaş ve devlet tarafından üretilmiş her türlü veri vardır.

Ancak dijital/siber sınırlar daha muğlaktır. Yalnızca coğrafî sınırlarımızla da düşünülemez. Ülkemize ait bir sistemin veya verinin, başka bir ülkede bulunuyorsa dahi, bir ekslav gibi dijital vatan içerisinde kabul edilmesi gerekir.

Dijital vatanın kara yolları ise iletişim ağlarıdır. Bu iletişim ağları bugün baktığımızda, bakır ve fiber tabanlı kablolu ağlar ile mobil gibi kablosuz ağları içerir. Bu noktada dijital yolların kime ait olacağı, kara yollarının devletin mülkiyetinde olup olmadığı tartışması kadar önemlidir. Tüm dijital yolların da devlete ait olması beklenmelidir.

Dijital vatanın toprak altı kıymeti veridir. Veri, bir maden gibi büyük bir kıymettir. Verinin işlenmesi işine de veri madenciliği denmesi bu anlamda bir tesadüf değildir. Bu veriye kimlerin sahip olacağı, sahipliklerinin sınırları, bu veriye (madene) devletin uygulayacağı mevzuat, devletin veriden kazanacağı pay gibi başlıklar hali hazırda yoğun tartışmaların olduğu bir alanlardır. Dijital vatan, "dijital münhasır ekonomik bölgeler" oluşturmak için de ülkelere büyük fırsatlar sunmaktadır.[3]

Elbette, dijital vatanın güvenliği de önemli bir başlıktır. Bu noktada şu anda yalnızca coğrafî sınırlar içindeki veri ve sistemlerin güvenliği tartışılmaktadır. Hâlbuki bir Türk şirketine ait Almanya'daki bir sistem ve altındaki veri de bu anlamda vatan içinde kabul edilmelidir.

Bundan 50 yıl önce internet nasıl ortaya kondu ve bugün internete hâkim olmak bir millî güvenlik konusu ise, bundan 20 yıl önce Google, 15 yıl önce Facebook nasıl ortaya kondu ve millî güvenlik konusuna döndüyse, 5G'de de bu olacaktır. 5G, dünyada var olacaksa, 5G'de üretici ve önde olmak, her detayına hâkim olmak, bir millî güvenlik konusu hâline gelecektir. Çünkü 5G teknoloji olarak her zaman her yerde olan bir teknoloji olarak tasarlanmış, dolayısıyla bugünün kablolu ağlarını dahi içine alacak bir teknolojidir. Bu anlamda bakıldığında, kendi 5G altyapısına sahip olmamak, kendi otoyollarına sahip olmamak anlamına gelecektir.

Bu anlamda üzerinde çalışılması gereken başlık önerilerinden birkaçı şu şekilde listelenebilecektir.

1- Dijital dönüşümün kamu ortaklı şirketler tarafından ele alınması, dünya çapında rekabetçi olabilecek sivil bir dijital sektör oluşunu engellemektedir. Yakın zamanlı bir örnek olarak, sektörde uzaktan görüntülü konuşma sağlayıcıları olarak bulunan Karel, Netaş ve diğer 6 firmaya ek olarak, Aselsan ve Havelsan bu alana giriş yapmıştır. Üst seviye teknoloji dahi diyemeyeceğimiz görüntülü konuşma alanında dahi bu şekilde bir durum oluşması, iç pazardan beslenecek rekabetçi sivil bilişim sektörünün gelişmesinin önündeki refleksi ifade etmektedir. Bu anlamda askerî alandan farklı

tal-munhasir-makale-117109. [Erişim: 25 Mayıs 2020].

3 O. Yılmaz, "Dijital vatan, dijital sınırlar, dijital hukuk ve dijital münhasır ekonomik bölgeler", Türkgün, 2020. [Çevrimiçi]. Adres: https://www.turkgun.com/dijital-vatan-dijital-sinirlar-dijital-hukuk-ve-dijital-munhasir-makale-117109. [Erişim: 25 Mayıs 2020].

olan bu dijital dönüşüm alanlarında, tam rekabetçi ve sivil bir sektör oluşumu için politikalar düzenlenmelidir.

2- Türkiye'nin oyun sektöründe ulaştığı başarı, bu sektörle ilişkili olan AR, VR, Hologram gibi dikeylerde de başarı getirebileceğinden hareketle, dikey sektör geliştirme politikalarında bu teknolojiler göz önüne alınmalıdır.

3- İnternet bağlantı genişliği ve kalite ihtiyaçlarının artması ile beraber Türkiye'de internet altyapısının geliştirilmesine ihtiyaç bulunmaktadır. İnternet bundan önce daha çok tek yönlü yani internetten bize doğru gelen trafik için kullanılırken, artık bizden dışarı doğru giden, örneğin video trafiği için de kullanılmaktadır. Bu nedenle Türkiye'deki xDSL hatlardaki asimetrik karakter nedeniyle var olan düşük yükleme (*upload*) hızlarının artırılması sağlanmalıdır.

4- Akıllı fabrikalar, nesnelerin interneti gibi, bir alanda internete bağlı yüksek cihaz sayısı beklentisi ile beraber yüksek veri transfer ihtiyaçları için 5G teknolojisi tasarlanmıştır. Bu teknoloji için, Amerika'nın ticaret savaşlarını bahane ederek Çin'e uyguladığı yavaşlatma da bu teknolojide önde olma yarışını ifade etmektedir. Bu nedenlerle 5G teknolojisinde 2018'de başlayan yerli ve millî yazılım ve donanım altyapısı geliştirme projeleri sonuca ulaştırılarak, Türkiye'nin yerli ve millî 5G altyapısına sahip olması sağlanmalıdır. İlgili lisans ihaleleri Türkiye'nin kendi sistemleri hazır olana dek yapılmamalıdır.

5- 5G teknolojileri ile ilgili bu teknolojinin zararları da olduğunu iddia eden çeşitli komplo teorileri oluşmuştur. Türkiye'deki 5G lisanslaması öncesinde, açılacak frekans bantlarına karar verilecektir. Türkiye şu ana kadar ki politikasında insan vücudunun özümseyeceği maksimum güç ölçüsü olan SAR seviyelerinde Avrupa ve Amerika'daki çok daha korumacı değerlere izin vermektedir. Türkiye'de uygulanacak 5G frekans bantları seçilirken, moleküler biyoloji, genetik, halk sağlığı gibi bilim dallarındaki çalışmaların o günkü geldiği nokta değerlendirilerek halk sağlığı için en uygun frekans bantları seçilmelidir.

6- Günümüzün frekans bantlarında işletmecilere komple alan ayrılması yerine, bantların ortak kullanılabildiği, farklı teknolojilerin de bantları ortak kullanabileceği frekans spektrumu yönetimi politikaları ile daha verimli frekans politikası geliştirilmelidir.

7- Kırsal alanlarda internet bağlantısı hâlen çok sorunludur. Geniş bant erişiminin kırsal alanlara da verilebilmesi için politikalar çalışılmalı, IEEE 802.22 (Sabit Kablosuz Erişim) gibi yenilikçi standartlara fırsat verilmelidir. Bu sayede internetin sağladığı gelişim kaldıracını kırsalda da kullanabilen vatandaşlar, şehirler yerine kırsalı tercih edebilmelidir.

8- İnternette var olan verinin artması ile beraber büyük veri çalışmaları ivme kazanacaktır. Büyük veri çok kıymetli politikalar oluşmasına imkân verecek bir nimettir. Günümüzün petrolü olarak ifade edilmektedir. Büyük veride başarılı olabilmek ise bu veri üzerinde çalışabilen ekiplerle olacaktır. Ancak her kurum kendi verisine büyük

kıymet vererek kapalı tutmaktadır. Bir anonimleştirme ve kişi/kurum özel verilerinin ayıklanması sayesinde ve büyük veri üzerinde büyük veri ve yapay zekâ araştırmacılarının çalışabileceği bir mevzuat ve akademik taban oluşturulmalıdır.

9- Eğitim sisteminde, hem öğretici hem öğrencileri kapsayan dijital dönüşüm hızlandırılmalı, uzaktan ders, seminer ve sınavlar örgün eğitimin bir parçası hâline getirilmelidir. Bu sayede halkımızda internet kapsaması da artırılabilecek, olası gelecek salgınlar hâlinde de, tatbikatı devamlı yapıldığı şekilde uzaktan eğitime devam edilebilmelidir.

10- Dijital vatanın hukuku da kendine özeldir. Bu "dijital hukuk", hâlihazırda 5651, 6698 sayılı Kanunlar gibi çeşitli kanunlar ile yerelde oluşmaya başlamışsa da, uluslararası hukuk tarafında alınan yol, gerekenin yanında neredeyse bir hiçtir. Bu anlamda dijital vatanın güçlenmesi ve korunması için yerel mevzuat ve uluslararası mevzuat çalışılmalıdır.

11- G20'de Güven İçinde Özgür Veri Akımı (DFFT) isimli bir öneri getirilmiştir. Verinin nerede tutulacağını ve internete nasıl muamele edileceğini ülke politikalarından bağımsız hale getirmeyi amaçlayan bu öneri, bir dijital IMF önerisi, devletin egemenliğini bu başlıkta askıya almaktadır. Bu öneri ülkemiz tarafından da sahiplenilmiş görünmektedir.[4] İçeride "verimiz yurt içinde kalsın" vizyonu ile hareket ederken, DFFT gibi bir yanda "güven vadeden", öte yandan tüm veriyi "özgür akıma zorlayan" anlaşmalara taraf olma politikaları gözden geçirilmelidir.

12- Dijital vatan, "dijital münhasır ekonomik bölgeler" oluşturmak için de ülkelere büyük fırsatlar sunmaktadır. Örneğin, Türkiye Cumhuriyeti vatandaşlarının verilerinden para kazanan bir sosyal medya şirketinin kazandığı, esasen Türkiye'nin verisinden kazanılmış olup, ülkemiz de pay almalıdır. Bugün ise, son mevzuat çalışmalarıyla, sadece bu ülkelerin Türkiye'de kazandıklarından pay alınmakta, yurtdışında Türk verileri üzerinden kazandıklarından pay alınmamaktadır. Bu gündem uluslararası örgütler nezdinde dile getirilmeli, yerel olarak da politika ve mevzuatlar ile verinin saklı kıymetine ulaşılması sağlanmalıdır.

Acele Dijitalleşme ve Siber Güvenlik

Siber güvenliğin üzerine oturduğu üç temel ayak gizlilik, bütünlük ve erişilebilirliktir. Bilgi ve sistemler üçüncü kişilere karşı gizli olmalıdır. Bilgi ve sistemler değiştirilmeye karşı dayanıklı ve değiştirildiğinde anlaşılabilir olmalıdır. Tüm bunları sağlarken sistemlerin hâlen kullanıcılar tarafından erişilebilir olması gerekmektedir. Diğer yandan, nasıl bir zincir en zayıf halkası kadar sağlam ise, sistemler de en ufak güvenlik açığı ile bu güvenlik üçlüsüne karşı zayıf kalabilirler. Dolayısıyla siber güvenliğin noktasal değil yüzeysel olduğunu söylemek mümkündür.

4 "Bakan Varank'tan G20 ülkelerine önemli tavsiye," Anadolu Ajansı, 08 Haziran 2019. [Çevrimiçi]. Adres: https://www.aa.com.tr/tr/dunya/bakan-varanktan-g20-ulkelerine-onemli-tavsiye/1498882.

Korona döneminin dijitalleşmesini "acele" kelimesiyle özetleyebiliriz. Salgın sonrasında şirketlerin ve kamunun acilen evlere taşınması ile daha önce ofiste kullanılan sistemlerin hızlıca internete açılmasını getirmiştir. Bu süreç çok hızlı ve güvenlikten ziyade işlev odaklı şekilde gerçekleşmiştir. Örneğin, sadece Windows işletim sistemlerine uzak erişim sağlayan RDP protokolü için 1.5 milyon yeni sistemin evlerden ulaşabilmek için internetten erişime açıldığı belirtilmektedir.[5] Uzak erişim için doğrudan RDP erişimleri kullanmak yerine kullanılabilecek VPN teknolojileri önemli bir güvenlik aracıdır. Bu sayede kullanıcılar güvenlik özel ağlar sayesinde kendi sistemlerine erişebilmektedirler.

Diğer yandan saldırganlar tarafındaki saldırı yöntemlerinde de salgın sürecinin paniğini kullanmaya yönelik değişiklikler olmuştur. Örneğin Covid-19 test sonucunuzun geldiğini belirten, borsalardaki hareketlilikte tüyo hisse öneren, sıfır faizli kredi sunan ya da salgına karşı korunma yöntemleri vaat eden epostalar ile kullanıcıları aldatan ve eklerdeki zararlı yazılımları bulaştırmaya çalışan yöntemler yaygınlaşmıştır. Daha salgının başlangıç dönemlerinde Google'a göre koronavirüs konulu zararlı e-posta sayısı günlük 18 milyondur.[6]

Daha önce ikincil hedefler olan üniversiteler ve araştırma kuruluşları özellikle salgın araştırmaları üzerinde çalışıyorlarsa birincil hedefler hâline gelmektedir.[7]

Ülkelerde salgına karşı korunma ve takip amaçlı telefon uygulamaları yaygınlaşmaya başlamıştır. Bu uygulamalar çevrenizdeki salgın kaynaklarını haber vermeyi vaat etmekte, bir yandan da sizin kişisel bilgilerinizin mahremiyet sınırlarını en uca kadar kullanmaktadır. Örneğin siz daha önce virüs aldığı bilinen başka bir kişiye bir mesafeden daha yakın ve bir süre bulunmuşsanız sizi uyarmaktadır. Bazı uygulamalar, salgın hastalığını geçirmiş kişilere yaklaştığınızdan sizi uyarabilmektedir. Bu sistemler olaydaki her iki taraf için de kişisel bilgi mahremiyeti sorunları getirmektedir.

Diğer yandan elbette devletler tarafından geliştirilen bu uygulamalar yanında, büyük çevrim içi şirketler de benzer uygulamalar geliştirmeye başlamıştır. Yakın bir zamanda Google ve Apple'ın birlikte benzer bir çalışma içerisinde bulunduğu görülmektedir. Devlet otoriteleri dışında gerçekleşen bu tip çalışmalar merkezî sağlık yönetimleri tarafından pek kabul görmemektedir.[8] Devlet güdümlü uygulamalar daha çok merkeziyetçi tasarımlara sahipken mahremiyet savunucuları dağıtık mimaride tasarlanmış uygulamaların kullanımını önermektedir. Google ve Apple ile beraber Almanya da dağıtık yapıyı tercih

5 L. Constantin, "Attacks against internet-exposed RDP servers surging during COVID-19 pandemic", CSO Online, 2020. [Çevrimiçi]. Adres: https://www.csoÇevrimiçi.com/article/3542895/attacks-against-internet-exposed-rdp-servers-surging-during-covid-19-pandemic.html. [Erişim: 26- May- 2020]

6 S. Musil, "Google blocking 18M malicious coronavirus emails every day", CNET, 2020. [Çevrimiçi]. Adres: https://www.cnet.com/news/google-seeing-18m-malicious-coronavirus-emails-each-day/?ftag=CMG-01-10aaa1b. [Erişim: 26- May- 2020].

7 "Hostile states trying to steal coronavirus research, says UK agency", the Guardian, 2020. [Çevrimiçi]. Adres: https://www.theguardian.com/world/2020/may/03/hostile-states-trying-to-steal-coronavirus-research-says-uk-agency. [Erişim: 26- May- 2020].

8 "NHS rejects Apple-Google coronavirus app plan", BBC News, 2020. [Çevrimiçi]. Adres: https://www.bbc.com/news/technology-52441428. [Erişim: 26- May- 2020].

ederken, Fransa ve İngiltere merkeziyetçi yapıda diretmektedir.[9] Merkeziyetçi yapının önündeki engeller ise mobil işletim sistemlerinin tasarımlarındaki güvenlik korumalarıdır. Örneğin, Apple mobil işletim sistemi dışarı veri transfer eden uygulamalara arka planda bluetooth kullanma izni vermemektedir.[10]

Mobil uygulama marketlerinde de sahte koronavirüs ve salgın uygulamaları yer almaya başlamıştır. Kendilerine yeni bir maske bulan bu uygulamalar yüklendikleri telefon aracılığı ile kimlik, bilgi ve para hırsızlığı için kullanılmaktadır. Sadece uygulamalar değil internet sayfaları da on binlerce benzeri tuzakla dolmaktadır.

Sadece son kullanıcılar değil, devletler de hedeftedir. Salgın döneminde yoğun kamuoyu baskısı altında kalan devletler ve hükümetleri muhtelif karşı güçlerin saldırılarına karşı daha açık veya bunlardan daha çok etkilenebilir hale gelmiştir. Örnek olarak, bu salgın döneminde Azerbaycan ve Hindistan'ı hedefleyen bir uzak erişim truva atı keşfedilmiştir. Bu zararlı yazılım özellikle enerji altyapılarında saldırı altyapısı oluşturmayı hedeflemektedir.[11]

Fiziki iletişimin azaldığı dönemde elektronik haberleşme önem kazanmıştır. Avrupa Siber Güvenlik Ajansı (ENISA)'ya göre bir kritik altyapı olarak tanımlanan ancak enerji altyapılarının yanında şu ana kadar hak ettiği kritik bir altyapı muamelesi görmeyen Elektronik Haberleşme altyapılarının önemi ve kritikliği anlaşılmıştır.

Salgın karşısında ülkelerin vatandaş mahremiyetine verdikleri önem oldukça farklılık göstermektedir. Çin vatandaşları için sağlık kodu uygulaması başlatmıştır. Bu sistem ile belirlenmiş algoritmalara göre insanlar renk kodu almaktadır. Renk kodu ise girebilecekleri alanları belirlemektedir. Bu renk kodunun belirlenmesinde ise yaygın veri toplama yöntemleri kullanılmaktadır. Örneğin Alipay ve WeChat hesaplarının tarihçeleri incelenerek gittikleri yerler, salgın noktalarında bulunup bulunmadıkları gibi veriler kullanılmaktadır.[12]

Bunun yanında, uyguladığı yaygın yüz tanıma sistemlerine ateş ölçme nitelikleri kazandırılmasıyla beraber Çin'in yaygın yüz tanıma sistemlerinin oturduğu zayıf gerekçeler güçlenmiştir. Daha önce uygulanmayan, örneğin mobil aboneliklerde dahi yüz tanıma kaydı

9 C. Osborne, "Germany pivots from centralized coronavirus tracing app to privacy-protecting alternative | ZDNet", ZDNet, 2020. [Çevrimiçi]. Adres: https://www.zdnet.com/article/germany-pivots-from-centralized-coronavirus-tracing-app-to-privacy-protecting-alternative/. [Erişim: 26- May- 2020].

10 "Bloomberg - Are you a robot?", Bloomberg.com, 2020. [Çevrimiçi]. Adres: https://www.bloomberg.com/news/articles/2020-04-20/france-says-apple-s-bluetooth-policy-is-blocking-virus-tracker. [Erişim: 26- May- 2020].

11 C. Osborne, "PoetRAT Trojan targets energy sector using coronavirus lures | ZDNet", ZDNet, 2020. [Çevrimiçi]. Adres: https://www.zdnet.com/article/poetrat-trojan-targets-energy-sector-using-coronavirus-lures/. [Erişim: 26- May- 2020].

12 L. Kuo, "'The new normal': China's excessive coronavirus public monitoring could be here to stay", the Guardian, 2020. [Çevrimiçi]. Adres: https://www.theguardian.com/world/2020/mar/09/the-new-normal-chinas-excessive-coronavirus-public-monitoring-could-be-here-to-stay. [Erişim: 26- May- 2020].

zorunluluğu getirilmesi de bu salgın döneminin paniğinde gerçekleşmiştir. Çin'e benzer şekilde Güney Kore de yaygın büyük veri analizi ile salgın riski belirlemeye çalışmaktadır. İsrail ise salgınla beraber Shin Bet'e tüm ülkedeki mobil konum verisine erişim yetkisini vermiştir.[13]

Bu anlamda üzerinde çalışılması gereken başlık önerilerinden birkaçı şu şekilde listelenebilecektir.

1- Salgın süreci yeterli güvenlik önlemleri alınmaksızın sistemlerin internete açılmasını getirmiştir. BTK USOM Siber Olaylara Müdahale Merkezi daha proaktif bir rol üstlenerek Türkiye'de hizmet veren IP adreslerini tarayarak, güvenlik açığı oluşturabilecek sistemlerle ilgili sistem sahiplerini haberdar etmelidir.

2- Her şeyin dijitalleşmesi diye bahsedebileceğimiz bu dönemde siber güvenlik kaçınılmaz olarak öne çıkacaktır. Bu anlamda yerli siber güvenlik sanayinin kayıtsız şartsız desteklenmesi için en etkili yöntem, yabancı ürün girişinin teknik, ticarî, gümrük bariyerleri ile yavaşlatılması olacaktır. Siber güvenlik alanında yerli ve millî üretimin önemine binaen bu alanda gümrük ve koruma politikaları kullanılmaya başlanmalıdır. Bununla beraber ihracata dayalı bir teşvik sistemi ile korumacı hâle gelmiş Türkiye pazarında üretilen ürünlerin yurtdışına da satılabildiğinden emin olunabilmelidir.

3- Türkiye'ye ithal edilecek her türlü siber güvenlik sisteminin yerel siber güvenlik test ve sertifikasyonuna tâbi tutulması sağlanmalıdır.

4- Zaten salgın nedeniyle yoğun kamuoyu baskısı altındaki hükümetler için, olası enerji ve su kesintilerinin oluşturacağı baskının dış güçlerce hedeflenebileceği unutulmamalıdır. Salgın, siber saldırılar için bir algı-odak şaşırtma (sisleme) yöntemi olarak kullanılabilecektir.

5- Artan VPN kullanımı, devletler açısından gözetleme (sürveyans) faaliyetlerinin engellenmesi sonucunu doğurmaktadır. Bu anlamda, devlet kaynaklı gözetleme politikalarında günün doğal dijitalleşme gereksinimlerine göre değişim öngörülmelidir.

6- Türkiye'de sunulan cep telefonlarının üzerlerindeki ön tanımlı uygulamalardaki zorlamalar engellenmeli ve yerli üreticilerin kendi, internet, harita, disk ve benzeri uygulamalarını ön tanımlı sunabilme, Android ön tanımlı uygulamalarını sunmama hakkı kanunen sağlanmalıdır. Rekabete aykırı da olan bu durum karşısında yerli üreticilerin özgürlüğü, bir mevzuat olmadığı sürece gerçekçi şekilde sağlanamamaktadır.

7- Şirketler için geçmişte internet sayfası olması zorunluluğuna benzer şekilde minimum siber güvenlik önlemlerini bulutta ya da kendi yerlerinde alma zorunluluğu politikaları çalışılmalıdır.

13 C. Cimpanu, "US, Israel, South Korea, and China look at intrusive surveillance solutions for tracking COVID-19 | ZDNet", ZDNet, 2020. [Çevrimiçi]. Adres: https://www.zdnet.com/article/us-israel-south-korea-and-china-look-at-intrusive-surveillance-solutions-for-tracking-covid-19/. [Erişim: 26- May- 2020].

8- 06.07.2019 tarihli "Bilgi ve İletişim Güvenliği Tedbirleri" Konulu Cumhurbaşkanlığı Genelgesi'ndeki adımlar bir başlangıç olmakla beraber yetersizdir. Yeni mevzuat ile siber güvenliğin noktasal değil tüm yüzeyi kapsayan bir gayret gerektirdiği unutulmadan alandaki politikalar geliştirilmelidir.

9- Siber güvenlik alanındaki tehditlerin önemli çoğunluğu ağ katmanlarından uygulama katmanına kaymıştır. Bu kapsamda uygulama katmanında güvenlik sağlayabilen sistemlerin yerli ve milli geliştirilmesi için politikalar ve araçlar çalışılmalıdır.

10- Türkiye'deki mevzuat ile yerli malı belgesi alımı tasarım ve yazılımı göz ardı etmektedir. Örneğin, tüm tasarım ve yazılımı Çin'de yapılan bir ürün Türkiye'de monte edilerek yerli malı belgesi alabilmektedir. Bu kapsamda Çin'in amiral gemisi teknoloji markalarının ürünleri Türkiye'de yerli malı belgesi alabilmektedir. Yerli malı mevzuatında bu durumun düzeltilmesi için ilgili mevzuat yerli sanayiciler işbirliği ile yenilenmelidir.

11- Siber güvenlik alanındaki ürünlerin başarımları, korumacılık ile ters orantılıdır, yaygınlık ile doğru orantılıdır. Devlet ortaklı şirketler aracılığı ile siber güvenlik alanındaki yerli şirketlerle rekabete yol açan politikalar engellenmeli, bunun yerine açık standardizasyon kapsamında test edilen, sertifikalandırılan, serbest pazar içerisinde yarışarak yetkinlik geliştirecek üreticiler modeli tercih edilmelidir.

12- Türkiye'de kullanılan ana akım yazılımların (ofis, işletim sistemleri, siber güvenlik sistemleri) tüm veri güncellemelerini Türkiye'de konuşlanmış sunucular üzerinden yapmaları sağlanmalıdır.

13- Millî güvenliğe doğrudan etkileyen kurumlarda ürettikleri ürünleri kullanılan yabancı üreticilerin ve kanallarının destek personelleri ile yerli üreticilerin AR-GE dâhil tüm personelleri ile ilgili güvenlik soruşturması ve arşiv araştırması kanalları bu firmalara açılmalıdır.

14- SPK mevzuatına tabi şirketlerin siber güvenlik olgunluklarının garanti edilmesine yönelik mevzuat hazırlanarak ilgili mevzuata eklenmelidir.

15- Yerli ve millî arasındaki ayrım mevzuat ile yapılmalı ve Millî Ürün Belgelendirmesi oluşturulmalıdır.

Sonuç

Covid-19 sonrasında genel söylem "Hiç bir şey eskisi gibi olmayacak" şeklinde oluşmuştur. Bakıldığında salgın ve evde kalma sürecinin insan davranışlarında değişimlere yol açacağı açıktır. Salgın sonrasında beklenen teknoloji değişimleri ise daha önce olmayıp da birden ortaya çıkan olaylar olarak tanımlamak mümkün değildir. Aslında zaten devam eden bir dijitalleşme sürecinin içerisinde biraz hızlanma, biraz önceliklerin değişmesi söz konusu olmuştur.

Bu süreç aynı salgın öncesinde dijitalleşmenin akışındaki gibi, ülkeler için tehdit ve fırsatlar içermektedir. Tehditlerin ele alınması ve hatta birer fırsata çevrilmesi de, ancak bunlara farkındalık içerisinde yapılan politikalar ve bu politikaların sağlıklı icrası ile mümkün olabilecektir. Bu alanlardaki en kapsayıcı fırsat günümüzün ve geleceğin sektörü olarak belirtilen teknoloji sektörlerinin güçlendirilmesi olacaktır.

KAYNAKÇA

"Patentability of Medical Methods in Europe | European IP Blog", Finnegan | Leading Intellectual Property Law Firm, 2020. [Çevrimiçi]. Adres: https://www.finnegan.com/en/insights/blogs/european-ip-blog/patentability-of-medical-methods-in-Europe.html. [Erişim: 13 Mayıs 2020].

"Bakan Varank'tan G20 ülkelerine önemli tavsiye," Anadolu Ajansı, 08 Haziran 2019. [Çevrimiçi]. Adres: https://www.aa.com.tr/tr/dunya/bakan-varanktan-g20-ulkelerine-onemli-tavsiye/1498882. [Erişim: 22 Mayıs 2020].

O. Yılmaz, "Dijital vatan, dijital sınırlar, dijital hukuk ve dijital münhasır ekonomik bölgeler", Türkgün, 2020. [Çevrimiçi]. Adres: https://www.turkgun.com/dijital-vatan-dijital-sinirlar-dijital-hukuk-ve-dijital-munhasir-makale-117109. [Erişim: 25 Mayıs 2020].

L. Constantin, "Attacks against internet-exposed RDP servers surging during COVID-19 pandemic", CSO Online, 2020. [Çevrimiçi]. Adres: https://www.csoÇevrimiçi.com/article/3542895/attacks-against-internet-exposed-rdp-servers-surging-during-covid-19-pandemic.html. [Erişim: 26- May- 2020].

"Hostile states trying to steal coronavirus research, says UK agency", the Guardian, 2020. [Çevrimiçi]. Adres: https://www.theguardian.com/world/2020/may/03/hostile-states-trying-to-steal-coronavirus-research-says-uk-agency. [Erişim: 26- May- 2020].

"NHS rejects Apple-Google coronavirus app plan", BBC News, 2020. [Çevrimiçi]. Adres: https://www.bbc.com/news/technology-52441428. [Erişim: 26- May- 2020].

C. Osborne, "Germany pivots from centralized coronavirus tracing app to privacy-protecting alternative | ZDNet", ZDNet, 2020. [Çevrimiçi]. Adres: https://www.zdnet.com/article/germany-pivots-from-centralized-coronavirus-tracing-app-to-privacy-protecting-alternative/. [Erişim: 26- May- 2020].

S. Musil, "Google blocking 18M malicious coronavirus emails every day", CNET, 2020. [Çevrimiçi]. Adres: https://www.cnet.com/news/google-seeing-18m-malicious-coronavirus-emails-each-day/?ftag=CMG-01-10aaa1b. [Erişim: 26- May- 2020].

"Bloomberg - Are you a robot?", Bloomberg.com, 2020. [Çevrimiçi]. Adres: https://www.bloomberg.com/news/articles/2020-04-20/france-says-apple-s-bluetooth-policy-is-blocking-virus-tracker. [Erişim: 26- May- 2020].

C. Osborne, "PoetRAT Trojan targets energy sector using coronavirus lures | ZDNet", ZDNet, 2020. [Çevrimiçi]. Adres: https://www.zdnet.com/article/poetrat-trojan-targets-energy-sector-using-coronavirus-lures/. [Erişim: 26- May- 2020].

L. Kuo, "'The new normal': China's excessive coronavirus public monitoring could be here to stay", the Guardian, 2020. [Çevrimiçi]. Adres: https://www.theguardian.com/world/2020/mar/09/the-new-normal-chinas-excessive-coronavirus-public-monitoring-could-be-here-to-stay. [Erişim: 26- May- 2020].

C. Cimpanu, "US, Israel, South Korea, and China look at intrusive surveillance solutions for tracking COVID-19 | ZDNet", ZDNet, 2020. [Çevrimiçi]. Adres: https://www.zdnet.com/article/us-israel-south-korea-and-china-look-at-intrusive-surveillance-solutions-for-tracking-covid-19/. [Erişim: 26- May- 2020].