KORKULMASI GEREKEN ROBOTLARIN İNSANLAŞMASINDAN ZİYADE İNSANLARIN ROBOTLAŞMASI

Naman BAKAÇ *

Orcid ID: https://orcid.org/000-0002-7806-4827

Günümüzde internet ve bilişim teknolojisinin baş döndürücü bir şekilde gelişimi ile birlikte; siber güvenlik, siber saldırı hatta "siber vatan", siber politikalar, dijital şirketler, dijital vatandaşlık gibi binbir envai çeşit disiplin ve sorun alanlarının doğuşuna şahitlik etmekteyiz. Hakeza, sosyal medya mecralarının insanı hem apolitik ve asosyal hem de politik ve sosyal hayata güçlü katılımını sağlayan iki ucu keskin bıçak olduğu şeklindeki tartışmalar ise, hem gündelik hayatta hem de siyasi ve akademik elitler tarafından tartışılmakta. Tüm bu sorun ve tartışma alanlarında uzunca bir süredir akademik çalışmalarıyla bilinen Selçuk Üniversitesi Uluslararası İlişkiler Bölümünden Prof. Dr. Nezir AKYEŞİLMEN ile bu güncel meseleleri teorik bir çerçevede konuşmaya çalıştık. AKYEŞİLMEN, Siber Politika alanında Türkiye'de ilk ve tek, dünyada ise sayılı dergilerden biri olan Uluslararası hakemli "Siber Politikalar Dergisi'nin editörlüğünü de sürdürmekte olan bir isim.

Teknoloji bu hızla ilerleyecek olursa, insanlığı ne tür tehditler ve fırsatlar bekliyor? Kimilerinin Transhümanizm ya da insansız çağ bir başkasının ise dijital çağ veya yapay zekâ çağı nitelendirmesi sözkonusu. Siz insanlığı neyi beklediğini öngörüyorsunuz?

Teknoloji nötr bir şeydir. Onu iyi ya da kötü yapan insanların kullanım biçimleridir. Bilim kurgu dizisi Black Mirror izlenirse yakın zamanda bizi nasıl bir dünyanın beklediği hakkında fikir edinilebilir. Siber teknolojinin sağlıktan, ulaşıma, iletişimden gıdaya her alanda büyük zenginlik, konfor ve kolaylık sağlayacağı bir gerçek. Akıllı giysilerden, robot bakıcılara, ucuz, hızlı ve kaliteli üretim modellerinden, kullanıcı dostu makinelere kadar bir dizi kolaylaştırıcı teknolojiler bizi bekliyor. Fakat aynı zamanda büyük tehditler de onu izliyor. Özellikle insanın zihinsel ve psikolojik bütünlüğüne yönelik girişimlerde ahlaki anlamda büyük zorluklarla karşı karşıya kalabiliriz. Herkes yapay zekânın kodların ötesine geçerek kendi kendilerine karar vermelerinden korkuyor. Oysa korkulması gereken robotların insanlaşmasından ziyade insanların robotlaşmasıdır. İnsan beyninin fiziken hacklenmesi bugün bile tartışılan bir konu. Bugünden insanın zihinsel, ruhsal ve fiziksel bütünlüğünü koruyacak küresel çapta bir takım hukuki önlemler alınamazsa, yarın çok geç olabilir.

* Öğretmen, Gazeteci ve Yazar.

İnternet ve sosyal medya araçlarının sıklıkla kullanılması, siber ve siber güvenlik, kişisel verilerin korunması gibi konularla insanları daha çok ilgilenir gördük. Cumhurbaşkanı Erdoğan "Siber Vatan"ın da savunumuna dönük açıklamaları oldu malumunuz. Bu insanın ilkçağlardan gelen koruma/güvenlik ihtiyacının şekil almış başka bir hali mi yoksa bireyin/ kurumun/şirketin kendi mahrem alanına karşı bir tepkisi mi? Ya da varsa sizce başka saikler nelerdir?

Güvenlik tıpkı diğer pek çok sosyal ve siyasal alanlar gibi dinamik bir alandır. Sürekli değişen ve dönüşen bir şeydir. İlk dönemlerde fiziksel güvenlik merkezde iken sonra ekonomik güvenlik, siyasal güvenlik, çevre güvenliği, sağlık ve gıda güvenliği gibi insani güvenlik öne çıktı. Bugün siber güvenlik bu gelişen güvenliğe sadece yeni bir boyut ekliyor. Ve bütün bu güvenlik sektörleri birbiriyle ilintili ve bağlantılıdır. Veri güvenliği ihlali ya da özel hayatın ifşası bireyin ve hatta toplumun ekonomik güvenliğini, siyasal güvenliğini, çevre ve gıda güvenliğini tehdit edebilir. Siber güvenlik o kadar genişledi ki bugün bana göre insan güvenliğinin bir bileşeni haline geldi.

ABD'deki 6 Ocak 2021 Darbe girişimi olarak görülen ve Trump'ın dijital çağrısı ile başlayıp, Twitter, Facebook, İnstagram'ın dijital darbe önleme tedbirleri ile ayyuka çıkan bir tür dijital savaşlar da sözkonusu gibi. Politik mücadeleler, onların karşıtları ve buradan kurulacak yeni politik düzende sizin uzmanlık alanınız da olan siber siyasetin nasıl şekil alacağına dair neler söylersiniz?

Siber siyaset dediğimiz şey siyasal süreçler üzerinde siber teknolojinin etkisinden başka bir şey değildir. Siyasi alanı yer yer genişleten ve yer yer daraltan bir fonksiyon görüyor sosyal medya platformları. Bir yandan seçmenle iletişim ve ilişki kurmada dezavantajlı siyasal aktörlere imkânlar sunarken, öbür yandan manipülasyonlara açık bir alan konumundadır. Seçim süreçlerini manipüle etme, gerçek-dışı haberler yayma, dezenformasyon, algı operasyonları ve hatta seçim süreçlerine doğrudan müdahale etme fırsatı veriyor kötü niyetli aktörlere.

Sosyal medya şirketleri sadece platform sağlamıyor, yeri geldiğinde siyasal bir aktör gibi de davranabiliyorlar. Trump olayında görüldüğü gibi, birilerinin sesini kısabiliyorlar. Tabi bu güç; demokrasi ve insan hakları, çevre ve azınlık haklarının korunması için kullanılırsa insanlığın hayrına olur. Fakat bu şirketler burada da seçici davranırlarsa o zaman insan hakları, barış, istikrar ve küresel demokratikleşme süreçlerine yönelik büyük bir tehdit oluşturabilirler.

DİJİTAL YARGIÇLAR YOLDA

Günümüzde kişisel verilerin korunması, siber saldırılar, sanal suçlar, teknolojinin tahakkümü gibi tartışmalar almış başını gidiyor. Eğitimin dijitalleşmesi gibi adeta bir nevi hukukun dijitalleşmesi diyebileceğimiz bir evreye de geçiyor muyuz acaba? Hukukun; bu kişisel veriler, siber saldırılar ve suçlar bahsinde gücü nedir?

Hiçbir şey dijitalleşmeden beri değildir. Bu çerçevede hukuk bir istisna değildir. Bugün bile hukuk dijitalleşmekten çokça yararlanmaktadır. Örneğin, delillerin toplanması, tasnifi ve süreçlerin hızlandırılmasında önemli bir rol oynuyor. Ayrıca, dijital yargıçlar da yolda. Makineler daha mı adil olacak? Yoksa hata üstüne hata mı yapacaklar? Peşin hükümlü olmamak gerekir. Makinelerin çok daha adil olacağı durumlar da olacak, işlevsiz kalacakları durumlar da. Siyasi davalar ve bağımsız olmayan yargı süreçleri düşünüldüğünde makinelerin daha güvenilir ve daha adil bir yargı kurmaları olasıdır. Fakat verinin ötesinde bazı durumlar olduğunda makinelerin insanı anlaması veya insanca karar vermesi zor olacaktır. Gerçi makineden insanlık beklemek de tuhaf bir şeydir ayrıca.

Siber hukuka gelince o daha emekleme aşamasında. Ulusal düzeyde kısmen bir gelişme göstermesine rağmen, Uluslararası düzeyde çok daha zayıftır. Bazı bölgesel düzenlemeler var. Örneğin, Avrupa Konseyi'nin Siber Suçlarla Mücadele Sözleşmesi var. Afrika Birliği ve Arap Ligi'nin de benzer bazı düzenlemeleri var. Avrupa Birliği'nin bazı direktifleri var. Yani bölgesel düzeyde üç beş düzenleme var. Fakat küresel düzeyde yani Birleşmiş Milletler düzeyinde siber alanlar ilgili yapılmış bir uluslararası anlaşma henüz yok. Bu çok büyük bir sorun. Çünkü her ülke, özellikle büyük güçler, bu alanı farklı algılıyor ve farklı çıkarlar peşinde olduklarından anlaşamıyorlar.

Diğer önemli bir mesele, devletler siber alanı hukuk dışı bir alan olarak telakki ediyor ve öyle kalmasını istiyorlar. Kendilerini bağlayacak düzenlemelerden kaçınıyorlar. Başka bir husus, siber alanda fiziksel alanın aksine, egemen aktörler devletler değil şirketlerdir. Bu alanın süper güçleri özel şirketlerdir. Sosyal medya şirketleri ABD Başkanını bir anda siber alanda yok ediyorlar, etkisiz eleman haline getirebiliyorlar. Trump artık siber alanda adeta yok oluyor. Trump'ın aynısını onlara yapma gücü yok oysa. Devletler bu yeni gerçeği kabullenmek istemiyorlar. Siber uluslararası ilişkilerin devlet-merkezli bir alan olmadığını görmek istemiyorlar. Hala devlet dışı aktörlerle geleneksel ilişkiyi sürdürmek istiyorlar. Bu da mümkün değil. Ulusal ve uluslararası hukukun da buna göre yeniden dizayn edilmesi

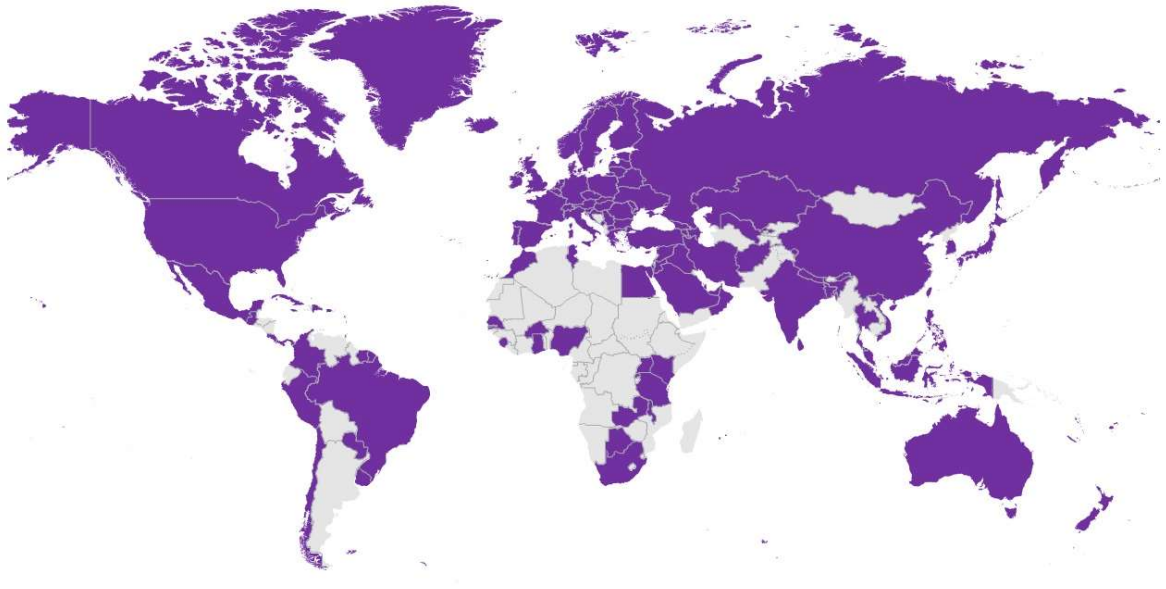
gerekiyor. Yani bütün paydaşların ya da uluslararası aktörlerin eşit temelde rol alacağı bir zeminin oluşturulması lazım. Aksi takdirde özgür ve güvenli bir siber uzay mümkün değildir.

SİBER UZAYDA HİÇBİR KULLANICI GÜVENDE DEĞİL

Hukukun dijitalleşmesi beraberinde ulusal siber hukuk durumu ve küresel siber hukuk durumu gibi başlıkları da gündemimize aldırmaya başladı. Türkiye bu alanda Avrupa ve diğer gelişmiş ülkeler ile kıyaslandığında hukuki altyapısı açısından ne durumda? Whatsapp, Facebook ile başlayan kişisel verilerimiz ne kadar güvende sorunsalına karşı, Türkiye ve Dünyadaki hukuki duruma dair bize ne söylersiniz?

Az önce hukukun genel durumunu tartıştığımız gibi, daha çok küresel düzeyde bir sorun var. Bazı ülkeler içerde daha kapsayıcı ve ileri adımlar atmış olabilirler, fakat internet küresel bir network. Ve siber saldırıların çoğu uluslararası nitelik taşır. Bu nedenle, ulusal düzeyde alınan önlemler çok sınırlı bir güvenlik sağlayabilir. Küresel bir sorun olan siber saldırılar ve siber güvensizlik küresel çapta bütün paydaşlar arasında (devletler, uluslararası örgütler, özel firmalar, siberle ilgili STK'lar) bir işbirliği ile ancak çözülebilir. Bireysel çabalar ancak sınırlı ölçüde çözüm sağlar.

Aşağıdaki harita Ulusal Siber Güvenlik Strateji Belgesine (USGSB) sahip ülkeleri gösteriyor. Afrika ve Latin Amerika'daki birkaç ülke dışında herkesin bu önemli belgesi var. USGSB bir ülkenin siber alanda yapmış olduğu hukuki düzenlemeleri, aldığı teknik önlemleri, siber güvenlikle ilgili organizasyon yapısı, halkta bilinç oluşturma ve teknik eleman yetiştirme dâhil toplumsal kapasite geliştirme veya siber güvenlik kültürü oluşturma ve uluslararası işbirliği ile ilgili faaliyetlerinin tümünü içeren kapsamlı bir belgedir. Türkiye geçen haftalarda üçüncü USGSB'ni yayınladı. Onun değerlendirilmesine girmek istemiyorum çünkü çok zaman alır. Ama en temel eleştirim etkin ve güçlü olabilmesi için, ulusal koordinatörlüğün bir bakanlığa değil, doğrudan Cumhurbaşkanlığına bağlı olması gerektiğini düşünüyorum.



Kaynak: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/National-Strategies-repository.aspx

Yine benzer kriterlere dayanarak BM Uluslararası Telekomünikasyonu Birliği (ITU) 2015 yılından beri küresel siber güvenlik endeksi hazırlıyor. 2018 endeksinde Türkiye 20. Sırada görece güvenli ülkeler arasında yer alıyor. Tabi yöntem itibariyle bu endeks pek güvenilir değil, ama yine de bir gösterge. Ülkeler siber uzayda sadece güvenlik üreten değil, aynı zamanda güvenlik tüketen aktörlerdir. Yani siber güvenlik sorunlarının önemli bir kaynağı devlet ya da devlet destekli gruplardır. Siber alanın doğası saldırıya açık olduğundan güvenlik hep sorun olarak var olmaya devam edecektir.

Özünde siber alanda gerçek bir güvenlikten bahsetmek zor. Yıllar önce Animal Planet TV'de bir belgesel izliyordum. Bir çita yanında birkaç yavrusu var. 60-70 metre ileride bir Aslan bakıyor. Ve sunucu "savanada hiçbir yavru güvende değil, çünkü hiç kimse komşusunun gerçek niyetinden emin değil" diyordu. Siber uzay için de aynısını söylemek mümkün. Siber uzayda hiçbir kullanıcı güvende değil, sadece komşularımızın niyetinden emin olmadığımızdan değil, hiç kimse komşusunun kim olduğunu dahi bilemez. Siber alanda mesafe ve sınır olmadığından herkes herkesle komşu. Veya siber alanı şöyle de tarif edebiliriz. Herkes şeffaf köşklerde yaşıyor. Özel hayat ve güvenlik bu alana yabancı. Siber güvenlik ürünleri sürekli gelişiyor fakat siber uzayın anarşik doğası nedeniyle gerçek bir çözüm zor.

DEVLET-DIŞI AKTÖRLER DÜNYANIN HER YERİNDEN İNSAN HAKLARINI İHLAL ETMEKTELER

Sizin insan hakları-dijitalleşme çağı arasındaki ilişkiye dair akademik makaleleriniz ve konferanslarınız sözkonusu. İnsan hakları teorisinde 3.dalga denilebilecek bir dijital insan hakları evresine mi giriyoruz diye sorsam? İnsan hakları mücadelesi dijital çağda nasıl şekil alır? İnsan hakları savunucularına neler önerirsiniz bu dijital çağ döneminde? Sizin "Siber güvenlik ve insan haklarında yeni paradigmaya ihtiyaç var mı?" isminde makaleniz var. Bu paradigmayı ve gündelik insan hakları mücadelesine yansımalarından bize bahseder misiniz?

Her alanda olduğu gibi, insan hakları da dijitalleşme sürecinden radikal bir şekilde etkileniyor. Bir taraftan ifade özgürlüğü imkânları genişlerken, eğitim hakkı muazzam olumlu etkilenirken, örgütlenme ve toplanma özgürlüğü, ekonomik haklar ve sosyal haklar gelişlerken, öbür taraftan siber gözetim ve istihbarat, özel hayatın gizliliği hakkı ve sansür gibi unsurlar insan haklarını olumsuz etkiliyor.

Geleneksel uluslararası insan hakları hukukuna göre, devletler insan haklarını ihlal eden ve yine insan haklarını korumaktan sorumlu tek aktördürler. Fakat siber alanda devletler insan haklarını koruyacak kapasitede değiller. Gerçi küreselleşme süreciyle birlikte uluslararası ilişkilerde ortaya çıkan yeni güçlü aktörler kısmen devletleri zorlamıştı, fakat siber uzay devletlerin sınırlarını iyice zorladı ve kapasitelerinin ötesinde alanlar oluşturdu. Artık devlet-dışı aktörler dünyanın her yerinden insan haklarını ihlal edebilirler ve etmektedirler. Bazen hukuki boşluk, bazen teknik yetersizlik ve bazen de kapasite yoksunluğu nedeniyle devletler bu ihlalleri engelleyemezler. Daha önce bahsedilen nedenlerden ötürü, devletler kendi aralarında işbirliği yapsalar bile insan haklarını korumaları kolay olmayacaktır. Tabi insan haklarını yine en çok ihlal eden aktörlerin devletler olduğu gerçeğini unutmamak gerekir.

Bu nedenle, tüm siber uzay paydaşlarının işbirliği ve tümünün ihlallerden doğrudan sorumlu tutulmasını sağlayacak yeni bir uluslararası insan hakları hukukuna ihtiyaç var. Geleneksel düşünen bazıları bu düşüncelere devletlerin egemenlik hakkından dolayı itiraz edebilirler. Fakat yeni bir toplumsal sözleşmeye ihtiyaç vardır. Bu yeni sözleşme yeni gerçekliğe uygun olarak çok katmanlı, sorumlu, sınırlı ve paylaşılmış bir egemenlik anlayışına dayanmalı. Yeni paradigma özünde yeni gerçekliği kavrayan ve insanı ve değerlerini koruyacak çok katmanlı, kişisel tercihleri merkeze alan yeni bir sözleşme. Bu yapılmadan insan haklarının korunması zordur.

EŞİTLİK FİKRİYATI ve ALLAH'IN "ONURLU YARATTIM" DEDİĞİ İNSAN MERKEZE ALINSA, KİBRE KAPILMAZSAK DİJİTAL NE DE MANUEL DİKTATÖRLÜK OLUR

Sizin altı ayda bir çıkan Siber Politikalar Derginizde "Dijital Savaşlar: Apple, Google, Microsoft ve İnternet Savaşı" isimli bir inceleme yazısı okudum. Dünya şirketler savaşına veya hegomonik mücadelesine mi sahne olmakta sizce? Yoksa bunu abartılı mı buluyorsunuz? Devletlerin rekabeti geride mi kaldı? Dijital diktatörlük başını alıp-gider mi? Matrix ve Yıldız Savaşları filmi yoksa gerçek mi oluyor?

Yeni bir dünya ile karşı karşıyayız. Google eski CEO'larından Eric Schmidt çok doğru bir tespit yapıyor. Diyor ki "internet insanoğlunun yaptığı ama anlayamadığı tek şeydir". Bana göre, siber alanla ilgili şimdiye kadar yapılmış en isabetli tespitlerden birisidir bu. Siber alanın anlaşılamadığının en tipik göstergesi 50 yıldır var olan ve son 30 yıldır World Wide Web (www)'in geliştirilmesiyle yaygınlaşan ve bugün 4.7 milyar tarafından kullanılan internetle ilgili hala bir teorinin geliştirilememesidir. Bilgisayar bilimciler de anlamadı, sosyal bilimcilerde tam olarak anlayamadı bu alanı. Geliştirmekle anlamak farklı şeyler tabi. Şöyle bir tespit var ki kısmen doğrudur. "Siber teknolojiyi teknisyenler ama siber disiplini (bilimini) sosyal bilimciler geliştirdi".

Bu alan çok dinamik, hızlı gelişen ve dönüşen bir alan olduğundan bilimin onu kavraması hele sosyal bilimcilerin güçlü teoriler geliştirmesi daha da zor. Bir gün mutlaka anlaşılacak, güçlü teoriler geliştirilecek belki ama bugüne kadar bu mümkün olmadı.

Her alanda olduğu gibi siber alanında da farklı aktörler arasında çeşitli düzeylerde bir rekabet ve hâkimiyet mücadelesi var. Çok güçlü aktörler var bu alanda. Özellikle şirketler. Bugün bütün dünya Zoom, Google Meet, Microsoft Teams gibi platformlarda eğitim yapıyor. 100 milyonlarca insan aynı anda online olabiliyor bu platformlarda. Hiçbir devletin böyle bir altyapısı yok. Buna ne diyeceğiz?

Devletlerarası çatışmalar da bu alana çekiliyor tabi. Estonya'ya yönelik DDoS saldırıları (2007), İran nükleer altyapısına yönelik Stuxnet saldırısı (2010), Suudi Aramco şirketine yönelik saldırı (2012), ABD başkanlık seçimlerine Rusya müdahalesi (2016) ve devletlerarası siber istihbarat süreçleri günden güne bu alanın artan faaliyetlerdir. Siber ordular giderek yaygınlaşan bir gerçeklik. Yine bu alana has çok yaygın olan ve "yeni vekâlet savaşları"

olarak bilinen yöntemle devletlerarası saldırıların devlet kurumları üzerinden değil, şirketler üzerinden düzenlenmesi meselesi var. Fakat şu var ki saf bir siyasi siber çatışmadan bahsetmek zordur. Bugüne kadar gözlemlediğimiz, bildiğimiz, literatürde yer bulan uluslararası siber siyasi çatışmalar genellik kinetik (fiziksel, geleneksel) bir çatışmanın devamı niteliğini taşımaktadır. Bahsedilen örneklerden de bu anlaşılıyor zaten.

Siber siyasi çatışmalar ya da abartılı da olsa savaşlar (ki teknik olarak bu çatışmalara savaş demek henüz doğru değil, ama bir kavram olarak literatürde sıkça kullanılıyor) var ve yeni teknolojilerle yeni yeni formlar kazanarak devam ediyor. Salt dijital bir savaştan bahsetmek zor, ama ileride de hibrit(karma) savaşlar ve çatışmalar şeklinde devam edecektir.

Dijital diktatörlük çok havalı bir kavram ama herkes kendinden daha diktatör olana diktatör diyor. İnsanlar bir dönüp kendilerine baksa, insanlara insan olduğu için saygı gösterse, eşitlik fikriyatını içselleştirse, insanlık onuruna değer verse, Allah'ın "onurlu yarattım" dediği insanı merkeze alsa ve şeytanın ameli olan kibre kapılmazsa ne dijital ne de manuel diktatörlük olur. Temennimiz dijitalleşmenin her türlü diktatörlüğü ortadan kaldıracak bir araca dönüşmesidir.

İnsanlık; savaş, yoksulluk ve ekolojik tahribat ile debelenirken hem dijital şirketlerin hem de silah şirketlerin payları nedense çok konuşulmuyor gibi. Dijital şirketler bize sevimli, albenili sunuluyor… Dijital emperyalizm diye kavramsal bir yaratıcılıkta bulunsam ya da şirket diktatöryalizmi (Twitter, Facebook, Instagram vb. hukuki ve mahkeme kararı olmadan Trump'un kullanımını yasaklamaları örneği veriliyor).
Siber alanda faaliyet gösteren şirketler giderek dünya ekonomisinden büyük paylar alıyorlar. Dijitalleşme arttıkça ekonomiden aldıkları pay da yükseliyor. Dünyanın ilk büyük yedi şirketinin altısı bilişim şirketleridir (Microsoft, Apple, Amazon, Alphabet, Facebook ve Alibaba) ilk 100 şirket için https://www.statista.com/statistics/263264/top-companies-in-the-world-by-market-capitalization/) içinde bu linke bakılabilir.

Bu şirketlerin gücü arttıkça tekelleşme ve dünya toplumunu sömürme ihtimalleri artacaktır. Her biri kendi alanında tekelleşen bu Big-tech firmaları aslında insan hakları ve demokrasi için de büyük bir risk oluşturabilirler. Bunu engelleyebilmek için özellikle uluslararası hukukla yeni önlemlerin alınması gerekir. Yoksa yarın kimsenin böyle bir hukuki düzenleme gücü de kalmayabilir. Bu şirketler küresel yönetişimde giderek daha çok söz sahibi olacaklar.

Tüm paydaşları sorumlu kılan yeni uluslararası düzenlemeler yapılmazsa, kaybeden hep insan olacak.

SİBER TEKNOLOJİ DÜNYAYA DOĞRUDAN DEMOKRASİ FIRSATINI DOĞURABİLİR

E-devlet derken; e-demokrasi, e-katılım, e-darbe gibi yeni siyasal katılım mekanizmaları ve süreçlerinin gelişen iletişim/bilişim teknolojileriyle daha fazla görünür olduğunu görüyoruz. Birey ve toplumların bu e-demokrasi, e-katılım süreçleri demokrasiye dair yeni kuramları doğuracağı söylenmekte. Bu iş nereye evriliyor sizce? Küresel çapta bir demokratikleşme dalgasına yol açar mı? Mesela sosyal medya araçları demokratikleşmeye destek mi köstek midir sizce?

E-demokrasi ve e-katılım gibi imkânlar demokrasiyi bambaşka noktalara taşıyabilir. Eski Yunan şehir devletlerinde doğrudan demokrasi vardı. Yani karar-alma süreçlerinde oy hakkına sahip olan herkes doğrudan etkin rol alabiliyordu. Tabi o zaman sınırlı bir katılım vardı. Genellikle yetişkin erkek vatandaşlar veya yetişkin zengin erkek vatandaşlar söz sahibi idi. Fakat bu sınırlı katılıma rağmen toplumsal kararlar vatandaşlar tarafından alınırdı. Buna da doğrudan demokrasi denir. Doğrudan demokrasi zamanla ülkelerin nüfus artışı ve toprakların genişlemesiyle imkânsız hale geldi ve bugünkü (temsilciler aracılığıyla ülke yönetimine katılmak anlamına gelen) temsili demokrasiye dönüştü. Temsili demokrasinin ne kadar demokratik (katılımcı) olduğu konusunda literatürde hep devam eden bir tartışma var. Fakat bugün siber teknoloji dünyaya yeniden doğrudan demokrasi fırsatını doğurabilir. Güvenli ve herkesin erişim imkânına sahip olduğu bir internet oluşturulabilirse hem toplumlar düzeyinde hem de dünya düzeyinde doğrudan bir demokrasi inşa etmek mümkündür. Cris Brown ve Terry Nardin'in hayalini kurduğu Küresel (doğrudan) demokrasi, küresel adalet ve küresel sorunların işbirliği ile çözülmesi de mümkün olabilir. Tabi bunların hepsi ihtimal ve ütopya ama imkânsız değil.

Tam tersine az önce değinildiği gibi, siber teknoloji ulusal ve/ya küresel bir distopyaya da dönüşebilir. George Orwell'ın 1984 distopyası gerçek olabilir ki bazı ülkelerde bu yönde ciddi adımlar da atılıyor. Covid-19 virüsü ya da Pandemi bahane edilerek toplumsal denetim mekanizmalarını sıkılaştıran bir dizi otokrasiler var dünyada.

Bu süreci toplumsal denetim ağına dönüştürmek isteyen diktatörler ya da baskıcı rejimler dijital araçları da kullanarak daha da kalıcı ve sürekli hale getirmenin arayışındadırlar. Çin'in

sosyal kredilendirme sistemi bunun tipik girişimleridir. Dünyanın dört bir yanında az veya çok bu yönde atılan adımlar var. İşte bu noktada düşünürlerin, akademisyenlerin ve demokrat bireylerin uyanık olması, toplumu uyarması, önlem alması ve distopya yerine ütopyayı inşa etmeye yardımcı olması gerekir. Demokrasi nazik bir rejimdir, sürekli korunması ve kollanması gerekir. ABD gibi oturmuş bir demokraside bile bir deli gelir ve halkın iradesini teslim alır. Bu olayın tüm dünyaya ders olması lazım. Demokrasiyi içselleştirmemiş, halkın iradesine saygısı olmayan, eşitliği benimsemeyen kişilerin iktidara gelmesi insanlık için büyük bir tehdit. Fırsat vermemek lazım.

KOMPLOLAR TOPLUMUN AFYONUDUR, HEM MUTLU EDER HEM DE SARHOŞ

Uluslararası ilişkiler alanındaki akademisyen kimliğinize binaen, küresel İlişkileri okuma biçimlerini konuşalım istiyorum. Küresel ilişkileri; komplocu okuma biçimi, realist okuma biçimi, normatif ya da ahlaki/etik okuma biçimi, eko-politik okuma biçimi, liberal okuma biçimi… şeklinde uzayıp giden bir liste var. Türkiye'nin dış politikasında hangi okuma biçimi öne çıkmakta sizce? Bir de toplum olarak küresel olaylara dair okuma biçimimizi de ele almanızı istesem ne dersiniz?

Türkiye'nin veya başka bir ülkenin dış politikasıyla ilgili böyle bir genelleme yapmak sağlıklı bir okuma olmayabilir. Zaman, mekân, aktörler ve olaylar bazında farklı yaklaşımlar görmek mümkün. Çoğu zaman bizleri pek etkilemeyen örneğin Latin Amerika'daki bir olaya daha realist yaklaşırken, Filistin'de daha etik, büyük güçlerle ilişkide daha liberalimsi yaklaşımlar görülüyor. Olay ve zamana bağlı olarak aynı bölgelere yönelik farklı yaklaşımlar gözlemlemek de mümkün. Demokratikleşme ve dışa açılma dönemlerinde daha gerçekçi, etik ve normatif yaklaşımlar karışımı bir eğilim egemenken, içe kapanmacı ve otokratik eğilimlerin arttığı dönemlerde daha komplocu eğilimler öne çıkmaktadır.

Sadece Türkiye'de değil, genelde kitleler/toplumlar komplocu eğilimlere daha yatkındırlar. Nedeni, kafa konforu sağlaması. Düşünmek, ölçmek, biçmek, objektif olma çabası hem kapasite hem bilgi hem de çaba gerektirir. Bu da herkesin altına gireceği bir yük değildir. Komplolar toplumun afyonudur. Onu hem mutlu eder hem de sarhoş. O nedenle, çok ama çok tehlikeli sonuçlar da doğurabilirler.

İnternet tam da bu iş için yaratılmıştır sanki. Algı oluşturmak için birebirdir internet. Toplumları yönlendirmek, manipüle etmek, kontrol etmek ve gözetlemek hepsi de internetin

işi. Bu nedenle, internetin yaygınlaşmasıyla beraber tüm dünyada komplo teorileri hem arttı hem de yaygınlaştı. Pandemi döneminde virüsün Bill Gates tarafından insanlara microchip taktırmak için geliştirildiği, ya da Çin veya ABD tarafından laboratuvarda üretildiğine dair bir sürü komplo teorileri geliştirildi. Aşılamayla bile microchip takıldığına dair komplolar havada uçuşuyor. Ve bütün dünyada büyük bir teveccüh gördü bu komplo teorileri. Komplo teorilerinin mantıklı ya da tutarlı olması gerekmiyor, hatta mantıksız ve tutarsız olması çoğu zaman onu daha da popüler yapıyor.

SOSYAL MEDYA ONLINE SOSYALLEŞİRKEN, OFFLINE İLİŞKİLERİ VE DAVRANIŞLARI UNUTTURUYOR

Sosyal medya araçları ve toplumsal değişim üzerine konuşalım isterim. Sosyal medyanın insanlığın kanseri olduğuna dair bir twitinizi gördüm. Bireyi veya toplumu hastalıklı kılan tarafı nedir? Memleket olarak sosyal medyayı nasıl görüyor ve nasıl kullanıyoruz sorusunu metaforik veya teşbih sanatıyla anlatın denilse size, bunu nasıl anlatırdınız?

Evet, sosyal medya insanlığın kanseridir gerçekten. Birkaç nedenden dolayı böyle düşünüyorum. Birincisi, kanser bir vücuda girdiğinde yavaş yavaş yayılır ve en sonda onu yok eder. Sosyal medya adının tersine kişileri ve toplumları asosyalleştiren bir fonksiyon görüyor. Online sosyalleşirken offline ilişkileri ve davranışları unutturuyor. İkincisi, üretkenliği öldürüyor. Yapılan araştırmalara göre dünya çapında internette geçirilen zamanın %80'i sosyal medya platformlarında geçiriliyor. Geri kalan sadece %20 iletişim, araştırma-geliştirme, okuma ve üretim gibi faydalı işler için kullanılıyor. Sosyal medya bu yönüyle bir oyalamaca ya da sosyal medya hayatı bir oyun ve eğlenceden ibarettir aslında. Üçüncüsü, sosyal medya platformları insanları radikalleştiriyor. Kodlar öyle tasarlanmış. Bir şeye bakıyorsunuz, sonra aynı konuda onlarca video, yazı ve resim geliyor ve insanların radikalleşmesini sağlıyor. Irkçı eğilimi olan birisi bir video izleyedursun. Ardından ırkçılıkla ilgili onlarca video gelecektir. Bu da radikalleşmeye hizmet eder. Dördüncüsü, insanlarda sürü psikolojisini oluşturuyor, toplumu kutuplaştırıyor ve bölmeye hizmet ediyor. Twitter'deki TT konularına bakın, normalde çok ılımlı, makul ve aklı başında insanlara bakıyorsun kendi mahallesinde boy göstermek için çok sert, tutarsız, seviyesiz ve ahlaksız twitler yazabiliyor. "Hayırlı Cumalar" konusunun altında bile bir dizi kombine küfür görebiliyorsunuz. Çünkü kullanıcılar TT akışına kendisini kaptırıyor, sürü psikolojisine tutuluyor ve rasyonaliteyi kaybediyor. Bütün bu aşırılıklar toplumu kutuplaştırıyor ve parçalıyor. Normalde yüz yüze olsa söyleyemeyeceği bir sürü mesajı ekranda rahatça paylaşabiliyor.

Sosyal medyada herkes mirketleşiyor. Mirketler hep iki ayaküstüne kalkıp etrafta bir tehdit var mı diye hızlı, çevik ve aynı zamanda sempatik bir şekilde etrafı gözetliyor. İnsanlar da sosyal medyada görünmek için kafalarını uzattıkları bir mecra. Hep birileri onları görsün, "hey, bak buradayım!" tavırları. Bol bol fotoğraf çeker, etkinlik paylaşır, twit atar, story oluşturur, durum paylaşır, yemek, ideoloji ve hatta öfke paylaşır…

HAK TEMELLİ DİJİTAL VATANDAŞLIK EĞİTİMİ VERİLMELİ

Siber siyaset ve siber güvenlik çalışmalarınız salt tespit ve sorunlar üzerine değil, çözüm önerilerine de kafa yoran bir akademisyensiniz. Siyasi elitlere veya iktidarlara şayet ulusal siber güvenlik stratejisi veya siyasi partilere siber siyaset vizyon belgesi hazırlama görevi verilseydi şayet size, bu strateji ve vizyon belgesinin yapısı, kapsamı ve ilkeleri neler olurdu diye sorsam?

Siber alanda sorunlar çok ama çözümsüz değiller tabi. Öncelikle siber alan fiziksel alanın devam ve öyle algılamakta fayda var. Ulusal siber güvenlik strateji belgeleri (USGSB) ve siyasi partiler için önerdiğim siber siyaset vizyon belgelerinin amacı özgür ve güvenli bir siber uzay oluşturmak olmalı. Hedef belli olduktan sonra yöntem ve stratejiler belirlemek kolaydır. Bu nedenle, bu belgelerin ruhu ve özü hukuk ve insan hakları olmalıdır. Bugün dünyada bu nitelikte bir vizyonu benimseyen bir belge yok maalesef. Kısmen daha fazla dokunanlar olabilir, örneğin Hollanda USGSB bu anlamda öne çıkıyor fakat o bile fazla eksik. Özellikle internete erişimin bir insan hakkı olarak tanımlanması, unutulma hakkının kodifiye edilmesi, çevrenin, gençliğin ve ailenin korunması için düzenlemelerin yapılması gerekir.

Siber güvenlikte en zayıf halka bireydir. Bu nedenle, bireyin siber yetenek kazanması ve siber güvenliği fark etmesi için eğitilmesi ve merkeze alınması gerekir. Siber güvenlik kültürünün oluşması lazım. Bu çerçevede, hak-temelli bir dijital vatandaşlık eğitimin verilmesi gerekir. Başta Avrupa Konseyi olmak üzere, birçok uluslararası örgüt bu alanda çalışmalar yapıyor, fakat bu çabalar yetersiz. Hükümetlerin, sivil toplum kuruluşlarının ve eğitim kurumlarının bu işe acilen el atması gerekir.

Oysa bugün dünya çapında yaygın olarak yapılan şey siber uzayın güvenlikleştirilmesidir. Bu da insan hakları ve siber güvenliğe çok zarar verir. Güvenlikleştirme ile güvenlik kültürünü karıştırmamak lazım. Fakat bunu bilinçli yapan bazı aktörler vardır. Bunlar daha rahat düzenleme yapmak ve alanı kontrol etmek için devletler, daha çok ürün satmak için siber

güvenlik firmaları ve maalesef bilmeden bazı akademisyenler de kullandıkları kavramlar(sürekli siber savaş, siber tehdit, siber güvensizlik gibi negatif kavramlara ağırlık vererek böyle bir zihniyet inşa etme sürecine katkı sağlıyorlar), abarttıkları konular ile bu sürece yardımcı oluyorlar. Biz dergimizde doğrudan alıntı olmadığı sürece siber savaş yerine siber çatışmayı tercih ediyoruz. Çatışma da olumsuz bir kavram ama en azından savaştan daha az olumsuz.

Bir yazınızda (11 Ocak 2021 tarihli Perspektifonline sitesi) sosyal medyanın; toplumsal etkileşimi, sosyal değerleri, siyasal süreçleri ve çatışma dinamiklerini değiştirmeye dönük olumlu-olumsuz tarafları olduğunu, bazen bir siyasal aktör gibi davrandıklarını söylüyorsunuz. Bize bunu somutlaştırır mısınız? Olumlu-olumsuz taraflarından bahseder misiniz?

Sosyal medya; iletişim, ticaret, haberleşme, örgütlenme, demokratikleşme, katılım, ifade özgürlüğü ve eğitim hakkının gelişmesinde önemli bir güç olabilir. Fakat tam tersine big-tech firmaları bu alanda tekelleştiklerinden ve devletlerin siber gözetim ve istihbarat faaliyetleri sonucu demokratikleşme ve insan hakları alanında ciddi zararları da olabilir. Bu nedenle, devletlerin siber uzay faaliyetlerinde özellikle gözetim ve istihbarat süreçlerinde hukukilik, orantılılık, meşruiyet, şeffaflık, hesap verebilirlik çok ama çok önemlidir. Yine Google, Facebook, YouTube, Twitter, Whatsapp, Instagram ve Pinterest gibi tekel oluşturan big-tech firmalarının bu gücü kötü kullanmasını sınırlandıracak yeni uluslararası hukuki düzenlemelere ihtiyaç vardır.

Büyük veri ve blok zinciri teknolojisiyle insanlara çok büyük faydalar sağlanabileceği gibi yine bu teknolojilerle insanlar tamamen sömürülebilir de. İnsan hakları ve demokratikleşme rafa kaldırılabilir de. Siber uzayın etik kullanımı, insan yüzlü bir siber uzay için yoğun bir çaba lazım aksi takdirde tüm insanlık kaybedecektir.

Siber Politikalar Dergisi (A Peer Review International E-Journal on Cyberpolitics and CyberSecurity) ismiyle Türkiye'de benzeri olmayan ilk ve tek uluslararası hakemli akademik bir dergi çıkarıyorsunuz. Derginizin geçmişten bugüne değin serüvenini, ele aldığınız temaları, neleri başarıp neleri başarmadığınıza dair bize neler söylemek istersiniz?

Teşekkür ediyorum. Evet, Cyberpolitik Journal (Siber Politikalar Dergisi) Türkiye'nin ilk ve tek ama aynı zamanda dünyanın siber politika ile ilgili ilk hakemli akademik dergilerinden

birisidir. Altıncı yılına giren dergi çok mesafe aldı. Dergimizin alt başlığı siber güvenlik, siber politika ve insan haklarıdır. Bu nedenle, önceliğimiz etik bir siber uzayın gelişmesine katkı sağlayabilmek. Her sayıda insan hakları, etik ve dijital vatandaşlık ile ilgili konulara yer vermeye çalışıyoruz.

Bugüne kadar, birçok seminer, çalıştay (ODTÜ'de) ve uluslararası konferanslar düzenledik. Uluslararası düzeyde İstanbul Bosphorus International Conference on Cybersecurity, Cyberpolitics and Social Sciences adında 2020'de dördüncüsünü yaptık bu yıl beşincisini yapma çalışmalarına başladık. Dergi ve konferans Türkiye ve dünyadan bu alanda çalışan akademisyenler için önemli bir platform oluşturdu.