Araştırma Makalesi Doi: 10.5281/zenodo.7081703

ULUSAL GÜVENLİK TEHDİDİ BOYUTUNDA SOSYAL MEDYA İNCELEMESİ[1]

1. Ahmet Emin Cerrah[2] **ORCID No 0000-0001-7685-2777**

2. Oya Dağlar Macar[3] **ORCID No 0000-0002-8163-8721**

Başvuru Tarihi: 08.07.2022 Kabul Tarihi: 15.07.2022 Yayın Tarihi: 14.09.2022

ÖZET

Kullanıcıların karşısına web 2.0 döneminde çıkan ve günden güne artan kullanımı ile siber uzayın fenomen ürünlerinden bir tanesi haline sosyal medya platformları, kullanıcılarına kolaylıkla erişim sağlayarak paylaşım yapabilmesi açısından sunmuş olduğu imkanlar dolayısıyla muazzam bir veri kaynağına dönüşmüştür. Ticaret, eğlence, siyaset ve habercilik gibi birçok alana ve farklı yaş gruplarına hitap etmesinin yanı sıra gerek devlet liderlerinin sosyal medya patronları ile yaşadığı sıkıntılar, gerek son yıllarda sayısı artan siber saldırılar ve neticesinde gündeme gelen veri güvenliği konusunda ki tartışma konuları, gerek ise sosyal medya bünyesinde gerçekleşen tehdit çeşitlilikleri sebebiyle devletlerin sosyal medyayı ulusal güvenlik tehdidi olarak ele alması özgürlük mottolarının sıkça kullanıldığı internet aleminde tartışma konularına sebebiyet vermiştir. Bu bağlamda hazırlanan bu çalışma nitel bir araştırma makalesi olup, devletlerin sosyal medya platformlarını ulusal güvenlik tehdidi olarak görmelerindeki motivasyonun ne kadar doğru veya yanlış bir karar olduğunu test etmeyi amaçlamaktadır. Kapsam açısından sosyal medyadaki güvenlik tehditlerinin son derece fazla olmasından kaynaklı olarak çalışmada sınırlı sayıda tehdit ele alınmıştır.

Anahtar Kelimeler: Siber Güvenlik, Ulusal Güvenlik, Ulusal Güvenlik Tehdidi, Sosyal Medya, Strateji

SOCIAL MEDIA REVIEW AS A NATIONAL SECURITY THREAT

ABSTRACT

Having emerged in the web 2.0 era and getting more and more widespread, social media platforms, one of cyberspace's popular outputs, have turned into a great source of data due to the easy access and sharing opportunities they provide for users. Despite the wide range of topics it covers, such as business, entertainment, politics or journalism, and various age groups it attracts, social media has become a matter of debate on the internet, which is known for its emphasis on freedom, due to the issues world leaders have with social media bosses as well as data security becoming an issue because of the recently-increased cyberattacks and social media being perceived as a threat to national security by governments because of various threats encountered on the internet. This is a qualitative research paper on this matter, which aims to determine whether the motivation behind governments' decision of perceiving social media platforms as a threat to national security is reasonable or not. This paper covers only a limited number of threats due to the excessive number of security threats on social media.

Keywords: Cyber Security, National Security, National Security Threat, Social Media, Strategy

[1] Bu makale yüksek lisans tez çalışmasından türetilmiştir.

[2] Ahmet Emin Cerrah, İstanbul Ticaret University, aemincerrah@gmail.com

[3] Oya Dağlar Macar, Prof. Dr., İstanbul Ticaret University, oyadr@ticaret.edu.tr

1. GİRİŞ

Bilgi, insanlığın başlangıcından bu yana hayati önem taşıyan bir ürün olma özelliği taşımaktadır. Tarihte birçok devlet adamı, komutan ve general bu önemin farkında olmasından dolayı bilgiye diğer değişkenlerden farklı bir anlam yüklemiştir. Buradaki bahsi geçen bilgi yalnızca gündelik yaşamdan tecrübe edilen bilgiler veya teknik bilgiler değil aynı zamanda istihbari bilgileri de kapsamaktadır. Bu bağlamda bilgi farklı alanlarda etkisini gösterdiği gibi insanın tehdit ve tehlikeden uzak, hayatta kalma içgüdüsü ile ortaya çıkmış olan güvenlik kavramında da kilit bir rol oynamaktadır. Tarihsel sürecine bakıldığında, geçmiş yıllarda bilginin muhafazası somut bir şekilde sağlanırken teknolojik gelişmelerin bir ürünü olarak, orijinsi Soğuk Savaş dönemine dayanan "internet" ile yeni bir iletişim imkânı doğmuş ve bilgi, geleneksel muhafaza yönteminden sıyrılarak "siber alanda" depolanmaya başlanmıştır. Başlangıçta bilginin kolay depolanması ve paylaşımının eskiye nazaran çok daha hızlı olması gibi pozitif yönleri birçok farklı zümreye etkilemiş olsa da gün geçtikçe siber alanın kendisi bir tehdit haline gelmeye başlamıştır. Yapısı gereği anarşik olan bu bilgi ekosisteminin bünyesinde çok fazla aktör bulundurmasının yanı sıra verilerin siber alanda nasıl korunacağı da yeni bir sorunsalı beraberinde getirmiştir (Yeşilmen, 2018, s.53).

Yeni medya olarak da adlandırılan "sosyal medyanın" ortaya çıkmasıyla beraber bu anarşik yapı daha da kompleks bir hale gelmiştir. Sosyal medya ağlarını kullanan bireysel kullanıcıların sayıları arttıkça bu mecraya yeni aktörler de dâhil olmaya başlamıştır. Kullanıcıların kendi elleriyle kişisel verilerini farklı doküman formatlarında (yazı, video, fotoğraf vb.) paylaştığı bu devasa veri tabanı; anket, reklam ve pazarlama gibi özel şirketlerin yanı sıra istihbarat birimlerinin de ilgi odağı olmuştur. Veri gizliliği ve güvenliği sorunu henüz çözüme kavuşturulamamışken, sosyal medyaya gösterilen bu yoğun ilginin sürekli olarak artması ciddi anlamda bilgi kirliliğine de sebebiyet vermiş ve hali hazırda güvenlik endişeleri barındıran bu platformu yanlış yönlendirmelere, algı operasyonlarına ve sosyal mühendisliklere karşı savunmasız bir hale getirmiştir. Bu durum ise genel anlamda siber dünyaya çok geç dâhil olan devletler için büyük bir tehdit haline gelmiştir.

Soğuk Savaş sonrası dönemde Yeni Dünya Düzeni'nin ve küreselleşmenin bireycilik, özgürlük gibi kavramlara etkilerinin siber alanın bünyesinde de tezahür ettiğini söyleyebiliriz. Sınırların henüz belirlenmediği, kullanıcıların özgür bir biçimde erişim sağlayarak etkileşimde bulunabildiği ve devletlerin uluslararası iş birliği ile örgütsel bir şekilde kontrol edip, denetleyemediği bu alan, ciddi bir güvenlik tehdidi haline gelmiştir. İnternetin bireylerin kullanımına açılması ile günden güne farklı etkileşim araçlarının meydana çıkması ile siber âlem yavaş yavaş -esasında teknolojik bir ürün için kullanılan- "sanal gerçeklik" haline getirmiştir. Bu kavramı biraz açmak daha faydalı olacaktır çünkü bu denli ticari imkânlar sunan ve bilginin elde edilmesinde sağladığı olanaklar gibi pozitif efektleri bulunan bir ürünü altı doldurulmadan aktarılan bir kelime ile havada bırakmak sağlıklı olmayacaktır. Oyuncaklar nasıl ki çocuklara hitap ederken genç veya yetişkinlere hitap etmiyor, aynı şekilde gazete okumak veyahut haber izlemek yetişkinlere hitap ederken gençlere ve çocuklara hitap etmiyorsa, bu örneklerin aksine siber âlem insanların kesişim noktasında bulunan bir uygulama alanı özelliği göstermektedir. Her kesimden insanı bünyesinde bulundurabilmesinin altında ki neden ise siber âlemin cümlenin "gerçeklik" kısmında anlatılmak istenen özelliğinden kaynaklanmaktadır. Bireylerin geleneksel olarak yapabileceği birçok (günümüzde neredeyse tamamı) aktivitenin siber âleme taşınması ile internet adeta bir temel ihtiyaç haline gelmiştir. Bu mecranın imkanları sayesinde insanlar birbirleri ile çevrimiçi etkileşimlerde bulunarak, ticaret yaparak, eğlenebilerek hatta yeni insanlar ile tanışıp network kurabilmektedirler. Siber alemi "sanal" kılan yegâne durum ise burada somut bir kimliğinizin olmamasıdır. Teknik yeterlilik ile rahatlıkla gizlenebilecek IP numaranız dışında birey kendisini burada olmak istediği şekilde tanıtabilmektedir ve toplum içinde belirtmediği veya belirtmekten çekindiği düşüncelerini burada rahatlıkla insanlara aktarabilmektedir. Tabi ki bu motivasyonun arka planında ki psikolojik durum çok farklı bir çalışma alanı olmakla birlikte siber güvenlik konusunda farkındalık kazandırabilmek adına ciddi çalışmaların yapılması gereken bir başka konu başlığıdır.

Son dönemlerde halkın belli bir kesiminden büyük tepkiler almasına rağmen birçok devlet başkanının siber alemin önemli ürünlerinden bir tanesi olan, sosyal medyayı denetlenmek ve gerektiğinde sansür uygulaması yapılarak kontrol etmek gibi eylemleri öngören sosyal medya hukukundan bahsetmesi, devletlerin artık sosyal medyayı bir ulusal güvenlik tehdidi olarak gördüklerini teyit eder niteliktedir.

Bu bağlamda hazırlanan bu çalışma öncelikle ulusal güvenlik ve tehdit kavramlarına değinerek, sosyal medyanın ulusal güvenlik tehdidi olarak görülmesinin ne kadar doğru bir yaklaşım olduğunu test etmeyi amaçlamaktadır.

2. ULUSAL GÜVENLİK KAVRAMI

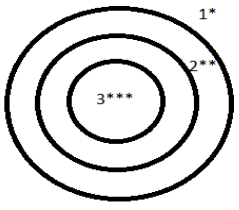
Güvenlik kavramı, Latince; endişesiz, kaygısız, güvenli anlamına gelen "*sēcūrus"* kelimesinden türetilmiştir ve kökeni; güvenlik, emniyet anlamına gelen "*securitas"* kelimesine dayanmaktadır. (Etimoloji, 2021) Güvenlik kavramının tanımlanmasında ise farklılıkların görülmesi; güvenliğin kişiden kişiye, devletten devlete, bölgeden bölgeye ve zamandan zamana değişken bir yapıya sahip olmasından kaynaklanmaktadır. Örneğin Helenistik felsefenin düşünürlerinden olan Epikür, mutlu bir yaşamın nihai amacının "bedendeki acılardan ve zihindeki sıkıntılardan kurtulma" olduğunu ve amaca ulaşmak için kişinin kendisine güvenlik sağlaması gerektiğini ifade etmiştir (Britannica, 2021).

Orta Çağ döneminde ise Batı'da Roma İmparatorluğu'nun sona ermesi pax veya barış ile eş anlamlı olarak kullanılan "securitas" kavramının da sonunu getirmiştir. Orta Çağ döneminde "securitas" M.S. 1. Yüzyılın aksine ne merkezi bir kavram ne de bir slogan olarak kullanılmamıştır (Arends,2008, s. 271).

Aydınlanma düşüncesinde ise bireylerin toplumsal hayata entegrasyonu sırasında meydana gelen çatışmalar güvenlik ihtiyacı olarak ele alınmıştır. Kant, Grotius, Rousseau ve Hobbes gibi düşünürler insan doğası üzerine çalışmalar yapmış ve toplumsal alanda meydana gelen savaş, barış, güvenlik, çatışmalar, güvende olma ve devletin oluşumu gibi durumları bu bağlamda açıklamaya çalışmışlardır (M. Salih Elmas, 2013, s. 22).

Ulusal güvenlik kavramı ise ilk olarak ABD'nin 1947 yılında dış politikasının ve askeri yapılanmalarının düzenlenmesini öngören "Ulusal Güvenlik Yasası" ile gündeme gelmiştir.[4] (U.S. Department of State, 2021) Fakat II. Dünya Savaşı'ndan sonra ilk olarak bu yasa ile kullanılan ulusal güvenlik kavramı basit bir tanımlamadan öteye gidememiş ve altı doldurulamamış, yani kavramdan daha çok bir politika olarak karşımıza çıkmıştır. Ağırlıklı olarak ABD'nin Soğuk Savaş dönemindeki anti komünist faaliyetlerini kapsayan ulusal güvenlik kavramı zamanla ülkelerin çıkarları doğrultusunda iç ve dış politikalarını kapsayacak şekle evrilmiştir. Bu yüzden güvenlik, strateji, istihbarat gibi günümüze ait olduğu düşünülen kavramlara retrospektif yaklaşmak kavramların tanımlanmasında daha sağlıklı sonuçlar elde etmemize yarayacaktır. Aynı zamanda diğer birçok kavramdan farklı olarak güvenlik kavramının ontolojik bir altyapıya sahip olmasından ötürü kavramın açıklamasında dikotomik yaklaşım faydalı olacaktır. Siyah ve beyaz, iyi ve kötü gibi güvenlikte, güvende olma hali yani tehditlerin ortadan kalkmasına bağlıdır. (Fikret Birdişli, 2011, s. 150-151)

Bu bağlamda ulusal güvenlik kavramını tanımlarken dikkate alınması gereken bazı ek kavramlar bulunmaktadır. Bunlar; risk, tehlike, tehdit, güç ve ulusal çıkarlardır. Risk, tehlike ve tehdit kavramlarını güvenlik çemberinde iç içe geçmiş üç halka olarak tasvir edebiliriz. Birinci halka risk, ikinci halka tehlike ve son halka ise tehdittir.



*: Risk
**: Tehlike
***: Tehdit

Şekil 1- Güvenlik Çemberi

[4] Yine bu yasa neticesinde günümüzde ABD'nin dış istihbarat servisi olarak görev yapan CIA yapılanması kurulmuştur.

Bu üç faktörü Beril Dedeoğlu komşu ve silah betimlemesiyle basit bir şekilde örneklendirmiştir. Komşumuzun evinde bir silahı olduğunu bildiğimizi ve bahçemize oturmak için dışarı çıktığımızı varsayalım. Komşumuzun evinde silah bulundurması bir risktir. Biz otururken komşumuzun elinde silahı ile dışarı çıkması ise tehlikedir. Elindeki silah ile bizim bulunduğumuz konuma doğru nişan alması ise tehdit boyutudur. Bu bağlamda risk, tehlike veya tehdit analizlerinde algı ve olgu ayrımının önemi karşımıza çıkmaktadır. Çünkü elinde silah ile dışarı çıkıp silahı bize doğrultan komşunun bizi hedef alma ihtimali bulunduğu gibi yalnızca silahın namlusunu kontrol etme gibi bir amacı da olabilir (Beril Dedeoğlu, 2014, s. 27-33). İçgüdüsel bir durum olan güvenlik ihtiyacı sebebiyle devletlerde bu aşamada algı ve olguları iyi ayırt etmek durumundalardır. Aksi takdirde herhangi bir riskli durum barındırmamasına rağmen kaynakları bu doğrultuda boş yere harcamak durumunda kalabilirler. Örneğin; komşu ülkelerde yaşanacak bir iç savaş ile ortaya çıkabilecek kontrolsüz göç dalgası veya sınır güvenliğinin risk analizinde olgusal bir yaklaşım söz konusu olacaktır. Analiz yapılırken kullanılabilecek somut veriler sayesinde öngörü oluşturulabilecektir. Fakat herhangi bir bilimsel kanıtı olmadan bir ülkenin uzaylı istilası için bütçe ayırması algısal bir yaklaşım olacak ve kaynakların boşa harcanmasına sebebiyet verecektir. Bu gibi olgu algı ayrımı ile alakalı örnekler daha detaylı bir şekilde ülkeler arası ilişkilerde dahi görülebilir. Bu bağlamda olgu ve algı ayrımı ulusal güvenlik açısından sağlıklı politikalar üretebilmek için elzem niteliktedir.

3. ULUSAL GÜVENLİK TEHDİDİ BOYUTUNDA SOSYAL MEDYA

İnternet her ne kadar günümüze çok yakın bir tarihte ortaya çıktığı düşünülse de aslında bir Soğuk Savaş ürünüdür. SSCB ve ABD'nin uzay ve teknoloji yarışı neticesinde ABD Savunma Bakanlığı'nın bir kolu olan DARPA, 1969 yılında paket iletim sistemini geliştirerek ARPANET projesini hayata geçirmiştir (İTÜBİDB, 2013). Bilginin taşınması, paylaşılması ve muhafazası bağlamında geleneksel yöntemlerden sıyrılarak siber alanı kullanmayı öngören ARPANET projesi, tek merkez kullanmaktan ziyade farklı noktalarda çok merkezli bir sistem üzerine inşa edilip herhangi bir noktanın saldırıya maruz kalması durumunda sistemin aksamadan devam etmesini amaçlamaktaydı. Bu yüzden günümüzde internetin çok merkezli bir yapıya sahip olmasının nedeni, internetin ilk kurulduğu bu dönemlerde siber güvenlik tehditlerinden ziyade fiziki güvenlik tehditlerinin düşünülerek hareket edilmesinden kaynaklanmaktadır (Nezir Akyeşilmen, 2018, s. 26).

İlerleyen süreçte internetin bireylerin kullanımı açılması ve 1989 yılında İngiliz bilim insanı Tim Berners-Lee'nin World Wide Web (WWW) uzantısını icat etmesi ile internet tamamen farklı bir boyut kazanmıştır. 90'lı yıllar interneti için kullanılan web 1.0 döneminin günümüze kıyasla çok daha statik ve tek merkezli bir yapısı bulunmaktaydı. İnternette içerik paylaşmak isteyen bir kullanıcının asgari düzeyde programlama ve grafik yeteneklerine, paylaşacağı içeriği yükleme için FTP yazılımına ve bunları yapabilecek bir sunucuya ihtiyacı bulunması internetin geleneksel medya tarzında işlemesine neden olmuştur (Jane Bozarth, 2010, s. 11-13). Fakat küreselleşme ve dijitalleşmenin de etkisiyle artık kullanıcıların ihtiyaçlarını karşılayamaz hale gelen bu yapı web 2.0 dönemini getirmiştir ve bu dönemle birlikte internet artık daha dinamik ve çok merkezli bir yapı halini alarak karşımıza sosyal medya platformlarını da çıkarmıştır.

Sunmuş olduğu eğlence ve ticaret gibi hizmet imkanlarının yanı sıra birbirinden farklı birçok platformun orijinal içerikler barındırması, sosyal medya platformlarını belirli bir yaş kitlesine kilitlenmekten kurtarmıştır ve her yaş grubundan insana çekici gelmesini sağlamıştır. Sosyal medya kavramı, A. Kazım Kirtiş ve Filiz Karahan tarafından; "Kabaca, internet kullanıcılarının birbirleriyle çevrimiçi etkileşimde bulundukları ve bloglar oluşturup, oluşturulan bu bloglara yorum yapma, içerik paylaşma veya Facebook, MySpace gibi sosyal ağ siteleri aracılığıyla arkadaşlarla iletişim kurma gibi etkinlikleri içeren farklı yolları ifade etmektedir" şeklinde açıklanmıştır (A. Kazım Kirtiş ve Filiz Karahan, 2011, s. 262). İnternete erişimin kolaylaşması ile kullanıcı sayısı astronomik şekilde artan sosyal medya platformlarının 2021 verilerine göre 7.83 milyar olan dünya nüfusunun %53.6'sına tekabül eden 4.2 milyar kullanıcısı bulunmaktadır ve 2020 yılı verilerine kıyasla bir sene içerisinde toplamda 490 milyon yeni kullanıcı kazanmıştır. Yani günümüz itibari ile dünyanın yarısı aktif olarak sosyal medya platformlarını kullanmaktadır (Simon Kemp, 2021).

Sosyal medya platformlarının sahip olduğu böylesine büyük verilerin nasıl korunduğu ise ayrı bir sorunsal olmakla birlikte sosyal medyayı kullanan bireylerin de sadece kedi videoları paylaşmadıkları başlıca gerçeklerden bir tanesidir. Reel dünyanın ve uluslararası sistemin aksine genel anlamda siber uzayın, özelinde ise sosyal medyanın farklı karakteristik özellikleri bulunmaktadır. Bunlardan bir tanesi temel aktörü devletler olan uluslararası sistemin aksine burada birçok aktörün bulunmasıdır. Devletlerin yakın tarihte sosyal medya ile ilgili vermiş oldukları demeçler -hatta bazılarının ulusal tehdit olarak nitelendirmesi (Li Zhou, Nancy Scola ve Ashley Gold, 2017)- ve hukuki alt yapısını oluşturmak için uyguladıkları politikalar bu konu hakkında ne kadar geç kaldıklarını ve realitede olduğunun aksine bu alanda tam olarak hâkim güç olmadıklarını göstermektedir. Bu durumda devletlerin kullanıcılara e-ticaret, e-ihracat, PR çalışmaları, reklamcılık ve eğlence gibi birçok farklı alanda imkanlar sunan sosyal medyayı "ulusal güvenlik tehdidi" olarak nitelendirmesindeki motivasyonu anlamak için sosyal medyanın devletleri ve bireyleri ne gibi tehditler ile karşı karşıya bıraktığını incelemek faydalı olacaktır.

3.1. Kişisel Verilerin Korunması

Sosyal medya platformlarında üyelik oluşturmak için her platformun kullanıcılarından talep ettiği bir dizin veri bulunmaktadır. Bunlar kabaca ad ve soyadı, telefon ve e-mail adresi gibi iletişim bilgileri, cihaz kimliği, satın alma geçmişi ve isteğe bağlı olarak konum bilgisi ile rehber senkronizasyonu gibi verilerdir. Bunların dışında üyelik oluşturulduktan sonra kullanıcıların yapmış olduğu yazılı, görsel veya işitsel paylaşımlar ise kullanıcılar tarafından girilen ekstra verilerdir. Milyarlarca kullanıcının "kendi rızası" ile sosyal medya platformlarının veri tabanına girmiş oldukları bu bilgilerin korunması önemli sorunlardan bir tanesidir. Siber uzayın aşırı derecede kompleks bir yapıya sahip olmasından dolayı devletlerin siber yasalar konusunda yapmış olduğu hukuki girişimlerin birçoğu eksik kalmaktadır. Örneğin Türkiye'de "Kişisel Verilerin Korunması Kanunu"; *Kişisel verilerin işlenmesinde başta özel hayatın gizliliği olmak üzere kişilerin temel hak ve özgürlüklerini korumak ve kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esasları* belirlemeyi amaçlamaktadır (Resmî Gazete, 2016). Her ne kadar kanunlarda amaç, kapsam ve tanımlar yapılarak cezai yaptırımlar belirlenmiş olsa da hem karmaşık bir yapıya sahip olan bu alandaki suçların da kendisi gibi karmaşık olmasından dolayı hem de PwC, CIO ve CSO'nun 2018 yılında hazırlamış olduğu rapora istinaden veri hırsızlığı amacıyla yapılan saldırıların %23'nün kimliğinin tespit edilememesi (PwC, CIO ve CSO, 2018) teoride başarılı gibi gözüken bu politikaları pratikte etkisiz hale getirmektedir. Buna örnek olarak 25 Mart 2021 tarihinde Türkiye'de online yemek siparişi verme platforma olan Yemeksepeti'ne yapılan siber saldırı gösterilebilir. Siber saldırı neticesinde toplamda 21.504.083 kullanıcının ad-soyad, doğum tarihi, platforma kayıtlı adres bilgileri, telefon numaraları ve e-posta adresleri, açık olarak görülmeyen, SHA-256 algoritması ile gizlenmiş giriş şifreleri siber korsanların eline geçmiştir. KVKK'nın bu durum hakkında yaptığı açıklamada platformun "veri güvenliğine ilişkin yükümlülüğe aykırılık" ve "siber güvenlikle ilgili tedbirlerin alınmaması" nedeniyle toplamda 3 milyon Türk Lirası cezaya çarptırılacağını ve platformun saldırıdan etkilenen kullanıcılara şeffaf bir şekilde bilgilendirme yapması gerektiğini belirtmiştir. (Webtekno, 2021). 21.5 milyon kullanıcının verisinin çalınmasına karşılık "en üst sınırdan" verilen 3 milyon Türk Lirası para cezası ve saldırganların kimliklerinin hala tespit edilememiş olması ise siber uzaydaki hukuki zeminin bahsedildiği gibi pratikte yetersiz kaldığını göstermektedir.

Bir başka örnek ise söz konusu durumlarda akla ilk gelen olaylardan bir tanesi olan Cambridge Analytica krizidir. Cambridge Üniversitesi'nde öğretim üyesi olan Aleksandr Kogan, 2014 yılında ABD seçmeni hakkında ayrıntılı profil çıkarmayı hedefleyen bir anket uygulaması geliştirmiştir. Anket uygulaması Facebook üzerinden sadece kullanıcıların verilerine değil aynı zamanda kullanıcıların vasıtasıyla profillerinde ekli olan arkadaşlarının verilerine de ulaşabilecek kapasiteye sahiptir. Bu şekilde toplanan 50 milyon kişilik bir kullanıcı verisi Cambridge Analytica'ya satılıp o dönemden itibaren başkan adaylarının seçim kampanyalarında kullanılmaya başlanmıştır. Veri güvenliği konusunda birçok defa kriz yaşayan Facebook şirketi bu olay sonrasında da sadece özür dilemekle yetinerek, elde edilen verilerin silineceğine dair başvuru yaptıklarını bunun karşılığında taahhüt olarak bir sertifika alacaklarını söylese de böyle bir belge hiçbir zaman paylaşılmamıştır (Burak Budak, 2018).

Sosyal medya platformlarının en önde gelen markalarında bile yaşanan veri güvenliği problemleri, sık sık yaşanan bu durumlar sonrasında adeta siber uzayda yaşanan normal olaylar olarak nitelendirilmeye

başlanmıştır. Bu duruma karşılık veri güvenliği konusunda kullanıcıların sıklıkla kullandıkları argüman ise; "Benim verilerim ile ne yapabilirler ki?" sorusu olmaktadır. Aslında bu soru cevaplanmadan önce başka bir sorunu daha ortaya çıkarmaktadır; oda kullanıcıların veri güvenliğe konusunda yeterli bilince sahip olmadıklarıdır. Siber güvenlik zincirinin en zayıf halkası olan kullanıcıların, sosyal medya özelinde de bu konumlarını koruduklarını rahatlıkla söyleyebiliriz. Her ne kadar sorulan sorunun motivasyonu veri güvenliği açısından pek sağlıklı olmasa da bu güvenlik tehdidinin daha iyi anlaşılması açısından önemli bir noktaya değinmektedir.

Veri hırsızlığı konusunda genel olarak çalınan verilerin saldırıyı yapan hacker gruplar tarafından internette satışa çıkarıldığına dair haberler sıkça karşımıza çıksa da bahsi geçen bu verilerin kullanılabileceği tek alan satışlarının yapılması veya fidyecilik değildir. Herhangi bir şekilde siber saldırı yapmadan da sosyal medya verileri üzerinden ciddi çalışmalar yapılabilmektedir. Çalışmanın önceki sayfalarında paylaşılmış olan sosyal medyanın kullanımının neticesinde sosyal medya platformlarının muazzam derecede veri potansiyeline sahip olduklarını söyleyebiliriz. Bu çerçevede sosyal medyanın kapasitesine bakıldığında geleneksel yöntemler kullanılarak bu verilerin işlenmesi, tasnif ve analiz edilmesi gibi işlemlerin uygulanamayacağı kadar fazla veri olduğu görülmektedir. Bu durumu tanımlamak için kullanılan "Büyük Veri" terimi; hem yüksek düzeyde karmaşıklığa sahip büyük hacimli verileri hem de bu verileri gelişmiş teknik ve teknolojik imkânlar ile anlamlı hâle getirecek analitik metotları tanımlamaktadır (Gov.uk, 2014). Yani anlamsız bir şekilde yığılmış binlerce verinin anlamlı hâle dönüştürülmüş biçimidir. Bu sebeple büyük verinin analize hazır hâle getirilmesi için yapay zekâ raporlama araçları kullanılmaktadır. Bunlardan en önemlisi, algoritmalara kalıpları tanımanın ve insanların bilgi parçalarının içindeki görmediği anlamların öğretildiği bir yapay zekâ çeşidi olan makine öğrenmesidir. Makine öğreniminin önemli uygulamalarından biri olan "Sentiment Analysis" ise hedef/hedeflerin duygu ve duyarlılık analizini yapmaktadır. Algoritmaya duyguların metinsel örnekleri tanımlandıktan sonra bu duyguyu araması istendiğinde veri hacimlerini otomatik olarak sınıflandırabilmektedir. Yapılan bu duygu analizi işlemleri ile sosyal medya kullanıcılarının hangi siyasi partiye nasıl duygular beslediği, ruh hâli, suç potansiyeli gibi özellikleri öğrenilebilmektedir (Sir David Omand vd., 2012, s. 810-811).

Duygu analizi yöntemi birçok konu başlığında kullanılabilmektedir. Siyasi bir olaya karşı verilen tepkileri ölçme amacıyla kullanılabileceği gibi sosyal olaylar ve ticari konularda dahi imkanlar sunmaktadır. Markaları hakkında müşterilerin veya potansiyel müşterilerin ne düşündükleri konusunda bilgi edinebilme amacıyla şirketler yapay zekâ algoritmaları vasıtasıyla bu işlemi yapan özel firmalar ile çalışmaktadır. Buna örnek olarak Mohamed M. Mostafa tarafından 2013 yılında yapılan duygu analizi çalışmasında, tüketicilerin T-mobile, Nokia, DHL, KLM ve IBM markaları hakkında görüşlerini öğrenebilmek için 3516 tweeti önceden tanımlanmış 6800 sözcük kullanarak analiz edilmiştir. Sonuç olarak ise DHL gibi bazı markalara yönelik genel olarak olumlu tüketici duyarlılığı tespit edilirken T-mobile gibi bazı markalarda ise olumsuz sonuçlar elde edilmiştir (Mohamed M. Mostafa, 2013, s. 4241-4251).

3.2. Algı Yönetimi ve Dezonformasyon

Sosyal medyanın ek olarak toplumsal hareketlerin genişlemesi ve yayılmasında da uygun imkânlar sunduğu görülmektedir. Toplumsal hareketlerin en önemli özelliklerinden bir tanesi kolektif bilincin oluşturulmasıdır. İşçi ve milliyetçi hareketlerin ağırlıklı olduğu eski toplumsal hareketler ile daha çok 1970'lerde ortaya çıkan çevre, insan hakları, barış ve feminizm gibi temaların bulunduğu yeni toplumsal hareketler, eylemlerini ve propagandalarını geleneksel yöntemlerle yürüterek kitlelere ulaştırmayı ve söylemelerini dile getirmeyi amaçlamaktaydı. Sosyal medya ise toplumsal hareketlerin oluşturması gereken kolektif bilincin kitlelere yayılması konusunda son derece etkili teknolojik imkânlar sunmaktadır. Bunun en büyük örneği yakın tarihte gerçekleşen Arap Baharı'dır.

Kısaca özetleyecek olursak, Tunus'taki ekonomik sıkıntıların ve işsizlik problemlerinin üstüne yolsuzluk iddialarının çıkması ile başlayan süreçte, üniversite mezunu işsiz bir gencin hayatını devam ettirebilmek için seyyar satıcılık yaptığı el arabasının polisler tarafından el konulması üzerine 18 Aralık 2010 tarihinde kendini yakması ile olaylar başlamıştır. *Facebook*, *Twitter* ve *YouTube* gibi sosyal medya platformlarının Arap Baharı sürecindeki en etkili iletişim araçlarından bir tanesi olması, bilginin

protestocular arasında hızlı dolaşımına katkı sağlamasıyla tansiyonu daha da yükseltmiştir. Komşu ülkelere de sıçrayan Arap Baharı hareketinin neticesinde Tunus, Libya, Mısır, Ürdün gibi ülkelerde yönetim değişiklikleri yaşanmış ve milyonlarca insan hayatını kaybetmiştir. Suriye'de ise günümüzde hâlen devam eden iç savaş başlamıştır (İsmet Göçer ve Sertan Çınar, 2015, s. 54-55).

Yeni medya araçlarının Arap Baharı sürecinde etkisi yadsınamayacak düzeyde olsa da sosyal medya bağlamında pek çok tartışmayı beraberinde getirmiştir. Her ne kadar bu argümanla alakalı bilimsel kanıtlar henüz bulunmasa da bir kesim Arap Baharı gibi hareketlerin sosyal medya üzerinden kasıtlı olarak kışkırtıldığını savunurken, diğer bir kesim toplumsal hareketlerin dijitalleşme öncesi dönemlerdeki varlığına atıfta bulunarak sosyal medyaya biçilen bu büyük rolün abartıldığını savunmaktadır.

Evgeny Morozov, "Facebook ve Twitter Sadece Devrimcilerin Gittiği Yerlerdir" başlıklı yazısında siber-ütopyacıların Arap Baharı hareketlerinin sosyal ağlar tarafından yönlendirildiğini düşünerek gerçek dünya aktivizmini görmezden geldiklerini ifade etmiştir. Yani bu tarz protesto gösterilerinin kamuya mal edilip, organize edilmesi için internet ve sosyal ağların kullanıldığı argümanının geçerli olabilmesi için aktivist ağlar tarafından düzenlenen bu hareketlerin arka planında bir koordinasyon olup olmadığının ortaya çıkarılması gerektiğini savunmaktadır (Evgeny Morozov, 2011). Sosyal medya ağlarının Arap Baharı hareketlerinde protestoculara sunduğu bilgi akışı ve iletişim imkânları yadsınamaz bir gerçektir. Fakat Morozov'un yazısında belirttiği gibi bu tip toplumsal hareketler sosyal ağlar üzerinden kendi kendiliğine oluşmamaktadır. Kolektif bir bilinç oluşturulabildiği doğrudur fakat bu bilincin oluşturulmasındaki planlama ve koordinasyon sanal olmayan yöntemler ile başlamıştır (NyTimes, 2011).

Malcolm Gladwell ise benzer bir şekilde *Facebook* icat edilmeden önce de devrimlerin yapıldığını, 1980'lerde Doğu Almanya'da neredeyse hiç kimsenin cep telefonu yokken Leipzig merkezinde yüz binlerce insanın neredeyse bir yüz yıl daha süreceği düşünülen rejimi devirdiklerini ifade etmiştir. Nihayetinde protestocuların organize olmak için kullandığı iletişim araçlarından çok protesto amaçlarının önemli olduğunu vurgulamıştır (Malcolm Gladwell, 2011).

Kitlelerin sosyal ağlar üzerinden bu şekilde organize edilmesi doğal olarak algı yönetimi konusunu gündeme getirmiştir. ABD Savunma Bakanlığı'nın algı yönetimi için yapmış olduğu tanımlama şu şekildedir: *"Kitlelerin duygu, düşünce, amaç, mantık, istihbarat sistemleri ve liderlerini etkileyerek seçili bilgilerin yayılması ve/veya durdurulması: bunun sonucunda hedef davranış ve düşüncelerinin hedefleyenin istekleri doğrultusunda yönlendirilmesi. Algı yönetimi gerçekler, yansıtma, yanıltma ve psikolojik operasyonların bir bütünüdür* (US Department of Defence, 2021)*."* Bu bağlamda sosyal medyanın sunmuş olduğu imkânlar ile bu tarz eylemlerin maliyetleri düşmüş, bireysel katılımın kolaylaşması ve artması ile yeni toplumsal hareketlerin başarıya ulaşması artmıştır (Tayfun Yücesoy, 2020, s. 12-13). Sosyal medyanın bu tarz algı amaçlı paylaşımlara maruz kalması karşımıza bilgi kirliliği sorununu da çıkmaktadır (Ramesh Pandita, 2014, s. 52-53). Sosyal, kültürel, siyasi veya ekonomik herhangi bir konuyu kendi fikirleri çerçevesinde paylaşan kullanıcılar "kasıtlı veya kasıtsız" bir şekilde bilgiyi dezonformasyona uğratabilmektedir. Buna ek olarak sosyal ağları hızlı bilgi alabilmek için kullanan bireylerin, edinilen bilgiyi ikinci veya üçüncü bir kaynaktan teyit etme motivasyonu bulunmadığı için her geçen gün kullanıcı sayısı artan sosyal ağlara paralel olarak bilgi kirliliği de artış göstermektedir. Ayrıca sosyal medyada paylaşılan içeriklerin *photoshop*, kırpma veya montajlama yöntemleri ile sunulmaları da zaman zaman görülmektedir (Merve Seren vd., 2018, s. 61).

Tabii ki sosyal medyanın sunmuş olduğu bu imkânlar sadece aktivistlerin değil aynı zamanda araştırmacıların ve istihbarat personellerinin de işini kolaylaştırmaktadır. Ben Zimmer bu konu hakkında *Twitter* ve *Facebook* gibi sosyal paylaşım sitelerinin dilbilim, sosyoloji ve psikoloji gibi alanlarda çalışma yapan bilim insanları için de altın değerinde olduğunu, uzun zaman alan zahmetli veri toplama işlemleri yerine araştırmacıların bu verilere sosyal medya platformlarından erişebileceğini belirtmiş ve *Twitteroloji* adı verilen bu çalışmanın küresel ölçekte belli halkların ruh hâlini analiz etmek için kullanıldığını ifade etmiştir (Deborah McMurray, 2011).

3.3. Sosyal Medya İstihbaratı (SOCMINT)

İstihbarat, kökeni insanlık tarihine kadar dayanan bir faaliyet alanıdır. Bu bağlamda analiz ve öngörü istihbarat için son derece önemli unsurlar olmakla birlikte istihbarat sürecinin bunların dışında kalan birtakım aşamaları bulunmaktadır. İstihbarat süreci teorik olarak ihtiyaçların belirlenmesi, veri toplama, tasnif-kıymetlendirme-analiz, dağıtım-kullanım ve geri besleme aşamalarından oluşmaktadır. Bunun yanı sıra pratikte ise bu yol haritasının sıkça dışına çıkılan interdisipliner bir önleyici faaliyettir. Önleyici faaliyet olması sebebiyle istihbarat alanı yaşanmış ve gerçekleşmiş olaylardan ziyade henüz meydana gelmemiş olayları hedef almaktadır. X konumundaki bombanın patlamasını engellemek veya Y konumundaki eylemin gerçekleşmesini önlemek gibi. Bu olaylar engellenemeden gerçekleşirse, her ne kadar suçluların yakalanması için destek amaçlı faaliyetler devam etse de yürütülen istihbarat faaliyetleri başarısız olmuştur ve geriye kalan iş yükü kolluk kuvvetlerine kalmış demektir.
Bu yüzden veri toplama ve bu verilerin analizi istihbarat sürecinde son derece kritik aşamalardır. Veri toplama bağlamında birçok farklı istihbarat disiplini bulunmaktadır (Görsel istihbarat, sinyal istihbarat, akustik istihbarat, siber istihbarat vb.). Fakat henüz tek başına bir disiplin olmak için yetersiz olsa da sosyal medya istihbaratı son dönemlerde literatüre kazandırılmış ve uygulamaları istihbarat servisleri tarafından yapılmaktadır. Açık kaynakların istihbarat sürecinde kullanılması çok da yeni bir yöntem değildir. Arşiv araştırmaları, akademik yazılar, dergi ve gazete taramaları istihbarat servisleri tarafından sıkça başvurulan kaynaklardır. Sosyal medya ise açık kaynak boyutunda yeni bir veri kaynağı olarak karşımıza çıkmaktadır. Doğru bir hukuki zemini oluşturulduğu takdirde SOCMINT'in güvenlik açısından birçok faydası bulunmaktadır.

Bunlardan bir tanesi durumsal farkındalık oluşturmasıdır. Durumsal farkındalık kavramı ilk olarak Alman havacı Oswalde Boelke tarafından düşmandan önce mevcut durumun farkına vararak üstünlük kazanmak amacı ile kullanılmıştır (Faruk Dinç, 2018). Çevresel faktörler ve olayların zaman-mekân ilişkisine göre algılanmasıyla hem mevcut durumu tanımlama hem de gelecek hakkında öngörüde bulunma imkânı tanımaktadır. Yeni medyada haberlerin yayılmasının ve oluşturduğu etkinin geleneksel medyaya göre daha fazla olması sebebiyle sorunun tespit edilmesi, veri akışının çok daha hızlı olduğu sosyal medya üzerinden etkin bir biçimde yapılabilmektedir.

Örneğin; coğrafi konum tekniğiyle paylaşım yapanların yerinin tespit edilmesi, belirli bir konumda olası şiddetle ilgili paylaşımların artması ile bölgeye daha hızlı ve daha etkili bir durum müdahalesi yapma imkânı tanımaktadır (Sir David Omand vd., 2012, s. 806). Yapılan bir çalışmada, sosyal medya paylaşımlarının bir sistem aracılığıyla sorulara tabi tutularak durumsal farkındalık oluşturmanın mümkün olup olmayacağı test edilmiştir. Örneklem olarak Boston maratonun bombalanmasında yaklaşık yarım milyon kadar *tweet* kullanılmış ve sistem elde etmiş olduğu bu *tweet*lere, "Henüz patlamamış başka bombaların nerede olduğu bildiriliyor? Bu mesajlar ne zaman yayıldı? Bu mesajlar ne sıklıkla yayıldı?" gibi sorular sorulmuştur. Sonuç olarak ise, sistem *tweet*lere sormuş olduğu bu sorular ile ana akım medyanın haberi yayınlamasından 11 dakika önce sonuca ulaşmış ve geleneksel medyada bahsedilmeyen St. Ignatius Kilisesi ve Mandarin Oriental Hotel'i gibi insanların olaydan sonra toplandığı lokasyonları da tespit etmiştir (Brian Ulıcny vd., 2013, s. 87-93).

Gruplara katılım imkânı ile pek çok farklı amaç için kullanılan sosyal medya platformlarının temel olarak kitleleri bir araya getiren iletişim aracı olma özelliğinden faydalanılmaktadır. Birbirini tanıyan veya tanımayan milyonlarca insanın fikirlerini paylaştığı bu ortam, benzer ilgi alanları veya hobileri olan kitlelerin gruplar oluşturmasına olanak tanımaktadır. Sosyal medyada yüz yüze iletişimden farklı olarak kullanıcılar profilleri -ki bu anonim olabilir- veya takma isimleriyle iletişim kurabilmelerinden ötürü bu alanda daha cüretkâr olabilmektedirler. Fakat sosyal medyada oluşturulan bu grupların hepsi futbol takımları, arabalar veya popüler kültür ile alakalı içerikler paylaşmamaktadır. Çalışmanın Terör Örgütleri ve Uyuşturucu Kartellerinin Sosyal Medya Kullanımı başlıklı bölümünde birçok organize suç örgütünün, kartellerin ve terör örgütlerinin hem propaganda yapmak hem de yeni üyeler kazanmak gibi amaçlarla sosyal medya platformları kullandığı belirtilmiştir.

Bu gibi durumlar emniyet veya istihbarat personelleri için gruplara katılım sağlayarak gözlem yapabilme ve hedef oluşumlar hakkında bilgi edinme imkânı sunmaktadır. Belirli grupların faaliyetlerini veya davranışlarını daha iyi anlayabilmek için gerekli yasal izinler alındıktan sonra bu grupların içine girerek ne gibi motivasyonlarının olduğunu, olaylara ne gibi tepkiler verdiklerini, söylem ve argümanlarının neler olduğunu ve hatta daha spesifik bir şekilde olası eylem ve gösteri planlarına ilişkin bilgilere SOCMINT yöntemiyle ulaşabilmektedir (Sir David Omand vd., 2012, s. 806).

Son olarak da suçun önlenmesi ve kovuşturulması açısından faydaları bulunmaktadır. Suçun önlenmesi ile ilgili birçok çalışma ve sınıflandırma yapılmıştır. Paul J. Brantingham ve Frederic L. Faust'un yapmış olduğu sınıflandırma üç aşamadan oluşmaktadır. İlk aşamada suç işleme potansiyeli bulunan kişilere müdahale etmek gibi bir durum yoktur. Bu önleyici faaliyette suça zemin hazırlayan koşullar hedef alınmaktadır. İkinci aşama ise suç işleme eğilimi olan kişi veya kişilere erken müdahale öngörülmektedir. Son aşama ise sabıkalı kişilerin tekrar suç işleme ihtimallerini önlemektir. Yani suçun tekrarını önleme amacı bulunmaktadır (Paul J. Brantingham ve Frederic L. Faust, 1976, s. 290).
Kişileri suç işlemeye yönelten fiziksel ve sosyal koşulların sosyal medya üzerinden analiz edilmesi yüksek teknik kabiliyet ve teknolojik imkân isteyen bir süreç olacaktır. İnsanların suçu neden işlediğini anlayabilmek için çok detaylı analizlerin yapılması gerekmektedir. SOCMINT yönteminin buna uygun kabiliyetinin olmasıyla birlikte sürekli olarak izleme yapan yapay zekâ ihtiyacı bulunmaktadır.
Suç işleme eğilimi olan kişiler ve sabıkalıların sosyal medya verilerinden veya gruplara katılımda olduğu gibi bulunduğu gruplardaki söylemlerinden ve etkileşimde bulunduğu kullanıcılardan motivasyonu anlaşılabilir.

Burada dikkat edilmesi gerekilen önemli bir nokta bulunmaktadır. Sosyal medyanın kendisi gibi faydalı yanlarının illüzyonu ile oluşturduğu tehdidi gölgede bırakabilecek SOCMINT faaliyetlerinin ülkeler tarafından uygun bir hukuki zemin ve denetlebilirlik ile güvenlik amaçlı kendi vatandaşları üzerinden uygulaması "özgürlük" mottoları sıkça kullanılan internet aleminde tartışılırken, devletlerin başka ülkeler üzerinde bu tür faaliyetleri uygulaması ise ciddi bir sorun teşkil etmektedir. Sosyal medya üzerinden kasıtlı olarak yanlış bilgilerin yayılıp, spesifik bölgelerde ki kullanıcıların dezenformasyona uğratılmış bu bilgilere karşı ne tepki verdikleri analiz edilerek hiç gerçekleşmemiş bir olay ile dahi kamuoyu tepkisi oluşturabilecek potansiyeli bulunan bu faaliyetin önlenmesi asıl sorunlardan bir tanesidir. Bu bağlamda Rusya, sosyal medya platformlarının alternatiflerini oluşturarak kontrol mekanizmasını güçlendirmeyi hedefleyen bir politika uygulamaktadır. Facebook, YouTube ve Whatsapp gibi dünya çapında kullanılan uygulamaların yerli versiyonlarını üreterek teşvik etmektedir (VK, RuTube, Telegram).

3.4. Sosyal Mühendislik

Siber uzayda gerçekleşen saldırılar akıllara ilk olarak teknik saldırıları getirmekte, daha sağlam altyapılar ve güvenlik duvarları ile bu sorunların vereceği hasarın azaltılabileceği düşünülmektedir. Fakat sosyal ve psikolojik siber saldırılar olan toplum mühendislikleri konusunda bu önlemler yetersiz kalmaktadır. Sosyal mühendislik konusundaki en meşhur vakalardan birisi Kane Gamble olayıdır. 15 yaşında lise öğrencisi olan Kane Gamble, iki arkadaşı ile dönemin CIA Başkanı, Ulusal Güvenlik Danışmanı, eski istihbarat müdürü ve FBI'ın bilim ve teknoloji bölümü başkan yardımcısı dâhil birçok ABD hükûmet yöneticisinin e-posta ve sosyal medya hesaplarını *hack*lemiştir. Fakat Gamble ve arkadaşları bunu teknik yollar ile değil sadece toplum mühendisliği olarak adlandırılan ikna etme ve dolandırma ile başarmışlardır (The Guardian, 2018). Bu şekilde Irak ve Afganistan operasyonlarına dair birçok askerî belge ve istihbarat raporlarını elde edip sonrasında ifşa edilmesini sağlamışlardır. Gamble öncelikle CIA Başkanı John Brennan'ı hedef alır ve telefon numarasını elde eder. John Brennan'ın kullanmış olduğu telefon şirketinin Verizon olduğunu öğrendikten sonra şirket ile alakalı bilgileri toplar ve Verizon firması ile irtibata geçer. Kendisini şirket çalışanı olarak tanıtan Kane Gamble, John Brennan isimli kullanıcının işlemlerini yaparken bilgisayarının arızalandığını bu sebeple John Brennan'ın bilgilerine erişemediği için işlemleri tamamlayamadığını söyler. Verizon firmasının çalışanları arasındaki kullanılan şifreleri doğru cevaplayarak John Brennan'ın gizli sorusunu, ana hesap bilgilerini ve kredi kartının son dört hanesini öğrenir. Telefonu kapattıktan sonra Verizon şirketini tekrar arayarak bu sefer kendisini John Brennan olarak tanıtır ve almış olduğu bilgiler ile güvenlik sorularını doğru

cevaplayarak Brennan'ın e-mail hesaplarına, icloud hesabına ve bağlantılarına erişim sağlar (Judiciary of England and Wales, 2018, s. 2-3).

Bu vakada görüldüğü üzere sosyal mühendislikte teknik imkânlar son derece sınırlı kullanılmaktadır. Üst düzey devlet görevlilerinden bilgi almak için başvurulabilecek bu yola, sıradan kullanıcıları dolandırmak için de başvurulmaktadır. Bu bağlamda sosyal mühendisliği; bir kişiyi kendi çıkarlarına uygun ya da aykırı bir eylemi gerçekleştirme yolunda etkileyen her türlü davranış olarak tanımlayabiliriz. Siber uzay ise bu yöntemin uygulanabilmesi için muazzam bir zemin hazırlamaktadır. İrtibata geçilecek hedef ile yüz yüze görüşmeden farklı bir kimliğe bürünerek eylem gerçekleştirilebilir. Ayrıca sosyal mühendislik için can damarı denilecek "bilginin" elde edilebileceği en uygun ortamlardan bir tanesidir. Elde edilen her yeni bilgi sosyal mühendislik sürecine katkı sağlamaktadır ve sosyal mühendislik eylemi yapacak kişinin veri toplama yöntemi ne olursa olsun temel düşüncesi "hiçbir bilgi gereksiz değildir" olmalıdır (Paul F. Kelly, 2018, s. 47-49). Son yıllarda sıkça kullanılan ve otomatik olarak birçok kullanıcıya gönderilen *spam* e-postaları da birçok hesabın ele geçirilmesinde etkili olmaktadır.

3.5. Siber Zorbalık

Siber zorbalık dolaylı olarak geleneksel zorbalığa benzerlik göstermektedir; birden fazla defa gerçekleşir, kasıtlı olarak yapılır ve psikolojik şiddet içermektedir. Bunun yanı sıra, siber zorbalığında kendine has özellikleri bulunmaktadır. Geleneksel zorbalığın aksine siber zorbalar genellikle anonimdir (Francine Dehue vd., 2008, s. 217). Kabaca, başkalarına zarar vermek veya rahatsız etmek amacıyla kişi veya kişilerin elektronik iletişim kaynaklarından veya dijital ortamda sergilemiş olduğu davranışlardır (Christopher P. Barlett ve Kristina Chamberlin, 2017, s. 446). Her ne kadar siber zorbalık vakalarının genellikle çocuklara yönelik yapıldığı düşünülse de günümüzde bu duruma yetişkinlerde maruz kalmaktadır. Siber zorbalığın yaygınlığı konusunda ise UNICEF toplamda 30 ülkede 13 ila 24 yaş arası 170.000'den fazla katılımcının bulunduğu bir anket yapmıştır ve anketin sonucuna göre her üç gençten birinin siber zorbalığa maruz kaldığı, her beş çocuktan birinin ise bu sebepten ötürü okula gidemediği belirtilmiştir (UNICEF, 2019).

Heidi Vandebosch ve Katrien Van Cleemput tarafından farklı okullarda toplam 279 öğrenci üzerinde siber zorbalık hakkında yapmış oldukları çalışma neticesinde gençlerin siber zorbalığı internet veya cep telefonları aracılığıyla yapılan basit alaylaşmadan ziyade birisinin gerçekten duygularını incitmek amacıyla yapıldığı şeklinde tanımladığı görülmüştür. Öğrencilere başkaları tarafından incitici olarak algılanabilecek şeyleri internet veya cep telefonları vasıtasıyla neden yaptıkları sorusu yöneltildiğinde ise kendilerine (gerçek hayatta veya sanal hayatta) zorbalık yapan, saldıran veya taciz edenlerden intikam almak, canı sıkılan gençlerin teknolojik becerilerini göstermek veya eğlence amaçlı siber zorbalık yapmak gibi güdüleri ortaya çıkmıştır. Öte yandan yapılan anket sonucunda gençlerin neyin siber zorbalık olduğu ve neyin siber zorbalık olmadığı konusundaki algılamalarının belirsiz olduğu görülmüştür (Heidi, Vandebosch ve Katrien Van Cleemput, 2008, s. 501).

Yapılan araştırmalar neticesinde ise siber zorbalığın özellikle gençler üzerinde ciddi derece psikolojik sorunlara (stres, korku, anksiyete, depresyon) yol açtığı görülmüş ve oluşturulan bu olumsuz bu sonuçların geleneksel akran zorbalığı ile benzerlikler gösterildiği tespit edilmiştir (Semra Aksaray, 2011 s. 418-419). Bu çerçevede özellikle gençlerin sosyal yaşamlarını olumsuz yönde etkileyen siber zorbalık konusunda gerek gençlere gerek ise okul yetkilileri ve ailelere farkındalık kazandırılması gerekmektedir. Yapılan çalışmaların yaş aralıkları gençlerin zihinsel ve bedensel gelişimlerinin devam ettiği dönemler olduğu göz önüne alınırsa, dışarıdan basit bir durum gibi gözüken siber zorbalığın oluşturacağı psikolojik travmalar, gençlerin geleceklerine olumsuz bir şekilde yansıma potansiyeli taşımaktadır.

4. SONUÇ

Kullanıcıların bilinçsiz bir şekilde siber uzayı ve ürünlerini kullanması onları tehditlere karşı savunmasız hale getirmektedir. İngiltere Başbakanı Boris Johnson'ın devlet yazışmalarını whatsapp üzerinden yapması üzerine MI5'ın başbakanın telefonuna el koyması sadece sivillerin değil devlet

nezdinde çalışan yetkililerinde bu konu hakkında ne kadar bilinçsiz olduğunu göstermektedir. Devletler açısından hem state centric hem de human centric politikası açısından iki teorinin de genel anlamda siber uzay, özelinde ise sosyal medya ulusal güvenlik tehdidi niteliği taşımaktadır.

Vatandaşlık kavramını devlet ile birey arasındaki zımmi bir sözleşme olarak ele alırsak, bireylerin devletlerin hâkim güç olduğu sınırlar içerisindeki yasalarına ve kurallarına uyması karşılığında devletlerin bireylerin en başta "güvenliğini" ve daha sonrasında temel hak ve özgürlükleri ila sosyal hizmetler konusundaki ihtiyaçlarını karşılaması gerekmektedir. Bu bağlamda güvenlik sadece somut anlamda değil artık siber alanda da sağlanması gereken bir ihtiyaçtır. Bunun yanı sıra bizzat devletin hedef olduğu tehditlerde bulunmaktadır ki bu durum güvenlik boyutunu daha da arttırmaktadır.

Bu durumda uygulanması gereken en önemli faaliyetlerden bir tanesi bilinçlendirmedir. Nasıl ki her vatandaş ilkokul eğitimini alırken toplum kurallarını ve nizamı öğrenebilmek için hayat bilgisi veya sosyal bilgiler gibi dersler alarak toplumun içine girmeye hazırlanıyorsa, aynı şekilde siber alanda da nasıl hareket etmesi ve nelere dikkat edilmesine dair verilecek siber eğitimlerin ilkokul seviyesinden itibaren başlatılması gerekmektedir. Özellikle toplum mühendisliği, siber zorbalık, algı yönetimi, dezenformasyon ve bilgi kirliliği gibi konuların kontrol altına alınabilmesi için bilinçli kullanıcı kitlelerin oluşturulması önem arz etmektedir. Devlet kademelerinde çalışan personeller, bürokratlar, askeri personeller dahil her bir kullanıcının siber uzay ve sosyal medya konusunda bilinçlendirilmesi ise devlet nezdinde yaşanacak potansiyel güvenlik sorunlarını hafifletecektir.

Bunun yanı sıra yerli ve milli yazılımların ve uygulamaların kullanılması olası durumlarda güvenlik amaçlı müdahale edilmesi açısından hareket kabiliyeti kazandıracaktır. İlerleyen süreçte yeni bir fenomen olarak karşımıza çıkması muhtemel olan sosyal medya istihbaratı konusunda ise aynı geleneksel istihbarat modelinde olduğu gibi karşı istihbarat faaliyetlerine ihtiyaç duyulacaktır. Bu bağlamda yapay zekâ algoritmalarının entegrasyonu ve bu çerçevede nitelikli personel yetiştirilmesi büyük önem taşımaktadır. Sonuç olarak yapay zekâ algoritmalarının normal bir insandan çok daha hızlı bir şekilde topladığı ve düzenlediği verilerin nasıl kullanılacağına nihai olarak yetkili merciler karar verecektir. Buna ek olarak yapay zekâ algoritmalarının güvenlik maksatlı sağlıklı bir şekilde uygulamaya geçirilebilmesi için bahsedilen nitelikli personellerin siber uzay ve sosyal medya jargonuna hâkim olması gerekmektedir. Sosyal medya alanında kullanılan dil farklılığı yapay zekaya tanımlanan sınırlı kelimeler dışında kalacak olursa alınan sonuç buna bağlı olarak yetersiz kalacaktır. Hepsinden önemlisi ise siber uzay ve sosyal medya konularında "hukuki altyapı" ve "denetlenebilirliğin" sağlanması gerekmektedir.

KAYNAKÇA

Akyeşilmen, N. (2018), Disiplinlerarası Bir Yaklaşımla Siber Politika & Siber Güvenlik, Ankara: Orion Kitabevi.

Arends, J. Frederick M. (2008) **From Homer to Hobbes and Beyond – Aspects of 'Security' in the European Tradition**, içinde Hans Günter Brauch, Úrsula Oswald Spring, Czeslaw Mesjasz, John Grin, Pál Dunay, Navnita Chadha Behera, Béchir Chourou, Patricia Kameri-Mbote, P. H. Liotta, **Globalization and Environmental Challenges: Reconceptualizing Security in the 21st Century**, Berlin and Heidelberg: Springer-Verlag.

Barlett, C. P. ve Chamberlın, K. (2017), **Examining Cyberbullying Across the Lifespan**. Computers in Human Behavior, (71).

Birdişli, F. (2011), **Ulusal Güvenlik Kavramının Tarihsel ve Düşünsel Temelleri**, Erciyes Üniversitesi Sosyal Bilimler Dergisi, 1 (31).

Bozarth, J. (2010), Social Media for Trainers – Techniques for Enhancing and Extending Learning, San Francisco CA: Pfeiffer.

Brantingham, P. J. ve Faust, F. L. (1976), A Conseptual Model of Crime Prevention, Crime & Delinquency, Vol. 22, No. 3.

Nytimes (2011), A Tunisian-Egyptian Link That Shook Arab History, *https://www.nytimes.com/2011/02/14/world/middleeast/14egypt-tunisia-protests.html?_r=0* (Erişim tarihi: 31 Temmuz 2021).

Britannica, Doctrine of Epicurus, *https://www.britannica.com/topic/Epicureanism/The-Epicurean-school*, (Erişim Tarihi: 15 Temmuz 2021).

Budak, B. (2018), Bilmeniz Gerekenler: Cambridge Analytica Hikayesi, Facebook ve Büyük Veri, Webrazzi, *https://webrazzi.com/2018/03/22/cambridge-analytica-hikayesi-facebook-ve-buyuk-veri/*, (Erişim tarihi: 28 Temmuz 2021).

Dedeoğulu, B. (2014). **Uluslararası Güvenlik ve Strateji**. İstanbul: Yeni Yüzyıl Yayınları.

Dinç, F. (2018), Durumsal Farkındalık, Anka Enstitüsü, *http://ankaenstitusu.com/durumsal-farkindalik/* (Erişim tarihi: 31 Temmuz 2021).

Elmas, M. S., (2013), **Modern Toplumun Güvenlik Çıkmazı: Tehdit, Risk ve Risk Toplumu Perspektifinden Güvenlik**, Ankara, Karınca Yayınları.

Etimoloji Türkçe, *https://www.etimolojiturkce.com/kelime/sigorta*, (Erişim Tarihi: 15 Temmuz 2021).

Gladwell, M. (2011), Does Egypt Need Twitter?, Newyorker, *https://www.newyorker.com/news/news-desk/does-egypt-need-twitter* (Erişim tarihi: 31 Temmuz 2021).

GOV.UK (2014), Emerging Technologies: Big Data, Hm Government Horizon Scanning Programme, *https://www.gov.uk/government/publications/emerging-technologies-big-data* (Erişim tarihi: 29 Temmuz 2021).

Göçer, İ. ve Çınar, S. (2015), Arap Baharı'nın Nedenleri, Uluslararası İlişkiler Boyutu ve Türkiye'nin Dış Ticaret ve Turizm Gelirlerine Etkileri, KAÜ İİBF Dergisi, C. 6, S. 10.

İTÜBİDB (2013), İnternet'in Tarihçesi, *https://bidb.itu.edu.tr/seyir-defteri/blog/2013/09/07/internet%27in-tarih%C3%A7esi*, (Erişim tarihi: 27 Temmuz 2021).

Judıcıary of England and Wales, (2018), The Queen -v- Kane Gamble, Sentencing Remarks of the Hon. Mr Justice Haddon-Cave, *https://www.judiciary.uk/wp-content/uploads/2018/04/r-v-gamble-sentencing.pdf* (Erişim tarihi: 31 Temmuz 2021).

Kartal, B. (2021), BTK ve KVKK, Yemeksepeti'ne En Üst Sınırdan Ceza Kesecek, Webtekno, *https://www.webtekno.com/btk-kvkk-yemeksepeti-en-ust-sinir-ceza-h108622.html*, (Erişim Tarihi: 28 Temmuz 2021)

Kelly, P. F. (2018), Sosyal Mühendisin Maskesini Düşürmek, İstanbul: Paloma Yayınevi.

Kemp, S. (2021), Digital:2021, Wearesocial, *https://wearesocial.com/digital-2021*, (Erişim tarihi: 27 Temmuz 2021).

Kirtiş, A. K. ve Karahan, F. (2011), "To Be or Not To Be in Social Media Arena as the Most Cost-Efficient Marketing Strategy after the Global Recession", Procedia Social and Behavioral Sciences, Vol. 24.

Mcmurray, D. (2011), Have Heard About "Twitterology?" It's the Latest How Now Science, Lexisnexis, *https://www.lexisnexis.com/legalnewsroom/legal-business/b/technology/posts/have-you-heard-about-quot-twitterology-quot-it-s-the-latest-hot-new-science* (Erişim tarihi: 31 Temmuz 2021).

Morozov, E. (2011), Facebook and Twitter are Just Places Revolutionaries Go, The Guardian, *https://www.theguardian.com/commentisfree/2011/mar/07/facebook-twitter-revolutionaries-cyber-utopians* (Erişim tarihi: 31 Temmuz 2021).

Mostafa, M. M. (2013), **More Than Words: Social Networks' Text Mining For Consumer Brand Sentiment,** Expert Systems with Applications, (40).

Omand, S. D., Bartlett, J. ve Miller, C. (2012), **Introducing Social Media Intelligence (SOCMINT),** Intelligence and National Security, 2012, Vol 27, No. 6.

Pandita, R. (2014), Information Pollution, a Mounting Threat: Internet a Major Casuality, J. Of infosci. Theory and Practice, 2014, Vol. 2, No. 4.

PwC, CIO ve CSO, (2018), The Global State of Information Security Survey, *https://www.pwc.com.tr/gsiss2018-en*, (Erişim tarihi 27 Temmuz 2021).

Resmi Gazete, (2016), Kişisel Verilerin Korunması Kanunu, Resmî Gazete Sayısı: 29677, *https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=6698&MevzuatTur=1&MevzuatTertip=5*, (Erişim tarihi: 27 Temmuz 2021).

Seren, M., Çelik, T., Özgeldi, N. ve Dumankaya, E. M. (2018), Sosyal Medya El Kitabı, Ankara: Orion Kitabevi.

The Guardian (2018), Two Years 'Detention for UK Teenager Who 'Cyberterrorised 'US Officials, *https://www.theguardian.com/technology/2018/apr/20/two-years-detention-for-uk-teenager-who-cyberterrorised-us-officials-kane-gamble* (Erişim tarihi: 31 Temmuz 2021).

Ulicny, B., Moskal, J. ve Kokar, M. M. (2013), Situational Awareness from Social Media, STIDS, *https://vistology.com/wp-content/uploads/2016/02/STIDS2013_T12_UlicnyEtAl.pdf* (Erişim tarihi: 30 Temmuz 2021).

UNICEF (2019), **UNICEF Anketi: 30 Ülkedeki Gençlerin Üçte Birinden Fazlası Çevrimiçi Zorbalık Mağduru Olduğunu Belirtiyor**, *https://www.unicef.org/turkey/bas%C4%B1n-b%C3%BCltenleri/unicef-anketi-30-%C3%BClkedeki-gen%C3%A7lerin-%C3%BC%C3%A7te-birinden-fazlas%C4%B1-%C3%A7evrimi%C3%A7i-zorbal%C4%B1k*, (Erişim tarihi: 31 Ağustos 2021).

U.S. DEPARTMENT OF DEFENCE, Perception Management, *https://www.militaryfactory.com/dictionary/military-terms-defined.asp?term_id=4039* (Erişim tarihi: 31 Temmuz 2021).

U.S. Department of State, **National Security Act of 1947 – Milestones: 1945-1952**, *https://history.state.gov/milestones/1945-1952/national-security-act*, (Erişim tarihi: 26 Temmuz 2021).

Vandebosch, H. ve Katrien, V. C. (2008), **Defining Cyberbullying: A Qualitative Research into the Perceptions of Youngsters**, CyberPychology & Behavior, 11 (4).

Yücesoy, T. (2020), Bireyden Kitleye Sosyal Medya Devrimleri ve Ötesine Kuramsal Yaklaşımlar, İstanbul: Duvar Yayınları.

Zhou, L., Nancy, S. ve Gold, A. (2017), Senators to Facebook, Google, Twitter: Wake up to Russian Threat, Politico, *https://www.politico.com/story/2017/11/01/google-facebook-twitter-russia-meddling-244412*, (Erişim Tarihi: 27 Temmuz 2021).