International
e-ISSN:2587-1587
SOCIAL SCIENCES STUDIES JOURNAL
Open Access Refereed E-Journal & Indexed & Publishing
Research Article
Article Arrival : 07/06/2021
Published : 15.08.2021
Doi Number http://dx.doi.org/10.26449/sssj.3365
Reference Mete, M. & Balta Peltekoğlu, F. (2021). "Sosyal Medyada Enformasyon Savaşı: Kurumsal Güvenlik Bağlamında Bireysel Sosyal Medya Kullanımı" International Social Sciences Studies Journal, (e-ISSN:2587-1587) Vol:7, Issue:86; pp:3328-3338

SOSYAL MEDYADA ENFORMASYON SAVAŞI: KURUMSAL GÜVENLİK BAĞLAMINDA BİREYSEL SOSYAL MEDYA KULLANIMI [1]

Information Warfare In Social Media: Individual Social Media Usage In The Context Of Corporate Security

Doktora Öğrencisi. Murat METE
Marmara Üniversitesi, Sosyal Bilimler Enstitüsü, Halkla İlişkiler Bölümü, İstanbul /Türkiye
ORCID ID: https://orcid.org/0000-0001-7228-0935

Prof. Dr. Filiz BALTA PELTEKOĞLU
Marmara Üniversitesi, İletişim Fakültesi, Halkla İlişkiler Bölümü, İstanbul /Türkiye
ORCID ID: https://orcid.org/0000-0001-6667-1737

ÖZET

Enformasyon savaşı, karar vericileri etkilemek için yürütülen iletişim faaliyetleriyle yakından ilgilidir. Enformasyon ortamında gerçekleşen bu etkinliklerin en önemli hedefi insan zihnidir. Gelişen teknoloji sayesinde devletlerin tekelinden çıkan enformasyon gücü ise artık diğer güç unsurlarını da etkileyecek düzeye ulaşmıştır. Bu etkiyi kolaylaştıran güçlü bir araç olarak sosyal medya, sadece hedef kitlenin kararlarını etkilemek için değil, aynı zamanda kullanıcılar tarafından oluşturulan verileri analiz ederek istihbarat elde etmek için de kullanılmaktadır. Araştırmada incelenen ihlal örnekleri, bireysel sosyal medya kullanımının, potansiyel bir risk alanı olduğunu göstermiştir. Söz konusu risk, ulusal düzeyden kişisel düzeye uzanan bir yelpazedeki güvenlik riskleri ile kurumsal itibarı olumsuz etkileyen durumları içermektedir. Etkili kurumsal iletişim politikaları belirlenmesi ve güncel gereksinimlere uygun yasal düzenlemelerin yapılması yanında doğru ve etkili kullanım için personelin bilinçlendirilmesine ve eğitimine önem verilmesi yararlı olacaktır.

Anahtar Kelimeler: Enformasyon savaşı, sosyal medya, kurumsal güvenlik, sosyal medya istihbaratı

ABSTRACT

Information warfare is closely related to communication activities carried out to influence the decision makers. The most important target of these activities in the information environment is the human mind. Thanks to the developing technology, the information power which has freed from the monopoly of the states, has now reached a level that will affect other elements of power. As a powerful tool that facilitates this effect, social media is not only used to influence the target audience's decisions but also to obtain intelligence analyzing the data created by users. The examples of violations examined in the study showed that individual social media use is a potential risk area. It includes security risks ranging from the national level to the personal level and situations that negatively affect corporate reputation. In addition to determining effective corporate communication policies and making legal arrangements in accordance with current requirements, it will be beneficial to give importance to building awareness and training of personnel for correct and effective use.

Keywords: Information warfare, social media, corporate security, social media intelligence

1. GİRİŞ

Enformasyon savaşının, karar vericilerin kararlarını etkilemeye odaklanması, bunu yaparken onların kalplerini ve zihinlerini hedeflemesi, iletişimin çok yönlü olanaklarının kullanılmasını da kaçınılmaz hale getirmektedir. Bundan dolayı *iletişim yönetimi* enformasyon savaşının merkezinde yer almaktadır. İletişim yönetimini daha hızlı, daha etkili ve daha ekonomik hale getiren İnternet ortamındaki sosyal ağlar ise kitle iletişiminin ötesine geçerek herkes için kişiye özel mesajlar üretebilme yeteneği ile iletişim ortamına damgasını vurmuştur. İletişim yönetiminin etkili bir aracı haline gelen sosyal medyanın, özgür ve

[1] Bu makale, Marmara Üniversitesi, Sosyal Bilimler Enstitüsü, Halkla İlişkiler ve Tanıtım Anabilim Dalı'nda Prof. Dr. Filiz Balta Peltekoğlu danışmanlığında devam etmekte olan doktora tezinden türetilmiştir.

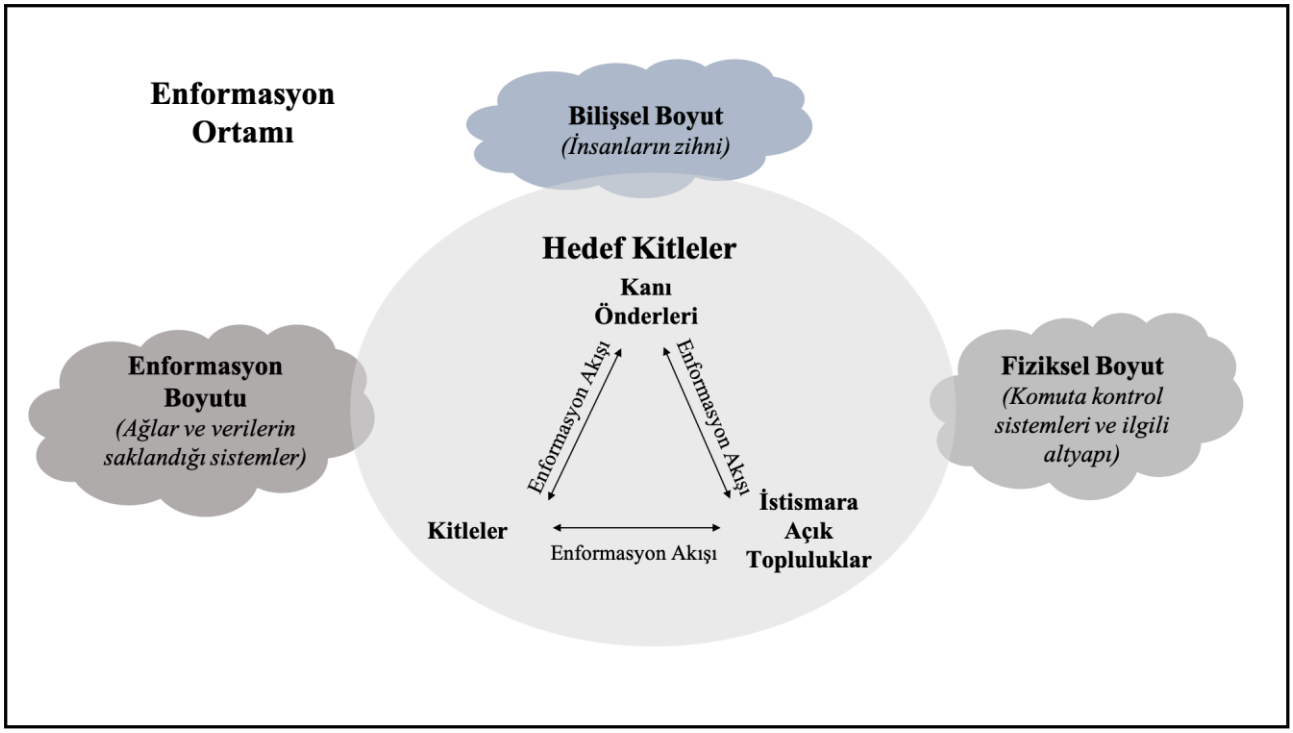
demokratik olduğu *iddia edilen* ortamı, insanların manipüle edildiği, bireysel paylaşımlarda yer alan verilerin, ticari şirketler kadar rakip ülkeler veya terör örgütleri gibi yasa dışı oluşumlar tarafından da kendi amaçlarına yönelik istihbarat elde etmek maksadıyla kullanıldığı bir mecra halini almıştır. Bireylerin, kendi kontrollerinin dışında kullanılabilecek ve istismar edilebilecek bu *verileri* farkında bile olmadan paylaşmalarının tehlikeli sonuçları olabileceği açıktır. Bu çalışmanın amacı, sosyal medyanın enformasyon savaşında kullanımını inceleyerek güvenlik güçlerinin bireysel sosyal medya kullanımından kaynaklanabilecek riskleri ve bu risklere karşı çözüm yollarını belirlemektir.

2. ENFORMASYON SAVAŞI İLE İLGİLİ KAVRAMLAR

Tarih boyunca meydana gelen güç mücadelelerinde rol alan enformasyonun etkili kullanımı prensipleri, enformasyonun edinilmesine, işlenmesine ve yayılmasına dayanmaktaydı. Genel ilkeler aynı kalsa da edinme, işleme ve yayma araçları değişime uğramıştır. Bilgi edinme ve yönetme için kullanılan bilgisayar temelli araçlar daha önceki teknolojilerin, insan kuryelerin ve yazılı iletişimin yerini almıştır. Büyük miktarda enformasyonu yönetebilen elektronik araçlara bağımlılığın ve bu enformasyonun değerinin artması, enformasyonun kendisini kazançlı bir hedef ve değerli bir savaş silahı haline getirmiştir. Bu değişiklikler enformasyonun rolü ve savaşın yürütülmesi konusunda devrim niteliği taşımaktadır (Waltz, 1998, s. 3). Bununla birlikte, özellikle Soğuk Savaş sonrası dönemde öne çıkan enformasyon savaşı kavramı, enformasyonun rakibe karşı üstünlük sağlayacak bir araç olarak kullanılmasının çok ötesinde bir kapsamı ifade etmektedir. Jones vd. (2002), enformasyon savaşının merkezinde, karar vericileri etkileme amacının bulunduğunu ve dergi, radyo, televizyon, gazete, broşür, e-posta, örün sayfaları ve diğer medya çeşitlerinin bu amacı gerçekleştirmek için kullanılacak araçlar olduğunu belirtirler (s. 14).

2.1. Enformasyon Ortamı

Enformasyon hiyerarşisi kapsamında süreklilik kazanan *enformasyon süreci*, enformasyon ortamında gerçekleşmektedir. Enformasyon savaşının gerçekleştiği savaş alanı olması bakımından da enformasyon ortamını anlamak ve tüm yönleriyle tanımak önemlidir. Enformasyon ortamı, bilgi toplayan, işleyen, dağıtan veya bunlara göre hareket eden bireylerin, kuruluşların ve sistemlerin toplamıdır. Bu ortam; bireylerle, kuruluşlarla ve sistemlerle sürekli etkileşim halinde olan, birbirleriyle ve hedef kitleyle ilişkili üç boyuttan oluşur: Fiziksel boyut, enformasyon boyutu ve bilişsel boyut (Şekil 1) (US DOD, 2012, s. I-1).



Şekil 1: Enformasyon Ortamı
Kaynak: US DOD (2012). JP 3-13 Information Operations, Washington D.C., Sf. I-4

Fiziksel boyut, enformasyon teknolojilerinin birbiriyle bağlantısı ve bunu sağlayan araçlardan (ağlar, bilgisayarlar, telefonlar vb.) meydana gelir. *Enformasyon boyutu*, bu bağlantılı sistemler tarafından aktarılan içeriktir (TV yayını, radyo programı, telefon araması vb.). *Bilişsel boyut*, bu içeriğin insanları

nasıl düşüneceklerine, nasıl karar vereceklerine ve ne yapacaklarına yönlendiren etkinin sağlandığı yer olması bakımından *en önemli boyut* olarak görülmektedir (Kuehl, 2007, s. 2). Bilişsel boyut; enformasyon ileten, alan ve bunlara yanıt veren veya bunlara göre hareket edenlerin *zihinlerini* kapsar. Bireylerin veya grupların bilgi işleme, algılama, yargılama ve karar verme süreçlerini ifade eder. Bu unsurlar, bireysel ve kültürel inançlar, normlar, güvenlik açıkları, motivasyonlar, duygular, deneyimler, ahlak, eğitim, zihinsel sağlık, kimlikler ve ideolojileri içeren birçok faktörden etkilenir. Bu faktörleri doğru tanımlamak, karar vericinin zihninin en iyi nasıl etkileneceğini ve istenen etkileri nasıl yaratacağını anlamak açısından önemlidir. Bu itibarla, bu boyut bilgi ortamının *en önemli* bileşenini oluşturmaktadır (US DOD, 2012, s. I-3). Küresel enformasyon ortamı, enformasyon çağı teknolojisinin, algıları şekillendirmek, fikirleri etkilemek ve davranışları kontrol emek amacıyla kullanıldığı bir savaş alanı haline gelmiştir (Kuehl, 2004, s. xvii).

2.2. Bir Güç Unsuru Olarak Enformasyon

Güç denklemine dahil edilen pek çok faktör bulunmasına karşın artık sadece devletler değil, gruplar, kuruluşlar, hatta bireyler tarafından politik sistemi kolayca etkileyecek şekilde kullanılabilen bir faktör olarak *enformasyon*, farklı alanlara farklı yetenekler oluşturacak şekilde aktarılabilme yeteneği sayesinde güç denkleminin en önemli unsuru haline gelmiştir. Teknolojideki hızlı değişim, özellikle telekomünikasyon ve medyanın gelişimi, güç paradigmasının büyük ölçüde değişmesine yol açmıştır (Armistead, 2004, s. 13). Diğer ulusal güç unsurlarının her birini etkileyen enformasyon, iletişim teknolojilerinde meydana gelen gelişmeler sonucu sıradan insanların bile kolaylıkla ulaşabildiği bir unsur halini almış, önemi daha da artmıştır (Jablonsky 2008:154). Neredeyse tüm toplumlarda, enformasyonun kontrolü ve erişimi gücün (iktidarın) araçları haline gelmiş ve enformasyon, değerinin farkında olanlar tarafından satılmış, satın alınmış ve takas edilmiştir (Branscomb, 2009, s. 1). Silahlı kuvvetler, ekonomi, diplomasi gibi geleneksel güç unsurlarının kontrolü devletlerin elinde olmasına karşın enformasyon gücünün kontrolü doğrudan bireylerin elindedir. Enformasyon gücünün bu en belirgin özelliği, devletlerin enformasyon akışını kontrol edemeyeceklerini ancak etkileyebileceklerini gösterir (Armistead, 2010, s. 84).

2.3. Enformasyon Çağında Gücün Evrimi

Enformasyon ve iletişim her zaman önemli olmuşsa da özellikle seksenlerden itibaren yaşanan bazı gelişmeler, bu kavramların tali ya da tamamlayıcı unsurlar olmaktan çıkıp belirleyici ve kapsayıcı bir rol edinmelerine yol açmıştır. Bu gelişmelerden biri teknolojik yenilikler, bir diğeri ise bütün dünyada devlet dışı aktörlerin (Sivil Toplum Kuruluşları (STK), ulus ötesi şirketler, terör örgütleri vb.) devlet kurumları üzerinde etkili olacak güce ve yaygınlığa erişmiş olmalarıdır (Arquilla ve Ronfeldt, 1999, s. 7). Teknoloji ve enformasyonun bileşimiyle ortaya çıkan yeni yetenekler, askerî, diplomatik ve ekonomik unsurlar dahil geleneksel güç unsurlarını derinden etkilemiştir. Gelişmiş hesaplama yöntemleri ve veri ağları ile güçlenen bu yetenekler sadece askerî ve siyasi kurumlar değil ticari şirketler ve sivil şahıslar için de yeni olanaklar sunmaktadır (Armistead, 2004, s. 15). Enformasyon devrimi, ulusal sınırları aşan sanal topluluklar ve ağlar yaratmıştır. Böylece ulus ötesi şirketler, sivil toplum aktörleri ve hatta teröristler daha büyük roller oynayacak duruma gelmişlerdir. Bu örgütlerin birçoğu kendi yumuşak güçlerine sahiptirler. Bilgiyi paylaşma yeteneği ve inanılırlık önemli bir çekim gücü halini almıştır. Küresel bilgi çağındaki bu politik oyun, yumuşak gücün göreceli öneminin artacağını göstermektedir. Bilgi çağında daha çekici ve yumuşak bir güç kazanması muhtemel olan ülkeler, sorunları çözmeye yardımcı olan çoklu iletişim kanallarına sahip ülkelerdir. Bu ülkelerin egemen kültürü ve fikirleri, hâkim küresel normlara daha yakındır ve savundukları değerler ile güttükleri politikalar sayesinde güvenilirlikleri fazladır (Nye, 2004, s. 32). Küreselleşme sayesinde uluslararası düzeyde güç daha yaygınlaşmıştır ve devletler artık onun tek sahibi değildir. Enformasyonun İnternet'te yayılması ve bazılarının yeni bir *uluslararası sivil toplum* olarak adlandırdığı, insanları sınırları aşarak birbirine bağlayan *sanal ağların* çoğalması, devletlerin, fikirlerin yayılmasına hâkim olma ve boyun eğdirme yoluyla kontrolü sürdürme kapasitelerini zayıflatmıştır (Nation 2008, s. 171).

2.4. Enformasyon Savaşı Kavramının Gelişimi

Enformasyon savaşı kavramının ilk kez Boeing Şirketi mühendislerinden Dr. Thomas Rona tarafından hazırlanan "Silah Sistemleri ve Enformasyon Savaşı" başlıklı bir raporda kullanıldığı kabul edilmektedir. Bu raporda, "Rakibin bilgi akışını bozarken, kendimizinkini korumak ve geliştirmek." şeklinde tanımlanan enformasyon savaşı fikrinin önemli uygulamalara yol açtığı ve öngörülebilir sonuçlarının sistematik olarak incelenmesi gerektiğinin altı çizilmiştir (Rona, 1976, s. 5). Soğuk Savaşın ardından 90'lı yıllarda ABD

Savunma Bakanlığı tarafından geliştirilmeye başlanan enformasyon savaşı konsepti, dünyada süregelen toplumsal ve teknolojik gelişmeler sonucu *gücün* devletlerin tekelinden çıkması ve buna bağlı olarak politikaların yeniden düzenlenmesi nedeniyle defalarca değişime uğramış, üzerinde herkesin anlaştığı, net bir tanım yapılamamıştır.

Enformasyon savaşı, ABD Savunma Bakanlığı tarafından "sahip olunan enformasyonu, enformasyona dayalı süreçleri, enformasyon sistemlerini ve bilgisayar tabanlı ağları güçlendirip savunurken, hasma ait bilgileri, bilgi tabanlı süreçleri, bilgi sistemlerini ve bilgisayar tabanlı ağları etkileyerek bilgi üstünlüğü elde etmek için yapılan eylemler" şeklinde (1998a, s. 230); şemsiye bir kavram olarak kullanılan *enformasyon harekâtı* ise daha genelleştirilerek "sahip olunan enformasyonu ve enformasyon sistemlerini korurken hasma ait olanları etkilemek" şeklinde (1998b, s. I-9) tanımlanmaktaydı. Amerikan doktrininde enformasyon savaşı *kriz veya çatışma esnasında gerçekleştirilen enformasyon harekâtı* olarak konumlandırılmıştı (US DOD, 1998b, s. I-11). Gerek *enformasyon savaşı* gerekse *enformasyon harekâtı* ifadeleri, askerî nitelikli bir çağrışım yapmaktadır. Zaman içerisinde, komuta ve kontrol savaşı, kamu diplomasisi, uluslararası kamu bilgilendirme, psikolojik harekât, algı yönetimi, ağ merkezli savaş, ağ savaşı, yumuşak güç, noopolitik, stratejik iletişim gibi terimler aynı amaçla kullanılmış olsa da uluslararası toplumdaki gücün gerçek genişliğini ve derinliğini açıklamak için yetersiz kalmışlardır (Armistead, 2010, s. 93). Enformasyon savaşını tanımlamak için *aktif önlemler, hibrit savaş, gri bölge savaşı, gayri nizami savaş, konvansiyonel olmayan savaş, asimetrik savaş, yumuşak güç, kamu diplomasisi* gibi enformasyonun askerî veya politik uygulamalarına odaklanan terimler kullanılabilmektedir (Theohary, 2018, s. 4). Enformasyon savaşı veya enformasyon harekâtı ile ilgili bu kavram kargaşasının, konuya ilişkin kapsamlı bir teorik altyapının olmamasından, sadece askerî bakımdan ele alınmasından, eğitim standartlarının ve kurumlar arasında sinerji oluşturacak bir koordinasyonun eksikliğinden kaynaklandığı tartışılmaktadır (Armistead, 2010, s. 85). Enformasyon savaşı kapsamında benimsenen alanlar, insanlığın başlangıcından beri insan faaliyetlerinin normal bir parçası olmuştur. Ancak, enformasyon savaşı kavramını benzersiz kılan şey, enformasyon ortamını oluşturan tüm alanları bir araya getiren ilk yaklaşım olmasıdır. Enformasyon ortamı, bir ülkenin, kuruluşun ve kişisel hayatın her yerindedir (Jones vd. 2002, s. 5). Huyge, enformasyon savaşının yalan, propaganda, manipülasyon, istikrarsızlaştırma, kamuoyu önünde suçlama, söylenti çıkarma, hükümet devirme, sanayi casusluğu veya elektronik gözetim, zararlı yazılım, hayati altyapıların sabote edilmesi ve bilgisayarlar üzerinde toplu kontrolün sağlanması, savaş alanının şeffaf hale getirilmesi, düşman üzerinde enformasyon üstünlüğü sağlanması ve psikolojik operasyonların yönetilmesi gibi anlamlarda kullanıldığını ileri sürmüştür (Huyge, 2011, s. 5).

3. SOSYAL MEDYA VE ENFORMASYON SAVAŞINDAKİ ROLÜ

3.1. Ağ Toplumu ve Sosyal Ağlar

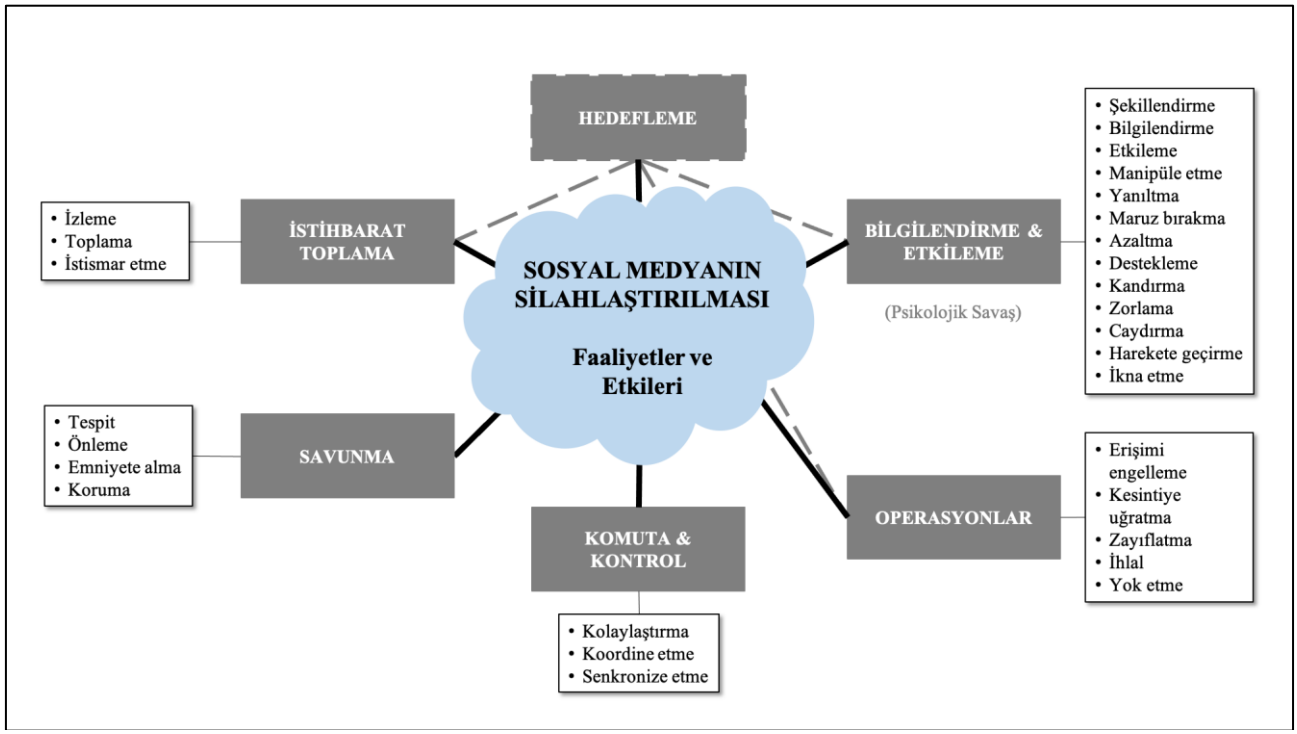
İnsanlık tarihiyle başlayan sosyal ağlara önce ticari ağlar, daha sonra da ulaşım ve üretim ağları eklenmiştir. van Dijk, 20. yüzyıl boyunca enformasyon ve iletişimin gelişmesi ve öneminin artması sonucu bir *ağ toplumundan* bahsetmenin olanaklı hale geldiği tespitinde bulunarak toplumun her seviyesine hizmet etmekte olan ve bu seviyeleri birbirlerine bağlayan ağlara İnternet'i örnek göstermekte, eşzamanlı olarak bireylere, örgütlere, topluluklara ve toplumlara hizmet eden İnternet benzeri bir kitle iletişim aracının tarihte bulunmadığını vurgulamaktadır (2016, s. 75). *Ağ toplumu*, sayısal olarak işlenen enformasyon ve iletişim teknolojilerinin harekete geçirdiği ağlar etrafında örgütlenmiş bir toplumdur. Sayısal ağlar küreseldir çünkü bilgisayar ağları sayesinde ülkesel ve kurumsal sınırları aşarak kendi kendilerini yeniden şekillendirebilirler. Bir sosyal ağ; kanı önderleri, küçük gruplar ve söylentileri kasıtlı olarak ya da istemeden kolaylaştıran kişilerden oluşur (Castells, 2004, s. 3, 2016, s. 59). "Diğer bireylerin tutum ve/veya davranışlarını etkileyebilen kişiler" olan *kanı önderleri* (Mutlu, 2012, s. 178), medyadan alınan bilgileri sosyal ağa yayma veya kamuoyunun medyadan aldığı bilgileri açıklama ya da onaylama görevini üstlenirler (Jowett ve O'Donnell, 2012, s. 395). Sosyal ağ kavramı; bilgiyi, algıyı ve dolayısıyla davranışı etkileyebilecek bir etkileşim yaratan, genel medya kuruluşları veya kullanıcı tarafından oluşturulmuş içeriği toplamak, depolamak, paylaşmak, işlemek, tartışmak ve yaymak için kullanılan İnternet bağlantılı platformlar ve yazılımların bütününü ifade etmektedir (Nissen, 2015, s. 123).

3.2. Enformasyon Ortamında İletişim Yönetimi ve Sosyal Medya

Enformasyon ortamı, enformasyonun kendisini, bu enformasyonu alıp işleyen ve dağıtan bireyler, kuruluşlar ve sistemler ile bunun meydana geldiği bilişsel, sanal ve fiziksel alanı kapsar. Son yıllardaki önemli değişiklikler sonucu dünya çapında dağıtılan bilginin önemi, bilginin iletilme hızı, sosyal medyanın

rolü ve bilgi sistemlerinin güvenilirliği sorunu, enformasyon ortamı üzerindeki potansiyel etkisi dikkate alınmadan hiçbir kararın alınamayacağı veya uygulamaya konulamayacağı bir durum yaratmıştır (NATO Military Committee, 2012, s. 2). Modern savaşlar sadece füzeler ve mermilerin kullanıldığı çarpışmalarla sınırlı değildir. Artık silahlı kuvvetlerin ateş gücünü kullanmak yerine, enformasyon savaşı kapsamında, bir devletin yararına veya ona karşı bir anlatı oluşturmak, yabancı bir ülkede lobi faaliyetleri yürütmek, diğer ülkeleri hedef ülkeye karşı kışkırtmak gibi dijital halkla ilişkiler araçlarını kullanmak olasıdır (Digital PR World, 2020). İnternet ortamında gerçekleşen enformasyon savaşında kullanılan araçlara, *trol fabrikaları* (Sahte sosyal medya profilleri oluşturarak *müşterinin* amacı doğrultusunda yorum/mesaj gönderen kişileri istihdam eden kuruluşlar.); *botlar* (Belli bir anahtar kelimenin ortaya çıkması gibi belirli durumlarda otomatik mesaj gönderen programlar.) ve *sahte haberler* örnek olarak verilmektedir (DEEP, 2020, s. 2). 20 ve 21. yüzyıllarda, sayısız kaynaktan yayılan sürekli bilgi akışını kontrol etme becerisini çok geride bırakan iletişim teknolojilerinin kapsamı ve hızında eşi görülmemiş bir büyümeye tanık olunmuştur. Bu gelişme, bir propagandacının mesajını hızlı ve etkili bir şekilde, zorlanmadan yayma yeteneğini büyük ölçüde geliştirmiştir. İnternet'in büyümesi, Facebook, Twitter ve YouTube gibi yeni sosyal medya araçlarının ve popüler arama motoru Google'ın dünya çapında önemli birer *kontrolsüz enformasyon kaynağı* haline gelmesini olanaklı kılmıştır (Jowett ve O'Donnell, 2012, s. 52).

Sosyal ağların operasyonel amaçlarla kullanımıyla ilgili sınırlamalar ve riskler olsa da sosyal medya platformları ve bunları kolaylaştıran teknolojinin günümüz çatışma ortamının bir parçası haline gelmiş olması "sosyal medyanın silahlaştırılması" olarak nitelenmiş, sosyal medyanın çatışmalarda, devletler veya devlet dışı aktörler, hatta bireyler tarafından, *askerî* nitelikli eylemler için kullanımı, altı ana faaliyet alanını içeren bir modelle açıklanmıştır (Şekil 2) Nissen (2015, ss. 60, 96). Sosyal medyanın silahlaştırılması dendiğinde, sosyal medyanın bir istihbarat ve toplumsal içgörü kaynağı olarak kullanılması ve aynı zamanda aktif bir güvenlik tehdidine dönüştürülmesi anlaşılmaktadır (Dover, 2020, s. 1). Nissen'e (2016) göre, çevrim içi ya da çevrim dışı etkileri olup olmadığına bakılmaksızın bu faaliyetlerin tamamı, sosyal medyada veya onun aracılığıyla yürütülebilir. Sosyal medya hemen hemen tüm etkileme faaliyetlerini gerçekleştirmek veya bunları desteklemek için kullanılabilir. Sosyal mühendislik için aktörlere geniş olanaklar sunan sosyal medyadaki etkileme faaliyetleri, açık ya da kapalı kaynaklar ve ağlar aracılığıyla eş zamanlı olarak gerçekleştirilebilecek, bu sayede tespit edilmesi ve etkisiz hale getirilmesi zorlaşacaktır (Nissen, 2016, s. 7).



Şekil 2: Sosyal Medyanın Silahlaştırılması Faaliyetler ve Etkiler Modeli

Kaynak: Nissen, T. E. (2015). #TheWeaponizationOfSocialMedia: Characteristics of Contemporary Conflicts. Copenhagen: Royal Danish Defence College. s. 61.

3.3. Sosyal Medya İstihbaratı (SOMİS[2])

Sosyal medya platformlarına kaydolurken verdiğimiz bilgiler (Ör. Profil bilgileri içindeki isim, rumuz, fotoğraf, meslek, yaşadığımız şehir vb.); paylaştığımız yazı, görsel veya videolardan oluşan içerikler; başkalarının paylaşımlarına yaptığımız yorumlar ya da işaretlediğimiz beğeni ifadeleri ve daha pek çok küçük detay, İnternetin sonsuz ortamını dolduran büyük verinin daha da büyümesine neden olmaktadır. Kullandığımız ve ürettiğimiz verilerle ilgili genel bir kontrolün olanaklı olamayacağı bir noktaya ulaşılmıştır (Bay ve Biteniece, 2019, s. 10). İstihbarat perspektifinden bakıldığında; gün geçtikçe İnternet'teki sosyal ağa daha fazla bağlı hale gelmemiz gerçek ve sanal kimliklerimizin bütünleşmesine, paylaştığımız bilgiler sayesinde bizimle ilgili eksiksiz analizler yapılmasına ve daha kolay izlenebilmemize yol açmaktadır (Lombardi vd., 2016, s. 2). İstihbarat dünyasında kullanılmakta olan İnsan İstihbaratı (İNİS) [Human Intelligence (HUMINT)], Sinyal İstihbaratı (SİNİS) [Signal Intelligence (SIGINT)], Görüntü İstihbaratı (GÖRİS) [Imagery Intelligence (IMINT)] gibi kategoriler, istihbarat kaynağına göre isimlendirilmektedir. Örneğin İnsan İstihbaratı (İNİS) dendiğinde, kişilerden toplanan veya kişilerin sağladığı enformasyonun analiz edilip değerlendirilmesiyle elde edilen istihbarat anlaşılmaktadır (US DOD, 2013, s. B-4). Bu istihbarat kategorilerine Sosyal Medya İstihbaratı (SOMİS) [Social Media Intelligence (SOCMINT)] kavramını ekleyen Omand vd.ne göre, büyük verinin yapay zekâ ve makine öğrenmesi teknolojileri kullanılarak analiz edilmesiyle anlamlandırılan bu devasa veri kümesinden pek çok alanda yararlanılmaktadır. Sosyal medya analizi olarak bilinen bu yöntemlerin, reklam verenlerin tüketicilerin markalarına karşı tutumlarını anlamasından şirketlerin sosyal medyadaki itibarlarını izlemelerine; insanlar arasındaki ilişkilerin haritalanmasından acil durumlarda toplumun fikirlerinin alınmasına kadar uzanan bir yelpazede kullanılması olasıdır (Omand vd., 2012, s. 804). Eğilim analizi, ağ analizi, duyarlılık analizi, coğrafi analiz, içerik analizi, davranışsal analiz, sistem analizi ve enformasyon analizi yaklaşımları sosyal medyadan istihbarat toplamak için kullanılabilir. Tüm bu analiz biçimleri hedef kitle analizine katkıda bulunarak psikolojik savaşı ve çevrimiçi veya çevrimdışı operasyonlar için hedeflerin seçimini destekleyebilir. Sosyal medya, ağlar, aktörler ve gerçekleşen iletişim hakkında ayrıntılı bilgi almayı olanaklı kılar. Böylece enformasyon ortamı ile hedef kitlenin durumu hakkında bilgi sahibi olunmasına yardımcı olur. Sürekli olarak üzerinde çalışılırsa, sosyal medya, durumsal farkındalık yanında gelecekteki bir krizin erken uyarı sinyallerini belirlemek için yararlı bir kaynak olabilir (Nissen, 2015, ss. 64, 83).

3.4. Sosyal Medya İstihbaratı (SOMİS) Kaynağı Olarak Kullanılabilecek Güvenlik İhlali Örnekleri

Sosyal Medya İstihbaratı (SOMİS), yalnızca yapay zekâ veya makine öğrenmesi yoluyla değil, sosyal medyadaki paylaşımların ilave bir teknoloji kullanılmadan incelenmesi ve bulguların analiz edilmesiyle de elde edilebilir. Aşağıda buna örnek olabilecek bazı vakalar sıralanmıştır:

Bulundukları yerin haritadaki konumunu; kendileriyle birlikte arkadaşlarının, birliğe ait araç, silah, mevzi, nöbet yerleri vb. görüntülerini herkesin kolaylıkla ulaşabileceği şekilde paylaşan askerî personel, İnternet ortamında olağan görülmektedir. Oysa aralıklarla paylaşılan bu konumlar birleştirildiğinde, birliğin intikal güzergahı net olarak ortaya çıkmakta, ulaşacağı konum kolayca tahmin edilebilmekte; birliğin konuşlandığı yer ve tertibatı incelemesi muhtemel teröristler bu bilgileri kullanarak saldırı planlayabilmektedir (Özel Tümer, 2018). Siber Bülten'de yer alan bir habere göre, sosyal ağ özelliklerine sahip Strava isimli bir uygulama; kullanıcılarının yürüyerek, koşarak, bisikletle vb. geçtikleri güzergahı kaydetmekte, merkezî olarak depolamakta ve dünyadaki diğer kullanıcılarla paylaşmaktadır. Bu uygulamanın kullanıcılarının bazıları da askerlerdir. Askerler koşularını muhtemelen üs bölgelerinin veya kışlalarının çevresinde yaptıkları için kat ettikleri güzergahın haritadaki görüntüsü, askerî bölgenin krokisinden başka bir şey olmayacaktır. Farklı ülkelerin ordularına mensup askerlerin farkında olmadan sağladığı bu verilerle birlikte bir milyarı aşan veri Strava firması tarafından *ısı haritası* adı altında herkese açık olarak yayınlanmaktadır. Avusturalyalı bir üniversite öğrencisi, bu ısı haritalarının bazılarının ABD ordusunun Afganistan'daki üsleri ile Türk Silahlı Kuvvetlerine (TSK) bağlı unsurların Suriye'deki muhtemel yerlerini gösterdiğini tespit ederek Twitter'da yayınlamıştır. Diğer araştırmacılar da Nijer'deki bir Fransız askerî üssünü, Cibuti'deki bir İtalyan üssünü, hatta Amerikan Merkezî Haber Alma Teşkilatı (CIA) üsleri olduğundan şüphelendikleri bazı yerleri açıklamışlardır (2018).

Rusya'da olduğu kadar Doğu Avrupa ve Orta Asya'da da popüler olan Rus menşeli, Vkontakte ve

[2] Türkçe "SOMİS" kısaltması, "Sosyal Medya İstihbaratı" kavramı için tarafımızdan önerilmektedir (y.n.).

Odnoklassniki isimli sosyal ağ sitelerinde yer alan Rus askerlerinin fotoğraf ve özçekim paylaşımlarının analizi ile ulaşılan sonuçlar, SOMİS bakımından dikkate değer örnekler oluşturmaktadır. 2014 yılında Rusya'nın Ukrayna'ya ait olan Kırım'ı ilhak etmesiyle başlayan gerginlik, Rus yanlısı silahlı muhaliflerle Ukrayna devlet güçleri arasında başlayan çatışmalara dönüşmüştü. Rus ordusuna bağlı askerlerin, muhaliflerin yoğun olduğu Ukrayna'nın doğusunu işgal ettikleri ve muhaliflere silahlı destek verdikleri iddiaları Rusya tarafından reddedilmişti (Peter, 2014). Ancak, Rus askerlerin sosyal medyadaki fotoğraf paylaşımları, resmî açıklamaların aksini ispatlamıştır. 2015 yılında, VICE News için hazırlanan, "Selfie Soldiers: Russia Checks in to Ukraine" isimli belgesel, Bato Dambaev isimli bir askerin paylaştığı fotoğrafların ve özçekimlerin izini takip ederek, Rus birliklerinin Ukrayna-Rusya sınırında konuşlandığını ve Ukrayna'ya girip burada faaliyette bulunduklarını göstermiştir (Ostrovsky, 2015). Ukraynalı bir askerî yetkili ise verdiği demeçte "Askerlerin sosyal medya paylaşımlarından tespit edilen yerlerin Ruslar tarafından ateş altına alındığı durumlarla karşılaştıklarını, iki tarafın da aynı hataları yaptığını, konum hizmetlerinin kapatılması ve konumu belli edecek görüntülerin paylaşılmaması şartıyla sosyal medya sitelerinin kullanılması gerektiğini" ifade etmektedir (Zhuk, 2015). BBC News'de (2017) belirtildiğine göre, çok sayıda İsrailli askere sosyal medya aracığıyla, kadın kimliğinde ulaşıp telefonlarının kamera ve mikrofonlarını kontrol eden bir sohbet uygulaması indirmeye ikna eden ve İsrail Ordusu'nun hareketlerini izlemeye çalışan siber saldırganların Hamas üyesi oldukları tespit edilmiştir. McKirdy ve Pokharel (2019) ise Facebook'tan kendisi gibi Hindistan Ordusu'nda görevli bir sağlık subayıyla bağlantı kurduğuna inanan bir askerin bir yıl boyunca birlik ve tank hareketleri dahil pek çok gizli bilgiyi paylaştığı hesabın Pakistan kaynaklı olduğunun anlaşıldığını, benzer olayların sıkça yaşandığını bildirmişlerdir.

3.5. Güvenlik Güçlerinin Bireysel Sosyal Medya Kullanımına Yönelik Düzenleme Örnekleri

2016-2019 Ulusal Siber Güvenlik Stratejisi Dokümanında "kurum yöneticilerinden bilgisayar kullanıcısı vatandaşa kadar toplumun tüm kesimlerine siber güvenlik kültürünün kazandırılmasına yönelik eylemlerin gerçekleştirilmesi" hedeflenmiştir (T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı, t.y., s. 15). Güçlü ağ güvenliği olmazsa olmaz koşulsa da tek başına teknoloji, sosyal medyadaki siber güvenlik risklerine karşı koruma sağlayamaz. İnsan hatası ve çalışanların işyerinde sosyal ağları kullanmasına yönelik resmî bir yaklaşım geliştirilmesi gerekir. Siber suçlular, bir kurumun gizli bilgilerini elde etmek için çalışanları sosyal medyada manipüle etmekte ustadır. Bu tür siber saldırılar, işle ilgili bilgileri riske atan basit hatalar nedeniyle başarılı olurlar. Sızdırılan parolalar, marka kimliğine bürünme ve diğer kimlik avı dolandırıcılıkları, tüm sosyal siber risk olaylarının neredeyse %95'ini oluşturur (Walker, 2019). Sosyal medya kullanıcılarının geniş yaş aralığı ve teknoloji deneyimi düzeyindeki farklılık, güvenlik yönetimini daha da karmaşık hale getirmektedir. Bir sosyal platformun yalnızca bilgisayar korsanlarıyla savaşması değil, aynı zamanda kişisel güvenlik uygulamaları bilgisi yetersiz olan kullanıcıları da koruması gerekir (Sobers, 2020). 15 Mart 2019 tarihinde Yeni Zelanda'da gerçekleşen terör saldırısı İnternetin ve özellikle sosyal medyanın bireylerin radikalleşmesinde önemli bir rol oynadığını göstermiştir. Radikalleşme sürecinin tespitinin oldukça zor olduğu, ülkelerin bu kontrolü sağlamak için siber tedbirlerini artırdığı ve özellikle sosyal medyanın takibi ile sosyal medya istihbaratının önem kazandığı vurgulanmakta, çok büyük miktarda veri içeren sosyal medyanın bu bakımdan kontrolü için disiplinler arası bir anlayışla oluşturulacak uzman bir teşkilat kurulması önerilmektedir (Bural, 2019).

Bu sorun, diğer ülkeler tarafından da yakından incelenmekte ve çözümler geliştirilmeye çalışılmaktadır. Bununla birlikte, batı ülkeleri orduları, sosyal medyanın belirlenen politika ve yönergelere uyulması şartıyla, bireysel olarak da etkin şekilde kullanılmasını özendirmekte, bu sayede kurum imajına olumlu katkı sağlanacağı ve kurumun hedef kitleleriyle daha sağlıklı bir iletişim sürdürüleceği düşünülmektedir. ABD Savunma Bakanlığı, 2009 yılında, güvenlik ihlallerine sebebiyet verdiği gerekçesiyle askerî personelin sosyal medya kullanmasını yasaklamış ancak 2010 yılında yaptığı bir çalışma sonucu, muhtemel zararlarından daha fazla yarar getireceğini değerlendirerek sosyal medya kullanımını serbest bırakmıştır. Böylece askerî personelin, yasal düzenlemelerde belirtilen kuralları ihlal etmediği müddetçe sosyal medyada paylaşım yapabilmesine olanak tanınmıştır ki bu kurallar genel olarak kurumsal bir şirketin kendi personeli için belirlediği kurallara benzemektedir (Matthews-Juarez vd., 2013, s. 769). ABD Kara Kuvvetleri Komutanlığı'nın yayınladığı Sosyal Medya Elkitabında genel olarak kurumsal sosyal medya yönetimine ilişkin esaslar belirlenmekle birlikte askerlerin, ordunun en iyi ve en etkili habercileri olduğu, sosyal medya sayesinde hem kendi hikayelerini özgün ve samimi bir şekilde anlatabileceklerini hem de kurumun hikayesinin anlatılmasına katkı sağlayacaklarını vurgulayarak Kara Kuvvetlerinin sosyal medyayı sadece kendi hikayesini anlatmak için değil aynı zamanda *dinlemek* için de kullandığı ifade edilmektedir.

Elkitabında sosyal medya kullanırken dikkat edilmesi gereken hususlar; kişisel imajın kurumsal imajı yansıttığının unutulmaması; güvenlik açığı yaratacak konuların ve gizli bilgilerin paylaşılmaması; kurumsal değerlerin gözetilmesi; telifli veya ticari markalı materyal paylaşılmaması; sahte kimlik kullanılmaması; kişisel bilgilerin (kimlik ve iletişim bilgileri vb.) paylaşılmaması ve konum hizmetleri gibi elektronik fonksiyonların kapalı tutulması; bir tehdit algılandığında yetkili makamlara bildirilmesi şeklinde sıralanmıştır (US Army, 2016).

İngiliz Ordusu tarafından ilk olarak 2018 yılında yayınlanan ve 2020 yılında güncelleştirilen "#DIGITALARMY Using Social Media in The British Army" isimli dokümanda, ordu personelinin ve ailelerinin sosyal medya kullanırken kurumun değerlerini ve yüksek standartlarını yansıttığı ve ordunun vermek istediği mesajı doğru şekilde iletmelerinin önemi vurgulanmaktadır. Üniformalı ve askerî bölge olduğu belli olan yerlerde çekilmiş fotoğraf paylaşımına dikkat edilmesi; suçlular, teröristler veya potansiyel düşmanlar tarafından istismar edilebilecek nitelikte olan, işle ilgili ayrıntıların paylaşılmaması; yalnızca arkadaşlar tarafından görülebildiği düşünülen kısıtlı profillerin bile üçüncü şahıslarca kolaylıkla görülebileceğinin göz önünde bulundurulması; konum hizmetlerinin kapatılması; özellikle ölü ve yaralıların olduğu büyük olaylar esnasında sosyal medyada paylaşım yapılmaması ve bir siber güvenlik tehdidi durumunda belirlenen makama haber verilmesi vb. hususlar da dokümanda yer almaktadır (Biritish Army, 2020).

NATO sosyal medya politikasını içeren direktifte halkla ilişkiler birimleri için sosyal medyanın askerî amaçlarla kullanımına yönelik prensipler açıklanmış ayrıca kişisel sosyal medya kullanımı kapsamında kişisel veriler ve hesaba ait ayrıntılar ile birliğin konumu, personel sayısı, rütbeler gibi bilgilerin paylaşılmaması gerektiği belirtilmiştir. Ayrıca, fotoğrafların önemli bilgileri verebileceği, bu nedenle paylaşılan fotoğraflarda kimlik kartlarının, bilgisayar ekranlarının, kâğıt belgelerin ve hassas askerî malzemelerin veya ekipmanların görünmemesi gerektiği vurgulanmıştır (NATO, 2014).

2016 yılında Çin'de, bir askerin cep telefonundaki bir uygulamayı kullanarak görev yaptığı kışlaya taksi çağırması sonucu fark edilen olayda, kışlanın coğrafi konumunun tam olarak paylaşılmasının güvenlik riski oluşturabileceği anlaşılmış, Çin Halk Kurtuluş Ordusu tarafından bu tür uygulamaların kullanılması yasaklanmıştır (Middleton, 2016). Sosyal medya kullanımının ulusal güvenlik sorunlarına yol açması üzerine askerlerin görevdeyken akıllı telefon kullanmalarını yasaklayan bir tasarı üzerinde çalışan Rusya Parlamentosu, askerî personelin fotoğraf çekme, video kaydetme ve internete erişim özelliğine sahip telefonlara ek olarak tabletler ve dizüstü bilgisayarların kullanımını da durdurmayı planlamaktadır. Askerlerin temel arama ve mesajlaşma olanaklarına sahip telefonları kullanmaya devam edebilecekleri bildirilmiştir (BBC News, 2019). 2019 Aralık ayında, Hindistan Donanması, sosyal medya platformlarında hassas bilgileri sızdıran yedi askerin casusluk suçlamasıyla tutuklanmasından sonra personelin tesislerde ve gemilerde akıllı telefon ve sosyal medya kullanmasını yasaklamıştır (Press Trust of India, 2019). Yine 2019 yılında gerçekleştirilen bir NATO Tatbikatında, askerleri ve çeşitli birlikleri hedef alan sosyal medya saldırıları simüle edilmiş (canlandırılmış), kötü niyetli saldırganların sosyal medya aracılığıyla önemli miktarda bilgi toplayabilecekleri ve askerlerin davranışlarını kolayca etkileyebilecekleri sonucuna varılmıştır. Uzmanlar, bu sorunun, askerlerin akıllı telefon kullanmasını engelleyerek çözülemeyeceği konusunda hemfikirdirler. Bir harekât esnasında telefonların kullandırılmayabileceğini ama bunun sürekli hale getirilemeyeceğini düşünen yetkililere göre, askerleri, kendilerini sosyal medyadayken nasıl koruyacakları ve bu konuda ailelerini nasıl eğitecekleri konusunda sürekli eğitmek, önemli bir çözüm olarak öne çıkmaktadır (NATO STRATCOM COE, 2019). Türk Silahlı Kuvvetleri (TSK) ise kışlalarda tamamen yasak olan cep telefonu kullanımını 2015 yılında düzenleyerek erbaş ve erlerin askerlik hizmeti süresince kışlada, İnternete bağlanma, ses ve görüntü alma özelliği olmayan cep telefonlarını belirli saatlerde kullanmasına olanak tanımıştır (Sözcü, 2015). Subay, astsubay, uzman erbaş ve sivil memurların cep telefonlarını kışla ve karargâh girişlerindeki görevli personele teslim etmeleri ve mesai saatleri içinde kullanmamaları gerekmektedir (Bkz. TSK Disiplin Kanunu Md.19.1.j).

Enformasyon savaşında sosyal medyanın kullanımına ilişkin bilgiler, ihlal örnekleri ve mevcut düzenlemeler dikkate alındığında, sosyal medya ve güvenlik ilişkisi daha belirgin hale gelmektedir. Bu bakımdan sosyal medya kullanımının, kurumsal iletişim politikasıyla uyumlu şekilde düzenlenmesi ve personelin bu konudaki bilinç düzeyinin artırılması kritik bir konu olarak öne çıkmaktadır.

4. SONUÇ

Enformasyon savaşı, sadece silahlı kuvvetleri ya da İnternet ortamındaki siber saldırıları kapsamaz. Devlet veya devlet dışı kurumların, özel şirketlerin hatta yasa dışı örgütlerin ve bireylerin bir parçası olduğu enformasyon ortamında, kontrol sağlamaya yönelik faaliyetler bütünü olan enformasyon savaşı, bir askerî harekâtta hasım komutanın karar verme yeteneğini etkileyerek hasmın etkisiz hale getirilmesini amaçlarken iş dünyasında, şirketin rakiplerinin önüne geçip pazar payını ve kârını yükseltmesini amaçlar. Enformasyon ortamının güvenlik risklerine duyarlılığı en yüksek olan boyutu, tüm teknolojik araçlar ve ağlardan oluşan fiziksel boyut gibi görünse de aslında kullanıcıların zihinlerinin etkilenerek duygu ve düşüncelerinin yönlendirildiği, nasıl düşünüp karar alacaklarının belirlendiği bilişsel boyutun risklere duyarlılığı daha yüksektir. Enformasyon ortamının bir diğer bileşeni olan enformasyonun İnternet teknolojileri sayesinde hızla ve son derece ekonomik şekilde yayılması ile oluşan sosyal ağlar da enformasyonun güç denklemindeki yerini sağlamlaştırmasına katkıda bulunmaktadır. Bilişsel boyutu oluşturan kullanıcıların zihinlerini etkileyecek güçlü bir araç olarak sosyal medya, enformasyon savaşında istihbarat elde etmek ve hedef kitleyi etkileyerek istenilen istikamette karar almasını sağlamak amacıyla kullanılmaktadır. Güvenlik güçlerine mensup personelin bireysel sosyal medya kullanımı, paylaşımların niteliğine dikkat edilmemesi veya kullanılan cihazların bazı teknolojik özelliklerinin bilinmemesi nedeniyle riskli durumlar yaratabilmektedir. Bu riskli durumlar, ulusal düzeyden kişisel düzeye uzanan bir yelpazedeki güvenlik riskleri ile kurumsal itibarı riske atan durumlar olabilmektedir. Etkili kurumsal iletişim politikaları belirlenmesi ve güncel gereksinimlere uygun yasal düzenlemelerin yapılması önemli bir husus olarak görülmektedir. Bununla birlikte, tam olarak kontrol edilmesi olasılık dahilinde olmayan sosyal medyanın risk yaratmayacak, hatta kurumsal yararlar sağlayacak şekilde doğru ve etkili kullanımı için personelin bilinçlendirilmesine ve eğitimine önem verilmesi yararlı olacaktır.

KAYNAKÇA

Armistead, L. (Ed.). (2004). *Information Operations: Warfare and the Hard Reality of Soft Power*. Brassey's issues in twenty-first century warfare (1st ed.). Washington, D.C: Brassey's.

Armistead, L. (Ed.). (2007). *Information Warfare: Separating Hype from Reality*. Issues in twenty-first century warfare (1st ed.). Washington, D.C: Potomac Books.

Armistead, L. (2010). *Information Operations Matters: Best Practices* (1st ed.). Washington, D.C: Potomac Books.

Arquilla, J. ve Ronfeldt, D. (1999). *The Emergence of Noopolitik*. Santa Monica, CA: RAND.

Bartholomees, J. B. (2008). *U.S. Army War College Guide to National Security Issues*. Carlisle, Pa.: Strategic Studies Institute, U.S. Army War College. http://purl.access.gpo.gov/GPO/LPS95737 adresinden erişildi.

Bay, S. ve Biteniece, N. (2019). *The Current Digital Arena and its Risks to Serving Military Personnel*. Responding to Cognitive Security Challenges (ss. 6-16). Riga: NATO Strategic Communications Centre of Excellence. https://www.stratcomcoe.org/current-digital-arena-and-its-risks-serving-military-personnel adresinden erişildi.

BBC News. (2017, 12 Ocak). Israeli Soldiers "Caught in Hamas Online Honey Trap". *BBC News*. 2 Şubat 2021 tarihinde https://www.bbc.com/news/world-middle-east-38594669 adresinden erişildi.

BBC News. (2019, 20 Şubat). Russia Bans Smartphones for Soldiers over Social Media Fears. *BBC News*. https://www.bbc.com/news/world-europe-47302938 adresinden erişildi.

Biritish Army. (2020). #DIGITALARMY Using Social Media in the Biritish Army. Biritish Army. https://indd.adobe.com/view/52dd0428-cf20-4314-8ba0-43ff72b8b464 adresinden erişildi.

Branscomb, A. W. (2009). *Who Owns Information?: From Privacy to Public Access*. New York: Basic Books.

Bural, E. B. (2019, 22 Mart). Radikalleşmeden Terörizme: Bir Teröristin Anatomisi. *21. Yüzyıl Türkiye Enstitüsü*. 27 Ocak 2021 tarihinde https://21yyte.org/tr/merkezler/islevsel-arastirma-merkezleri/terorizm-ve-terorizmle-mucadele/radikallesmeden-terorizme-bir-teroristin-anatomisi adresinden erişildi.

Castells, M. (Ed.). (2004). *The Network Society: A Cross-Cultural Perspective*. Cheltenham, UK ;

Northampton, MA: Edward Elgar Pub.

Castells, M. (2016). *İletişim Gücü*. (E. Kılıç, Çev.) (1. bs.). İstanbul: Bilgi Üniversitesi Yayınları.

DEEP. (2020). Media-(Dis)information-Security. NATO Defence Education Ehancement Programme. https://deepportal.hq.nato.int/goto.php?target=file_1873_download&client_id=DEEP adresinden erişildi.

Digital PR World. (2020, 11 Haziran). 5th Generation Information Warfare and How the Brands are bracing against it? *Online PR Agency India*. https://digitalprworld.com/. https://digitalprworld.com/5th-generation-information-warfare-brands-bracing/ adresinden erişildi.

Dover, R. (2020). SOCMINT: A Shifting Balance of Opportunity. *Intelligence and National Security*, *35*(2), 216-232. doi:10.1080/02684527.2019.1694132

Jones, A., Kovacich, G. L. ve Luzwick, P. G. (2002). *Global Information Warfare*. Boca Raton, Fla: Auerbach Publications.

Jowett, G. ve O'Donnell, V. (2012). *Propaganda & Persuasion* (5th ed.). Thousand Oaks, Calif: SAGE.

Lombardi, M., Rosenblum, T. ve Burato, A. (2016). From SOCMINT to Digital HUMINT. De Gasperi Foundation.

Matthews-Juarez, P., Juarez, P. D. ve Faulkner, R. T. (2013). Social Media and Military Families: A Perspective. *Journal of Human Behavior in the Social Environment*, *23*(6), 769-776. doi:10.1080/10911359.2013.795073

McKirdy, E. ve Pokharel, S. (2019, 15 Ocak). Indian Soldiers Being "Honey Trapped" by Fake Social Media Accounts from Pakistan. *CNN*. 2 Şubat 2021 tarihinde https://www.cnn.com/2019/01/15/asia/indian-soldiers-honey-trap-intl/index.html adresinden erişildi.

Middleton, R. (2016, 16 Şubat). China Warns Soldiers Against Using Taxi Apps from Mobile Phones for Security Reasons. *International Business Times UK*. https://www.ibtimes.co.uk/china-warns-soldiers-against-using-taxi-apps-mobile-phones-security-reasons-1544026 adresinden erişildi.

NATO Allied Command Operations. (2014, 16 Eylül). ACO Directive on Social Media. NATO Supreme HQ Allied Powers Europe. https://shape.nato.int/resources/3/website/AD_095-003_Social_Media.pdf adresinden erişildi.

NATO Military Committee. (2012). NATO Military Policy on Information Operations. NATO.

NATO STRATCOM COE. (2019). *Soldiers on Social Media—Good or Bad?* https://www.youtube.com/watch?v=5YA-LrCa844&feature=youtu.be adresinden erişildi.

Nissen, T. E. (2015). *#TheWeaponizationOfSocialMedia- @Characteristics_of_Contemporary_Conflicts*. Copenhagen: Royal Danish Defence College. forsvaret.dk/FAK/eng/publications/Documents/The%20Weaponization%20of%20Social%20Media.pdf adresinden erişildi.

Nissen, T. E. (2016). Social Media's Role in "Hybrid Strategies". NATO STRATCOM COE. https://www.stratcomcoe.org/social-medias-role-hybrid-strategies-author-thomas-elkjer-nissen adresinden erişildi.

Nye, J. S. (2004). *Soft Power: The Means to Success in World Politics* (1st ed.). New York: Public Affairs.

Omand, D., Bartlett, J. ve Miller, C. (2012). Introducing Social Media Intelligence (SOCMINT). *Intelligence and National Security*, *27*(6), 801-823. doi:10.1080/02684527.2012.716965

Ostrovsky, S. (2015). *Selfie Soldiers: Russia Checks in to Ukraine*. VICE News. https://www.youtube.com/watch?v=2zssIFN2mso&has_verified=1&bpctr=1612043945 adresinden erişildi.

Özel Tümer, D. (2018). 'Askerin Fotoğraf Paylaşımı Riskli'. *Milliyet*. Haber. 29 Ocak 2019 tarihinde http://www.milliyet.com.tr/askerin-fotograf-paylasimi-riskli--gundem-2607239/ adresinden erişildi.

Peter, L. (2014, 1 Eylül). Beş Soruda: Ukrayna Krizi. *BBC News Türkçe*. 31 Ocak 2021 tarihinde https://www.bbc.com/turkce/haberler/2014/09/140901_bes_sorudaukrayna adresinden erişildi.

Press Trust of India. (2019, 31 Aralık). After Spying Sase, Navy Bans Smartphones, Social Media on Bases, Ships. *Business Standard India*. 3 Şubat 2021 tarihinde https://www.business-

standard.com/article/pti-stories/navy-bars-personnel-from-using-smartphones-social-media-at-its-installations-119123001264_1.html adresinden erişildi.

Rona, T. P. (1976). Weapon Systems and Information War. Boeing Aerospace Company.

Siber Bülten. (2018, 5 Şubat). Suriye'deki Türk Askeri Üslerin Konumları Strava ile Açığa Çıktı. *Siber Bülten*. Blog. https://siberbulten.com/sektorel/suriyedeki-turk-askeri-uslerin-konumlari-strava-ile-aciga-cikti/ adresinden erişildi.

Sobers, R. (2020, 29 Mart). Social Media Security: How Safe is Your Information? *Inside Out Security*. https://www.varonis.com/blog/social-media-security/ adresinden erişildi.

Sözcü. (2015, 14 Nisan). Askerde Cep Telefonu Müjdesi! *Sözcü*. 26 Mayıs 2021 tarihinde https://www.sozcu.com.tr/2015/gundem/askerde-cep-telefonu-mujdesi-803341/ adresinden erişildi.

T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı. (t.y.). 2016-2019 Ulusal Siber Güvenlik Stratejisi. T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı.

Theohary, C. A. (2018). *Information Warfare: Issues for Congress* (No: R45142) Congressional Research Service. www.crs.gov adresinden erişildi.

US DOD. (1998a). *Department of Defense Dictionary of Military and Associated Terms*. Washington, DC: US DOD.

US DOD. (1998b). *Information Operations*. Washington, DC: US DOD. http://www.bits.de/NRANEU/others/jp-doctrine/jp3_13%2898%29.pdf adresinden erişildi.

US DOD. (2012). *Information Operations*. Washington, DC: US DOD.

US DOD. (2013). *Joint Itelligence*. Washington, DC: US DOD.

U.S.Army. (2016). U.S. Army Social Media Handbook. Office of the Chief of Public Affairs. https://www.slideshare.net/alphacompanysfrg/the-united-states-army-social-media-handbook-2016?from_action=save adresinden erişildi.

van Dijk, J. (2016). *Ağ Toplumu*. (Ö. Sakin, Çev.) (3. bs.). İstanbul: Epsilon Yayıncılık.

Ventre, D. (Ed.). (2011). *Cyberwar and Information Warfare*. London : Hoboken, NJ: ISTE ; John Wiley.

Walker, J. (2019, 22 Nisan). Social Media and Cyber Security Risks in 2019. *Social Media Perth #SMPerth*. https://www.smperth.com/news/social-media-and-cyber-security-risks-in-2019/ adresinden erişildi.

Waltz, E. (1998). *Information Warfare: Principles and Operations*. Boston: Artech House.

Zhuk, A. (2015, 4 Temmuz). War In The Age Of Social Media—Jul. 04, 2015. *KyivPost*. https://www.kyivpost.com/kyiv-post-plus/war-in-the-age-of-social-media-392572.html adresinden erişildi.