İstihbarat Çalışmaları ve Araştırmaları Dergisi

Journal of Intelligence Research and Studies

Ocak 2024, Cilt: 3, Sayı: 1, ss.127-152

January 2024, Volume: 3, Issue: 1, pp.127-152

ISSN 2822-3349 (Basılı/Print) **ISSN 2822-3357 (Çevrimiçi/Online)**

Makaleye ait Bilgiler / Article Information

İnceleme Makalesi / Review Article

Makale Başvuru Tarihi / Application Date: 14 Ocak 2024 / 14 January 2024

Makale Kabul Tarihi / Acceptance Date: 20 Ocak 2024 / 20 January 2024

Makalenin Başlığı / Article Title

Sosyal Medya İstihbaratı Çerçevesinde Harekât Güvenliği

Operational Security Within The Framework of Social Media Intelligence

Yazar(lar) / Writer(s)

Erol Başaran BURAL

Atıf Bilgisi / Citation:

Bural, E.B. (2024). Sosyal Medya İstihbaratı Çerçevesinde Harekât Güvenliği. *İstihbarat Çalışmaları ve Araştırmaları Dergisi*, 3(1), ss.127-152, DOI: http://dx.doi.org/10.29228/icad.27

Bural, E.B. (2024). Operational Security Within The Framework of Social Media Intelligence. *Journal of Intelligence Research and Studies*, 3(1), pp.127-152, DOI: http://dx.doi.org/10.29228/icad.27

Terörizm ve Radikalleşme ile Mücadele Araştırma Merkezi Derneği

Research Center for Defense Against Terrorism and Radicalization Association

Adres/Address: Beytepe Mah. Kanuni Sultan Süleyman Bulvarı 5387. Cadde No:15A D:58

06800 Çankaya/Ankara

www.icadergisi.com

e-posta/e-mail: editor@icadergisi.com

İstihbarat Çalışmaları ve Araştırmaları Dergisi-İÇAD, 2024, 3(1) :127-152 İnceleme Makalesi
Journal of Intelligence Research and Studies-İÇAD, 2024, 3(1) :127-152 Review Article
DOI: http://dx.doi.org/10.29228/icad.27

SOSYAL MEDYA İSTİHBARATI ÇERÇEVESİNDE HAREKÂT GÜVENLİĞİ

Erol Başaran BURAL*

ÖZET

Askeri harekâtın en önemli boyutlarından birisi harekât güvenliğinin sağlanmasıdır. Harekât güvenliği, harekâta ilişkin kritik bilginin tespiti ve bu bilginin düşmandan korunması prensibine dayanır. Günümüzde kritik bilgiler, düşman veya hasım güçler tarafından büyük oranda açık kaynaklardan elde edilmektedir. Çalışmanın amacı, sosyal medyada özellikle asker şahıslar tarafından yapılan paylaşımların hasımlar tarafından sosyal medya istihbaratına dönüştürülerek askeri harekâtın güvenliğini tehdit edebileceğini örnekleriyle ortaya koymaktır. Çalışmada harekât güvenliği ihlaline yol açabilecek sosyal medya paylaşımları örnekleriyle incelenerek, harekât güvenliği alanında alınabilecek tedbirleri ortaya konulmaya çalışılmıştır. Sosyal medyada askeri harekât alanından paylaşılan görüntü, özçekim fotoğrafları ya da videoların hasımlarımız tarafından istihbarata dönüştürülebildiği; sosyal medyada paylaşılan kritik bilgilerin harekât güvenliği ve harekâtın icrasını olumsuz yönde etkileyebildiği hatta askeri zayiata neden olabildiği; sosyal medyada paylaşılan kritik bilgilerin sadece toplama açısından değil istihbarata karşı koyma açısından da ele alınması gerektiği çalışmanın sonuçları arasında yer almaktadır. Askerlerin harekât güvenliğini ihlal eden paylaşımlar yapmaları için hizmet içi eğitimlerin verilmesi, broşürler hazırlanarak bilgilendirme yapılması, paylaşım sahiplerine karşı hukuki yaptırımlar uygulanması gerektiği çalışmanın sonucunda sunulan teklifler içerisindedir.

Anahtar Kelimeler: *Açık Kaynak İstihbaratı, Sosyal Medya, Sosyal Medya İstihbaratı, Kritik Bilgi, Askeri Harekât, Harekât Güvenliği.*

OPERATIONAL SECURITY WITHIN THE FRAMEWORK OF SOCIAL MEDIA INTELLIGENCE

ABSTRACT

One of the most important dimensions of military operations is ensuring operational security. Operational security is based on the principle of detecting critical information regarding operations and protecting this information from the enemy. Today, critical information is largely obtained from open sources. The aim of this study is to explain that social media posts can be turned into social media intelligence by adversaries and threaten operational security. Social media posts that may lead to operational security violations were examined, and measures that could be taken were tried to be put forward in the study. Images,

* Terörizm ve Radikalleşme ile Mücadele Araştırma Merkezi Başkanı, erolbural@teram.org, ORCID: 0000-0002-3355-2018.

Makale Başvuru Tarihi / Application Date: 14 Ocak 2024 / 14 January 2024

Makale Kabul Tarihi / Acceptance Date: 20 Ocak 2024 / 20 January 2024

selfie photos, or videos shared on social media from the field of military operations can be turned into intelligence by our adversaries. Critical information shared on social media can negatively affect operational security and the execution of the operation and even cause military casualties. It is among the results of the study that critical information shared on social media should be handled not only in terms of collection but also in terms of countering intelligence. Proposals presented as a result of the study include providing in-service training to soldiers to prevent them from sharing posts that violate operational security, providing information by preparing brochures, and imposing legal sanctions against the share owners.

Keywords: Open Source Intelligence, *Social Media, Social Media Intelligence, Critical Information, Military Operations, Operational Security.*

GİRİŞ

İstihbarat toplama ve analizi, bir yapbozu çözmeye benzetilmektedir. İstihbarat toplayıcıları, birçok kaynaktan küçük bilgi parçalarını, yani yapbozun parçalarını elde etmeyi ve bu parçaları genel resmi oluşturacak şekilde bir araya getirmeyi amaçlarlar. İstihbarat toplama uzmanları yapbozun parçalarını çok sayıda farklı kaynaktan elde etmeye gayret ederler. Yapbozun parçaları radyodan, telefon konuşmalarından, mali amaçlı belgelerden, iş ilanlarından, seyahat için kullanılan biletlerden, nakliye belgelerinden, çöp kutusuna atılan evraklar gibi çok sayıda farklı ortamdan elde edilebilmektedir (Army Study Guide, 2023). Benzer şekilde günümüzde büyük verinin oluşturulduğu sosyal medya araçları da yapbozu tamamlayabilmek için gerekli bilgi kırıntılarını fazlasıyla barındırmaktadır.

İstihbarat teşkilatları ve çalışanları on yıllardır açık kaynaktan elde ettikleri verileri analiz ederek ülkelerinin güvenliğini sağlamaya ve karşı tarafın açıklarını ve zaaflarını ortaya koymaktadırlar. Teknolojinin günümüzdeki kadar gelişmiş olmadığı dönemlerde bile televizyon, radyo, gazeteler, dergiler, konferanslar, akademik metinler gibi kaynaklar üzerinden elde edilen açık kaynak bilgilerinin derlenerek analiz edilmesi en az gizli kaynaklardan bilgi edilmesi kadar yaygın hale gelmişti. Bununla birlikte teknolojinin gelişmesi, iletişim hızının artması ve bu amaçlar için kullanılan video, kamera ve telefon gibi araçların ucuzlayarak herkes için erişilebilir hale gelmesi dünyanın her hangi bir yerinde gerçekleşen olayların kısa süre içinde açık kaynaklarda paylaşılmasına neden oldu. Bu gelişme kısa süre içinde açık kaynak istihbaratını en hızlı, kolay erişilebilir ve ucuz istihbarat toplama yöntemi haline getirdi.

Açık kaynaktan bilgi toplama yaygınlaşırken sosyal medyanın gelişimi yeni bir bilgi üretim tarzını da beraberinde getirdi. Profesyonel bilgi

toplayıcılarının çoğu haber niteliği bulunan toplumsal, siyasal, ekonomik ve güvenlik içerikli konularla ilgileniyor olsa da gündelik yaşama dair bilgi üretiminin hızlanması, ucuzlaşması, hatta ekonomik kaynak ve prestij üretim aracı haline dönüşmesi sosyal medyanın istihbarat servislerinin dikkatini çekmesine neden oldu. Çünkü her ne kadar her gün üretilen milyarlarca bilgi tanesi ve olay anının ezici çoğunluğu gündelik yaşama ait olsa da bu üretilen bilgiler sadece daha çok kar sağlamak isteyen dev şirketlerin değil toplumsal değişimi, siyasal gelişmeleri, güvenlik olaylarını izlemek isteyen istihbarat servislerinin de ilgi alanı haline geldi. Böylece 2010'larda açık kaynak istihbarat toplama yöntemi olarak gözlemlenmeye başlayan sosyal medya istihbaratı kısa süre içinde ayrı bir istihbarat toplama disiplini hale gelmeye başladı.

Başlangıçta daha çok toplumsal ve ekonomik alanlarla sınırlıyken sosyal medyanın kullanımının çığ gibi büyümesi sonucunda kısa sürede sosyal medya istihbaratı askeri güvenliğin de bir parçası haline gelmiştir. Önceleri çeşitli devlet dışı aktörlerin ve terör örgütü üyelerinin sosyal medyayı kullanması dikkat çekerken bir süre sonra sosyal medyayı kullanma alışkanlığı ABD ve Rusya başta olmak üzere pek çok devletin ordusunu da etkilemeye başlamıştır. Bu nedenle sosyal medya istihbaratının son birkaç yıldaki kullanımının en yoğun olduğu alanlardan birisi çatışma alanlarının incelenmesi sayesinde istihbarat toplanması haline gelmiştir. Bu nedenle askeri harekât başta olmak üzere pek çok önemli güvenlik olayında sosyal medya boyutu önem kazanmıştır. Askeri harekâtın en önemli boyutlarından birisi harekât güvenliğinin sağlanmasıdır.

Harekât güvenliği konusunda askeri birlikler, süreklilik arz eden tedbirler almaya çalışırlar. İngilizce alan yazında "*Operational Security (OPSEC)"* şeklinde kullanılan tabir esasen askeri harekâta ilişkin kritik bilginin tespiti ve bu bilginin düşmandan saklanması, korunması esasına dayanmaktadır. Harekâta ilişkin kritik bilgilerin düşmanın eline geçmemesini sağlamanın temel yolu harekât güvenliğine ilişkin etkin tedbirler almaktan geçer. Harekât güvenliği bir kez alınan bir tedbirden ziyade uzun süreli ve devamlılık gösteren döngüsel bir süreci ifade eder. Yüzyıllar boyunca ordularının büyüklüğünü, askerlerinin eğitimini, sahip olduğu silah ve teçhizatı, hareket tarzını, savunma ve taarruz planlarını saklamak için talimnameler yazan, kurallar geliştiren ve bunun eğitimini veren köklü ordular bugünün dünyasında harekât güvenliğini sağlayabilmek için yeni bir meydan okumayla karşı karşıya kalmıştır. Bu meydan okuma

dost veya düşman silahlı kuvvetleri izleyerek onun örgütlenme, silahlanma ve personel yapısı gibi kritik konularında bilgi toplamak isteyen istihbarat toplama uzmanlarına karşı nasıl koyabileceğiyle başlamakta; yürütülen bir askeri harekâtın güvenliğinin nasıl sürdürülebileceğiyle devam etmektedir. Özellikle ABD'nin Irak ve Afganistan, Rusya'nın Ukrayna'da düştüğü zor durumlar ile harekât güvenliğinin sağlanamaması arasında ilişki de bulunmaktadır. Bu çerçevede bir askeri harekâtın güvenliğinin nasıl tehlikeye girebileceği konusu gittikçe daha önem kazanır hale gelmektedir.

Bu noktada bu çalışmanın temel amacı şöyle özetlenebilir: harekât güvenliği ihlaline yol açabilecek sosyal medya paylaşımlarını örnekleriyle analiz ederek, alınabilecek tedbirleri ortaya koymaktır.

Bu kapsamda çalışmanın temel problem cümleleri şu şekilde tespit edilmiştir:

1. Askeri harekâtın icra edildiği alanlardan elde edilen ve sosyal medyada paylaşılan bilgiler açık kaynak istihbaratına dönüşür mü?
2. Askeri harekâtın icra edildiği alanlardan elde edilen ve sosyal medyada paylaşılan bilgiler harekât güvenliği açısından hangi tür sorunlara neden olabilir?
3. Askeri harekâtın icra edildiği alanlardan elde edilen ve sosyal medyada paylaşılan bilgiler sadece toplama açısından değil istihbarata karşı koyma (İKK) açısından da ele alınması gereken bir olgu olarak değerlendirmek mümkün müdür?

Yukarıda tanımlanan üç problem cümlesinden hareketle bu çalışmada; askeri harekâtın güvenliğinin sağlanması için sosyal medya kullanımı sosyal medyadan istihbarat toplanması ve İKK perspektifiyle değerlendirilerek, konu hakkında eğitim materyallerinin hazırlanması ve personelin bu konuda bilinçlenerek sosyal medya kullanımının belli kurallar çerçevesinin dışında kısıtlanması gerekliliği ortaya konulmaya çalışılacaktır.

1. AÇIK KAYNAK İSTİHBARATI VE ASKERİ İSTİHBARAT

1.1. Açık Kaynak ve Sosyal Medyanın İstihbarat Toplama Çerçevesinde Önemi

İstihbarat disiplininde "açık kaynak" tabiri, "halkın erişimine açık olan" anlamında kullanılan bir tabirdir. Geleneksel açık kaynaklar arasında herkesin kolaylıkla erişebileceği ve bilgi toplayabileceği, kitap, gazete, dergi, televizyon, radyo, devlet ve resmi kurum verileri gibi bilgi kaynakları

yer almaktadır. Günümüzde ise açık kaynak denildiğinde, geleneksel açık kaynak araçlarına ilaveten internet ve internet üzerinden kullanılan sosyal medya araçları akla gelmektedir. Açık kaynakları kullanarak istihbarat toplama ise halkın kolaylıkla erişebildiği kaynaklardan ilgi duyulan bilgiyi bulma, söz konusu bilgiyi seçme, bilgiyi elde etme süreci şeklinde ifade edilmektedir (Clark, 2013, s.53).

Açık kaynak istihbaratı, belirlenmiş bir soruyu cevaplayabilmek amacıyla açık kaynaklarda belirlenen, toplanan bilginin işlenerek analiz edilmesi sonucunda üretilen istihbarattır (NATO, 2001, s.v). Her ne kadar insan istihbaratı kadar etkin olup olmadığı tartışılsa da Ransom tarafından 1970'lerde hazırlanan bir çalışmada mevcut istihbarat verilerinin %80'inin (Gill ve Phythian, 2018, s.131), Johnson ise istihbaratın %90'ının açık kaynaklardan (Johnson, 2007, s.221) elde edildiğini ifade etmektedirler.

Yaşadığımız dönemde internete bağlanmış bir cihaz hem istihbarat bilgisi yayabilen hem de istihbarat bilgisi toplayabilen bir aygıt haline dönüşmüştür. İnternete bağlı olan bu cihazlar düşmanlarımız için önemli sayılabilecek çok sayıda bilgi üretmektedir. İnternete bağlı olan her türlü cihazın ürettiği büyük miktardaki veri yığını istihbarat servisleri için bilgi kaynağı haline gelmiştir. Günümüzde istihbarat servislerinin güvenlik kameraları, internet üzerinden kumanda edilen akıllı cihazlar, trafik verileri ve sosyal medya araçları gibi çok sayıda farklı kaynaktan veri toplayarak istihbarat ürettikleri değerlendirilmektedir (Office of the Director of National Intelligence, 2016, s.4).

İnternette oluşturulan büyük veriden istenilen verilerin bulunabilmesi ve tasnif edilebilmesi amacıyla günümüzde yapay zekâ kullanımına devreye girmiştir. Açık kaynak istihbaratı toplamak maksadıyla yapay zekâ dünyanın dört bir yanında üretilen devasa boyutlu veriyi tarayabilmekte, adeta bir istihbarat elemanı gibi çalışabilmektedir. İstihbarat servisleri için yapay zekâ açık kaynaklardan toplama faaliyetlerinde önemli bir hız ve doğruluk sağlayabilmektedir (Tucker, 2020).

İstihbarat servisleri özellikle toplum güvenliğini sağlayabilmek amacıyla sosyal medya istihbaratını kullanmaktadırlar. Taktik seviyede sosyal medya istihbaratı gerçek zamanlı olarak belirli bir durum hakkında güncel bilgi sağlarken, güvenliğe ilişkin olayların takip edilmesini sağlamaktadır. Sosyal medya istihbaratı operatif seviyede gelecekte oluşması muhtemel güvenlik olaylarının ortaya çıkarılmasını sağlayabilmektedir.

Stratejik seviyede ise diğer ülkeler tarafından ortaya konulan tehditler hakkında bilgi üretebilmektedir. İstihbarat servisleri bunlara ilaveten diğer ülkelerde stratejik etkiler yaratmak ve hasımlarını yanıltmak için sosyal medyayı kullanabilmektedirler (Momi, 2021).

Sosyal medya istihbaratı sayesinde sosyal medyada tartışılan konuları anlamak ve izlemek, sosyal medyada etkin olan şahısları belirlemek, kullanıcı davranışlarını tahmin etmek mümkün görülmektedir. Sosyal medya istihbaratı ayrıca belirli bir kişiyi ya da topluluğu tespit etmek ve bulmak, şahısların dijital ayak izlerini bulmak ve takip etmek için de kullanılmaktadır (Tudoriu, 2019).

Sosyal medya artık bireylerin ayrılmaz bir parçası haline gelmiştir. Hızla geleneksel medyanın yerini almaya aday olan sosyal medya sosyal ağların teşkil edildiği, iletişimden eğlenceye çok farklı alanlarda kullanılan ve büyük miktarda veri üreten bir platform haline gelmiştir. Sosyal medya araçlarının ve sosyal medya kullanıcılarının sayısının gün geçtikçe artması bu alanda istihbarat üretimini de artırmıştır. Bu kapsamda istihbarat servisleri gibi askeri istihbarat üreten birimlerin de dikkatleri açık kaynaklar ve sosyal medya üzerinde yoğunlaşmaktadır.

1.2. Askeri İstihbarat Kavramı

Komutanlar, tehdidin özelliklerini, amaçlarını, hedeflerini, etki alanlarını, hareket tarzlarını anlayabilmek için doğru ve tahmine dayalı istihbarata ihtiyaç duyarlar. İstihbarat, tehdide ait yeteneklerinin doğru zamanda ve yerde tespit edilmesi, tanımlanması, hedef alınmasında kritik öneme sahiptir. Komutanlar ve karargâhı stratejik seviyede tehdidin güçlü yönleri, zayıf noktaları, teşkilatı, teçhizatı, yetenekleri, eğitim durumu, askeri birlikleri kullanma ve kontrol etme taktikleri hakkında ayrıntılı bilgiye sahip olmak istemektedirler. Bu ayrıntıya sahip olmak için ise istihbarat fonksiyonunun kullanılmasını gerekmektedir (US Department of the Army, 2023, s.I-6). Savaşan taraflar minimum sayıda asker kaybetmek isterken aynı zamanda en az seviyede güç kullanarak savaşı kazanmak istemektedirler. Bu açıdan ele alındığında askeri istihbarat, askeri harekâtın plan, program ve politikalarının hazırlanabilmesi için gerekli bilgileri sağlayan istihbarat çeşididir (Urhal, 2008, s.204).

Askeri istihbaratın amacı, hükümetlerin ve komuta heyetinin karar vermesi için veri toplamak ve bilgi üretmektir. Askeri istihbarat faaliyetleri, üç amaca hizmet etmektedir:

a. Rakibin yeteneklerinin ve niyetlerinin kıymetlendirilmesi,

b. Silahlı kuvvetlerimizin kapasitesinin arttırılması,

c. İstihbarat üstünlüğü elde ederek caydırıcılık ve önleme sağlamaktır (Eyal ve Asher, 2015, s.1).

Bir başka açıdan askeri istihbarat muharebenin yürütüleceği alanda muharebeyi kazanmak i.in ihtiyaç duyduğu istihbarat türüdür. Askeri istihbarat düşmanın gücü, konumu, komuta kademesi, eğitim seviyesi, silah ve teçhizatı, moral gücü, niyeti, muharebe sahasının arazi yapısı ile hava durumu hakkında bilgilerin elde edilmesi ve kıymetlendirilmesi sürecidir (Gudgin, 1999, s.2).

Askeri istihbaratın ilgi alanı fiziksel ve fiziksel olmayan güç kapsamında değerlendirilebilir. Fiziksel güç alanında hasım ülke ordusunun asker miktarı, kara, hava ve deniz gücü, taktik teşkilatı, teçhizatı ve teçhizatının kalitesi ile miktarı, silah envanteri, askeri üslerinin konumu ve durumu, mühimmat durumu ve miktarı, askeri havaalanlarının ve tersanelerinin durumu, ikmal ve lojistik ile ilgili yetenekleri yer almaktadır. Fiziksel olmayan alanda ise düşman askerlerinin eğitim durumu, askerlerin savaş tecrübesi, askerlerinin kalite durumu, komuta kademesindekilerin kişilik özellikleri, askeri geleneğin gücü, halkın orduya verdiği önem ve destek gibi hususlar sayılabilir (Kent, 2002, s.23).

Askeri istihbaratın amacı, askeri harekâtı yürüten komuta kademesini bilgilendirmek, harekât ortamına ait ihtiyaç duyulan bilgileri sağlamak, hedef tespit etmek, harekât planının hazırlamak için gerekli bilgiyi temin etmek, düşmanı aldatmak ve harekâtın gidişatını kıymetlendirmektir (Joint Chiefs of Staff, 2013, I-3). Ayrıca askeri istihbarat; komutanın doğru karar vermesine yardımcı olunması, öngörülemeyen durumlarla karşılaşılmasının engellenmesi, birliklerin bekasının tesis edilmesi, harekât planının doğru yapılmasına katkı sağlanmasını amaçlar (Connable, 2012, s.12).

Askeri istihbaratın bir parçası olan İKK ya da karşı istihbarat ise askeri birliklere ait bilgi ve teknolojiyi düşmandan korumak maksadıyla yabancı istihbarat servisleri, düşman ülke orduları ya da hasım güçlerden gelebilecek tehditlerin tespitine, analizine odaklanır. Ordular İKK'yı karşı casusluk, kuvvet koruma, tehdidin tespiti ve tehdide karşı koymak için bilgi toplama, kritik tesis/alt yapı ile kritik askeri bilgiyi koruma amacıyla kullanırlar (US Department of the Army, 2023, s.1-16).

1.3. Açık Kaynak İstihbaratı ile Askeri İstihbarat Arasındaki İlişki

Askeri istihbarat birimleri sosyal medyaya ilgilerini artırsalar da açık kaynak istihbaratına olan ilgilerinin yeni olmadığı da bilinmektedir. Örneğin Napolyon'un açık kaynak istihbaratına önem verdiği, özellikle Birleşik Krallık menşeli gazeteleri dikkatle okuduğu bilinmektedir. Napolyon'un ayrıca harekât güvenliği çerçevesinde izin verilmeden askeri bilginin yayımlanmaması için talimatlar verdiği, kara ve deniz kuvvetleri birliklerinin hareketleri konusunda gazetelerde hiçbir şey yayımlanmaması için tedbirler aldığı da edinilen bilgiler arasındadır (Erol, 2022, s.31).

Açık kaynak istihbaratı özellikle insani yardım ya da terörle mücadele gibi harekât çeşitlerinde komuta kademesine daha hızlı bir şekilde doğru bilgiyi temin edebilmektedir. Açık kaynak istihbaratı, emarelerin tespit edilmesi, plan geliştirme, acil durum planlaması yapma, güvenlik desteği sağlama açısından önemli bir potansiyele sahiptir. Açık kaynak istihbaratı bir komutanı en hızlı şekilde yönlendirmenin bir aracı olarak hayati önem taşımaktadır (Steele, 1995, ss.458-459).

Başarılı bir açık kaynak istihbaratı kullanımı komutanın açık kaynak istihbaratını nasıl anladığına ve açık kaynağın kullanılmasına ilişkin verdiği talimatlara bağlıdır. Açık kaynak istihbaratı komutanın niyet ve maksadını desteklemek amacıyla, tıpkı diğer istihbarat disiplinleri gibi harekat planlamasına entegre edilmelidir. Bu kapsamda açık kaynak istihbaratı sosyal medya takibini, büyük veriye erişimi, diğer istihbarat türleri için uyarı niteliği taşıyabilecek anlık bilgi teminini, hedef hasarı tespitini, geleneksel medya ve süreli yayınların takibini içine alır (US Department of the Army, 2023, s.1-19).

Askeri istihbarat çerçevesinde açık kaynak istihbaratı askeri harekâtın sürdürüldüğü arazi ve harekât alanında bulunan sivillere yönelik faydalı bilgiler sağlayabilmektedir. Ayrıca açık kaynak istihbaratı komutana düşman askeri birliklerinin silah, teçhizat, imkân ve kabiliyetleri hakkında faydalı bilgi sağlayabileceği gibi aynı zamanda hedef bölgedeki hava ve yol durumu ile arazi şartları hakkında da önemli bilgiler sunabilmektedir (Steele, 1997, ss. 3-4).

Başka bir ülkede yapılacak askerî harekâttan önce ilk başvuruda bulunulacak ve en hızlı istihbarat kaynağı açık kaynaktır. Bunun temel nedeni açık kaynağa erişimin hızı, ikincisi ise diğer kaynaklara göre oldukça ucuz olmasıdır. Açık kaynak istihbaratı kullanılarak aynı zamanda diğer

kaynakların israf edilmesi de önlenmiş olmaktadır. Stratejik düzeyde açık kaynak istihbaratı kültürel, demografik, coğrafi ve siyasi bilgiler sağlayabilmektedir. Operatif düzeyde ise açık kaynaklardan hava durumu, mevcut su kaynakları, meskûn mahaller ve özellikleri, harekât alanındaki nüfuzlu kişilere ait bilgiler öğrenilebilmektedir. Taktik düzeyde ise açık kaynak istihbaratı sayesinde açık kaynaklarda yer alan ayrıntılı haritalardan faydalanılabilmektedir (Özdağ, 2015,ss. 150-152).

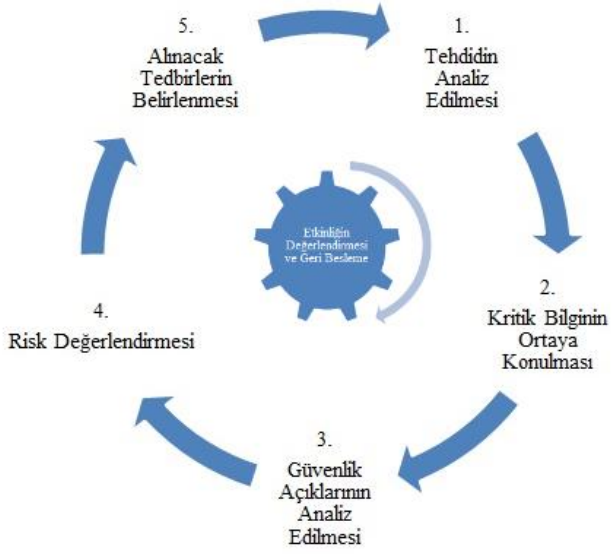
Açık kaynak istihbaratı askeri operasyonlar için harekât ortamına ilişkin durumsal farkındalık sağlayabilmektedir. Açık kaynak istihbaratı ayrıca düşmanın ve harekât alanındaki sivillerin özellikleri hakkında bilgi sağlarken, düşmanın niyetini ve muharebe sahası istihbarat hazırlığı için gerekli istihbaratı üretebilmektedir. İnsanların görüşlerini ifade etmesi ve bilgi yayması için önemli bir açık kaynak bilgi kanalı olan sosyal medya, çok sayıda yararlı bilgiyi de içermektedir. Sosyal medya, komutanın istihbarat elde etmesine ve muharebe alanındaki durumu doğru bir şekilde anlamasına yardımcı olabilmektedir. Askeri birlikler, sosyal medyadaki bilgileri analiz ederek gerçek zamanlı durumu anlayabilmektedir (Ju vd., 2020, ss.6-8).

2. ASKERİ HAREKÂTIN GÜVENLİĞİ

Askeri harekâtın başarısı gizliliğe ve yaratacağı sürpriz etkisine bağlıdır. Harekât güvenliği ise, birliklerin ne zaman harekete geçeceği / geçtiği, nereye intikal edeceği / ettiği gibi askeri açıdan kritik olan bilginin düşmanlarınızın eline geçmesini engelleyerek gizliliği sağlamaktadır. Düşmanlarımız ve hatta dostlarımız dahi askeri harekâtı etkileyebilecek kritik bilgiyi toplamak istemekte ve bu amaçla askeri personeli izlemektedirler. Yabancı ülke ajanları ya da devlete düşman konumunda olan devlet dışı silahlı aktörler özellikle internetin bilgi toplamada kritik öneme sahip olduğunu değerlendirmektedirler (US Marine Corps, 2023).

Askeri harekâtın güvenliğini ihlal edebilecek kritik bilginin tespiti ve bu bilginin düşmandan korunması prensibine dayanan harekât güvenliği sürecini Şekil 1.'deki gibi resmetmek mümkündür. Buna göre harekât güvenliğinin ilk basamağını tehdidin analizi, ikincisini kritik bilginin tespiti, üçüncü basamağı güvenlik açıklarının tespit edilmesi, dördüncüsünü risk değerlendirmesi ve son basamağı da alınacak tedbirlerin belirlenmesi teşkil eder. Sürecin değerlendirilmesi ve düzeltmelerin yapılması ise sürekli uygulanan bir faaliyeti ifade eder.

Şekil 1. Harekât Güvenliği Döngüsü (Kaynak: Yazar tarafından oluşturulmuştur)



Döngünün birinci aşamasında yer alan "tehdit" ifadesi askeri harekâtı tehlikeye atma niyeti ve kabiliyetine sahip olan düşmanı tarif eder. Bu safhada düşmanın kim olduğu ve düşman imkan / kabiliyetlerinin analizi yapılır. Düşman veya muhasım, ulusal çıkarları, askeri faaliyetleri tehlikeye atma potansiyeline sahip bir birey, grup, kuruluş veya devlet olabilir (Director of National Intelligence, 2022).

İkinci basamakta bulunan kritik bilgi ifadesi ise düşmanın harekâtı tehlikeye atmak veya kesintiye uğratmak için harekata yönelik niyet, yetenek ve askeri faaliyetlerle ilgili ayrıntıları içerir. Kritik bilgiler içerisinde askeri harekâtın yeri, zamanı, niyeti, lojistik, sınırlılıklar gibi önemli bilgiler de yer alır (Director of National Intelligence, 2022). Kritik bilgiler gizli olmasalar da, askeri birlikler için "kritik" olabilirler. Kritik bilgi düşman tarafından ele geçirildiğinde askeri harekatın başarısı ve birlik / personel güvenliğini tehlikeye girebilir. Bu nedenle harekat güvenliğini tehlikeye atabilecek kritik bilgi aile fertleri dahil hiçkimse ile paylaşılmamalıdır (US Marine Corps, 2023).

Üçüncü aşamada güvenlik açıklarının analiz edilmesi gelir. Harekâtın güvenlik açıklarının genellikle iletişim kanalları içerisinde kendisine yer bulduğunu söyleyebilmek de mümkündür. Düşman ya da hasım güçler askeri operasyonlara yönelik güvenlik açıklarını tespit edebilmek adına sürekli olarak gözetler ve izlerler (Director of National Intelligence, 2022).

Risk değerlendirmesi basamağında ifade edilen risk, düşmanın askeri harekata ilişkin kritik bilgiyi ele geçirmesidir. Risk derğerlendirmesi aşamasında düşmanın ya da hasım güçlerin askeri harekata ilişkin kritik bilgiyi ele geçirme olasılığı değerlendirilmektedir. Son aşamada yer alan alınabilecek karşı tedbirler ise kritik bilgilerin düşman tarafından ele geçirilmesi olasılığını azaltır. Bu tedbirler arasında birlikleri ve personeli tehditler ve güvenlik açıkları konusunda eğitmek, geleneksel güvenlik önlemlerini (fiziksel, kişisel, siber vb.) almak gibi hususlar yer alır. Harekat güvenliğine yönelik alınan tedbirlerin değerlendirilmesi ve müetakip tedbirlerin belirlenmesi için süreç sürekli olarak gözlemlenir ve değerlendirilir. Eksik hususların yapılan değerlendirme sonucunda giderilmesi sağlanır (Director of National Intelligence, 2022).

Askeri personelin kritik bilgileri internet ve özellikle sosyal medya üzerinden kolayca paylaşabilme ihtimali göz önüne alındığında harekat güvenliği konusu günümüzde eskisinden daha büyük bir endişe kaynağı haline gelmektedir. Düşman açısından bakıldığında ise internet ve sosyal medya üzerinden askeri harekata yönelik istihbarat toplamak en ucuz ve hızlı yöntem olarak görülmektedir (Bejar, 2010, ss.1-7).

3. SOSYAL MEDYA İSTİHBARATI VE HAREKÂT GÜVENLİĞİ

Sosyal medya kullanımındaki hızlı büyüme ve sosyal medyada üretilen büyük veri, sosyal medya istihbaratı adıyla ifade edilen yeni bir istihbarat disiplinini ortaya çıkartmıştır (Omand, 2013, s.139). Sosyal medya istihbaratı; sosyal medyadan verilerin toplanması, analiz edilmesi ve kullanıma sunulmasını ifade etmektedir (Bartlett ve Reynolds, 2015, s.27). Başka bir ifadeyle sosyal medyada araçlarından üretilen istihbarata sosyal medya istihbaratı denir (Omand vd., 2012, s.802). Sosyal medya istihbaratının temel hedefi, karar alcıların önündeki belirsizlikleri en aza indirmektir (Ivan vd., 2015, s.506).

Sosyal medya istihbaratı için sosyal medya paylaşımları oldukça önemlidir. Bazen bir sosyal medya paylaşımı, istihbarat disiplinleri için yararlı olabilecek çok sayıda bilgiyi bir arada barındırabilir. Mesela bir Facebook paylaşımı coğrafi konum verilerini içerebilir. Bu paylaşımın içerdiği coğrafi konum verisi görüntü istihbaratı vasıtasıyla değerlendirilebilecek kıymette olabilir. Facebook paylaşımını yapan cihazın sinyalleri ise sinyal istihbaratı ile analiz edilebilir. Facebook paylaşımını yapan kullanıcının çevrimiçi hareketliliği ve paylaşımlarında diğer insanlara

ilettiği duygular bu kullanıcının insan istihbaratı profilinde kullanılabilir (Mahood, 2014, s.4).

Tüm bu bilgiler ışığında sosyal medyanın günümüzün en önemli bilgi kaynağı haline geldiği, bu kaynaktan üretilen istihbaratın ise hem devletler hem de devlet dışı aktörler tarafından kullanıldığı, sosyal medya istihbaratının diğer istihbarat disiplinlerine destek olduğu, anlık ve hızlı değerlendirmeler sonucunda karar alıcıların zihnindeki belirsizlikleri ortadan kaldırmaya yardımcı olduğu söylenebilir. Özellikle terör örgütleri, milisler ve vekalet verilmiş silahlı yapılar gibi devlet dışı silahlı aktörlerde artık sosyal medyada üretilen büyük veriyi takip etmekte, izlemekte ve anlamlandırarak istihbarata dönüştürmektedirler.

Yakın geçmişte, farklı coğrafyalarda meydana gelen silahlı çatışmalarda ve savaşlarda sosyal medya kullanımında görülen artış dikkat çekicidir. Sosyal medyanın savaşlarda ve çatışmalarda daha yaygın bir şekilde kullanılması, gelecekte sosyal medyanın istihbarat açısında yeni imkânlar sunacağıan işaret etmektedir. Örnek olarak, askeri harekatın devam ettiği bölgelerde telefonla çekilen ve sosyal medyada yayımlanan özçekim fotoğrafından, fotoğrafın çekildiği mevkiinin coğrafi konumunu bulabilmek mümkün olabilmektedir (Treverton ve Miles, 2014, s.16). Bu çerçevede günümüzde harekat güvenliğini tehlikeye sokan en önemli faktörün sosyal medyada paylaşılan kritik bilgiler olduğu aşikardır. Sosyal medyada paylaşılan gönderilerde askeri birliklerin yeri, konumu, teşkilatı, imkan ve kabiliyetleri ile taktik ve tekniklerine ilişkin bilgiler bulunabilmektedir. Harekat güvenliğini ihlal edebilecek bir diğer faktör ise bu paylaşımlardan askeri birliklerin coğrafi konumlarının elde edilebilmesine ilişkin risktir.

Hasım güçler tarafından sosyal medyadan elde edilen istihbaratın harekat güvenliğini olumsuz yönde nasıl etkilediğini daha iyi anlatabilmek için örnekleri analiz etmek faydalı olacaktır. 2000 yılının Ekim ayında bir Amerika Birleşik Devletleri (ABD) askeri personeli eşine müteakip Salı günü bir liman ziyareti için Aden'de (Yemen) olacaklarını belirten bir e-posta göndermiştir. Askerin eşi bu kritik bilgiyi, diğer aile bireyleri ve arkadaşlarının askere ait güncel bilgileri takip etmek için hazırladığı web sayfasında yayınlamıştır. Bu bilgiyi internette yakalayan bir terörist, askerin adı ve rütbesini tespit ederek aynı zamanda askerin "USS Cole" isimli gemide görev yaptığını belirlemiştir. 12 Ekim 2000'de El Kaide terör örgütü mensupları patlayıcı dolu bir tekneyle USS Cole gemisine yanaşarak terör

eylemini gerçekleştirmiştir. Saldırıda 17 ABD askeri hayatını kaybederken çok sayıda askerde yaralanmıştır (US Marine Corps, 2023).

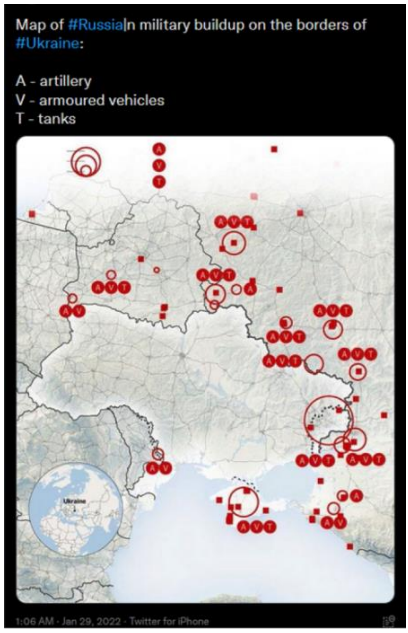
Diğer bir örnek ise yakın dönem çatışma alanlarından, Ukraynadan. Doğu Ukrayna'da bulunan Rus asker, kendisinin ve 10'uncu Spetsnaz Tugayına mensup askerlerin fotoğraflarını ve videolarını, daha çok Rusların kullandığı VKontakte adlı sosyal medya platformunda paylaşmıştır. Askerin paylaşmış olduğu bazı fotoğraf ve videolarda coğrafi konum özelliğinin açık olması nedeniyle, askerlerin kaldıkları "Grand Prix" isimli golf klübünün koordinatları kolaylıkla tespit edilmiş ve Ukrayna hava kuvvetleri tarafından belirlenen koordinatlara hava taarruzu düzenlenmiştir (Schogol, 2023).

Ukrayna'dan çarpıcı bir başka örnek ise Rus Ordusunda görevli Muhabere Çavuş Sanya Sotkin'in paylaşımlarıyla ilgilidir. Sotkin Rusya'nın Ukrayna'da asker bulundurduğunu inka ettiği günlerde Instagram üzerinden kendisini askeri araç içerisinde gösteren fotoğraflar paylamıştı. Sotkin'in Şekil 2'de görülen paylaşımları aynı zamanda coğrafi konum bilgisi de içermekte ve konum olarak Ukrayna'da Derkul Nehri'nin doğusunda olduğunu ispatlamaktaydı (Gallagher, S. (2023).

Şekil 2. Muhabere Çavuş Sanya Sotkin'in Paylaşımlarına Ait Coğrafi Konum Bilgileri (Kaynak: Gallagher, S. (2023).

Güncel olması açısından Ukrayna-Rusya Savaşıyla bilgili bir örnek daha paylaşmakta fayda görülmektedir. Yukarıdaki örneğe benzer şekilde Rus hesapların paylaştığı tweetler bir arada analiz edilerek, trenlerle Ukrayna doğu sınırlarına yapılan Rus yığınaklanması ayrıntılı şekilde ortaya konulmuş, üstelik bu birliklerin harita üzerindeki yerleriyle birlikte hareket için ne şekilde teşkilatlandıkları da belirlenmiştir. Şekil 3'te Rus askeri birliklerinin sosyal medyadan tespit edilen yığınaklanmalarının haritalandırmış hali görülmektedir (Vandersmith, 2023).

Şekil 3. Rus Askeri Birliklerinin Yığınaklanması (Kaynak: Vandersmith, 2023).



Harekat güvenliği ihlaline ilişkin verilebilecek bir diğer örnek de ABD ordusuna ait. Örnek olay 2007 yılında Irak'ta meydane gelmiştir. AH-64 tipi taarruz helikopterlerinin bulunduğu hangarda çektikleri helikopterlerle çektirdikleri özçekim fotoğraflarını sosyal medyada paylaşan askerler, coğrafi konum özelliğini kapatmamışlardır. Facebook'ta paylaşılan fotoğrafı inceleyen terör örgütü mensupları coğrafi konumu tespit ederek ilgili yere saldırı düzenlemiş ve AH-64 helikopterleri hasar görmüştür (Rodewig, 2012).

Diğer ülke ordularında görülen harekat güvenliği ihlalleri ne yazık ki Türk Silahlı Kuvvetlerinde de görülmektedir. Örneğin, Şekil 4'te yer alan sosyal medya paylaşımında görülen fotoğraf, Kuzey Kıbrıs Türk

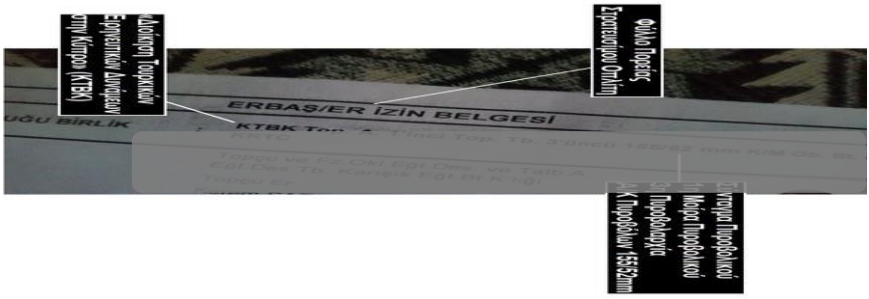
Cumhuriyetinde askerliğini yapan bir asker tarafından sosyal medyada paylaşılmıştır. Söz konusu fotoğrafı sosyal medyada gören Yunan ve Rum basını, fotoğraftaki tankların Leopard2-A4 olduğunu belirtmiş, kırkiki adet Leopard2-A4'ün Kuzey Kıbrıs Türk Cumhuriyetinde bulunduğu konusunu kamuoyu ile paylaşmış (Defence Turk, 2019) ve kendi lehlerine propagandaya başlamıştır. Bu propaganda kampanyası sonucunda Güney Kıbrıs Rum Kesimi, taarruza esas silah sistemlerinin Kıbrıs adasına sevk edildiğini, bu durumun ambargo ihlali anlamına geldiğini hem de "barış sürecini" sekteye uğrattığı mealinden görüşlerini içeren propaganda çalışmalarını yürütmüşlerdir. Sonuçta Yunanistan ve Güney Kıbrıs Rum Kesimi Almanya'ya diplomatik baskı yaparak ve Altay tanklarında kullanılması planlanan güç aktarma organlarıyla ilgili vetonun devamını sağlamışlardır (Erdem, 2021).

Şekil 4. Asker Paylaşımının Yunan Basını Tarafından Sosyal Medyada Paylaşımı (Kaynak: https://twitter.com/isozygio/status/1094884572028899328)[1]

Yine KKTC ile ilgili bir örnekte bir askerin sosyal medyada paylaştığı askeri izin belgesi (Şekil 5) üzerinden KKTC'ye T-155 Fırtına kundağı motorlu obüs konuşlandırıldığı belirtmiştir (Defence Turk, 2019). Bu paylaşımın sonucunda Rum ve Yunan basını tarafından yürütülen propaganda sonucunda ise Güney Kıbrıs Rum Yönetimi bir ülkeden kundağı motorlu obüs sistemi temin etmişlerdir (Erdem, 2021).

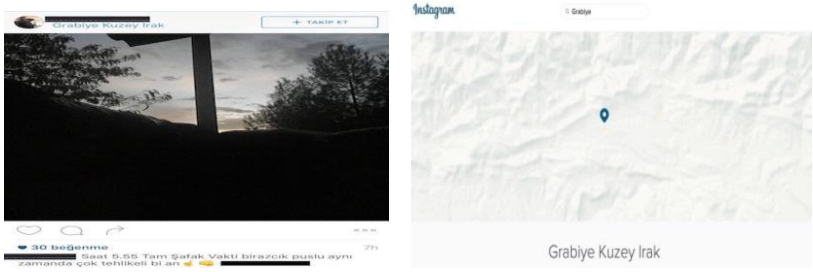
[1] Özçekimi paylaşan askerin yüzü karartılmıştır.

Şekil 5. Sosyal Medyada Paylaşılan Er İzin Belgesi (Kaynak: https://twitter.com/isozygio/status/1099951233115262977)[2]



Askeri harekata ait bilgilerin ihlaline ilişkin bir diğer örnek de Instagram uygulamasında yapılan bir paylaşımla ilgilidir: "Saat 5.55 tam şafak vakti. Birazcık puslu aynı zamanda çok tehlikeli bir an" yazan paylaşımla birlikte Şekil 6'da görülen fotoğraf paylaşılmıştır. Bir açık kaynak araştırmacısının sosyal medyada gördüğü paylaşımı incelemesi neticesinde coğrafi konum özelliğinin kapatılmadığı, fotoğrafın Irak'ın kuzeyinde "Grabiye" isimli bir mevkiden paylaşıldığı tespit edilmiştir (Ergürel, 2015).

Şekil 6. Instagramdan Konum Paylaşımı (Kaynak: Ergürel, 2015).[3]



Daha güncel bir örnek olması açısından TikTok uygulaması ve bu uygulamadan yapılan askeri paylaşımlardan söz etmek uygun olacaktır. Motivasyonlarının ne olduğu bilinmemekle birlikte TikTok uygulamasında çok sayıda askeri personelin paylaşım yaptığı görülmektedir. Bu paylaşımların büyük çoğunluğu askeri disiplini ihlal eden görüntüler içerirken bir kısmı da harekât güvenliğini ihlal eden görüntülere yer

[2] Her ne kadar açık kaynaklarda yer almışsa da belge üzerindeki askeri birlik ismi karartılmıştır.
[3] Paylaşımı yapan hesap ismi kapatılmıştır.

vermektedir. Örneğin Şekil 7'de görülen paylaşım örneğinde olduğu gibi TikTok'ta paylaşılan videolarda üs bölgelerindeki silah mevzileri ve üs bölgesinin konumunu açığa çıkarması muhtemel görüntüler yayımlanmıştır. Videoda yer alan arazi arızalarından yola çıkarak üs bölgesinin coğrafi koordinatlarını tespit etmenin mümkün olduğunu bilmeyen ya da bilse dahi farklı nedenlerle bu ihlali göz ardı eden çok sayıda paylaşım özellikle TikTok uygulamasında mevcuttur.

Şekil 7. TikTok Uygulamasında Paylaşılan Mevzi Görüntüsü (Kaynak: Öztürk, S, [@serkanozt06], 2022, 29 Kasım).

Şekil 8'de görseli bulunan bir diğer TikTok video paylaşımında ise harekât alanının coğrafi özellikleri açıkça görülmektedir. Ayrıca harekatta kullanılan taarruz ve genel maksat helikoptlerinin görüntüleri paylaşılarak harekâtın icra yöntemlerine ilişkin kritik bilgiler de paylaşılmış olmaktadır.

Şekil 8. TikTok Uygulamasında Paylaşılan Harekat Alanı Görüntüsü (Kaynak: Öztürk, S, [@emirhanyarkan], 2023, 13 Haziran).

Şekil 9, 10 ve 11'da görülen TikTok paylaşımlarında ise harekât alanındaki askeri birliklerin kullandığı silah malzeme ve teçhizata ait görüntüler paylaşılmaktadır.

Şekil 9. TikTok Uygulamasında Paylaşılan Silah ve Teçhizat Görüntüleri (Kaynak: Taha, E, [@emirhan.taha], 2023, 23 Aralık).

Şekil 10. TikTok Uygulamasında Paylaşılan Teçhizat Görüntüleri (Kaynak: kmando7333, [@kmndo], 2022, 20 Ağustos).

Şekil 11. TikTok Uygulamasında Paylaşılan Silah Görüntüleri (Kaynak: komando056. [@cankat] (2023, 11 Mayıs).

SONUÇ

Askeri harekâta ilişkin kritik bilginin tespiti ve bu bilginin düşmanın eline geçmemesi amacını taşıyan faaliyetlerin bütününe harekât güvenliği denilir. Harekât düzenini bozmak, harekâta katılan askeri birliklere baskın

düzenlemek, harekâtın gidişatını sekteye uğratmak amacıyla düşman veya hasım güçler sürekli olarak harekâta katılan birlikler hakkında istihbarat toplamaktadırlar. Günümüzde hasım güçler tarafından toplanan istihbaratın büyük kısmı ise açık kaynaklardan, bu istihbaratın çoğunluğu ise sosyal medyadan sağlanmaktadır.

Bu nedenle çalışmanın araştırma sorularından birincisi olan "Askeri harekâtın icra edildiği alanlardan elde edilen ve sosyal medyada paylaşılan bilgiler açık kaynak istihbaratına dönüşür mü?" sorusunun cevabı kesinlikle evettir. Sosyal medyada askeri harekât alanından paylaşılan masum görüntüler, özçekim fotoğrafları ya da videoları örneklerle açıklandığı üzere istihbarata dönüştürülebilmektedir.

İkinci temel problem cümlesi ise: "Askeri harekâtın icra edildiği alanlardan elde edilen ve sosyal medyada paylaşılan bilgiler harekât güvenliği açısından hangi tür sorunlara neden olabilir?" şeklinde tasarlanmıştır. Sosyal medyada paylaşılan kritik bilgiler harekât güvenliği ve harekâtın icrasını olumsuz yönde etkileyebilmekte, askeri zayiata neden olabilmekte ya da en basit haliyle hasım güçlere birliklerimiz hakkında ayrıntılı bilgi sağlamaktadır. İstihbarata dönüştürülen sosyal medya paylaşımları hasım ya da düşman tarafından değerlendirilmekte, elde edilen bilgilere uygun olarak askeri birlikler hedef alınmakta ya da bu bilgiler propagandanın bir parçası olarak kullanılmaktadır.

Çalışmanın son araştırma sorusu: "Askeri harekâtın icra edildiği alanlardan elde edilen ve sosyal medyada paylaşılan bilgiler sadece toplama açısından değil İKK açısından da ele alınması gereken bir olgu olarak değerlendirmek mümkün müdür?" şeklindedir. Çalışma süresince yapılan inceleme neticesinde harekât güvenliği ihlaline yol açan sosyal medya paylaşımlarının İKK açısından da ele alınmasının zorunlu olduğu sonucuna ulaşılmıştır. Zira İKK faaliyetlerinin temel amacı askeri birliklerin ve komutanın niyetini düşmandan gizlemek, düşmanın askeri birlikler hakkında istihbarat elde etmesinin önüne geçmek amacıyla tedbir almaktır. Bir başka açıdan İKK tedbirleriyle silahlı kuvvetlerin emniyeti sağlamak, düşman istihbarat faaliyetlerini etkisiz kılmak amaçlandığından ve bu maksatla karşı önlemleri planlamak ve uygulamak söz konusu olduğundan, harekât güvenliği kapsamında alınan tedbirler paralellik göstermektedir.

Harekât güvenliği ve harekât güvenliğinin ihlali kapsamında alınabilecek tedbirler de bulunmaktadır. Harekât güvenliğini sağlayabilmek

için kurum ve kuruluşlar tarafından halihazırda çok sayıda tedbir alındığı, emir ya da talimatlar verildiğine dair hiçbir şüphe yoktur. Ancak yine de kurum ve kuruluşlar tarafından yapılması gerektiği düşünülen işlemler olduğu değerlendirilmektedir. Bu kapsamda her ne kadar yasaklansa da akıllı telefonların kullanılmasının ve sosyal medya paylaşımlarının engellenmesinde güçlük çekildiği anlaşılmaktadır. Bu nedenle personele akıllı telefon ve sosyal medya paylaşım ayarları konusunda eğitim vermek, veya alınan tedbirleri daha sıkı takip etmek etkin sonuçlar verebilecektir. Şayet bulunmuyor ise, askeri personelin eğitim programlarına sosyal medya ve sosyal medya istihbaratı, harekât güvenliği konularının ithal edilmesi ve ders notu, broşür, web sayfası gibi eğitim materyalleri hazırlanması / dağıtılması etkili olabilecektir. Ayrıca harekât alanı ve üs bölgesi gibi yerlerden paylaşım ve canlı yayın yapılmaması, yapanlar hakkında ağır sonuçlar doğurabilecek hukuki işlem yapılması da alınabilecek tedbirler arasında yer almalıdır. Esasen sadece harekatın devam ettiği bölgelerde konuşlu birliklerden değil, askeri birliklerin tamamında fotoğraf çekilmesi, sosyal medya paylaşım yapılması yasaklanmalı, bununla ilgili hukuki mevzuat eksiği var ise giderilmelidir. Kurum ve kuruluşlar tarafından harekat güvenliğini ihlal eden paylaşımları takip etmek amacıyla takip birimleri kurulmalı, söz konusu birimler halihazırda var ise güçlendirilmelidir.

Harekât güvenliği kapsamında sosyal medya kullanımıyla ilgili olarak askeri personel tarafından alınması gereken kişisel tedbirlerin başında düşmanınıza doğrudan söylemeyeceğiniz sırrınızı sosyal medyadan da paylaşmayın ilkesini sürekli akılda tutmak gelmektedir. Sosyal medya uygulamalarının ayarlarının kontrol edilmesi, kritik bilgi içeren paylaşımların yapılmadan engellenmesi açısından önemlidir. Bir başka önlem olarak askeri personelin sosyal medya paylaşımlarını yalnızca arkadaş listesinde bulunan kişilerle sınırlaması da önemli görülmektedir.

Harekât güvenliğinin ihlali açısından en önemli hususun sosyal medya paylaşımlarıya birlikte konum paylaşılması hususu olduğu örneklerden de anlaşılmaktadır. Bu nedenle hem akıllı telefon hem de ilgili sosyal medya uygulamasının konum paylaşım özellikleri iptal edilmelidir. Cihazınıza uzaktan erişme ihtimaline karşılık cihaz ve sosyal medya hesaplarınıza ait şifrelerin sıkı sık ve zor tahmin edilecek şekilde değiştirimesi gerekmektedir.

Ayrıca akıllı telefonlarda kullanılan yürüyüş, koşu, bisiklete binmek gibi egzersiz takip programları, egzersiz yaptığınız bölgenin konum bilgilerini depoladığından kesinlikle kullanılmamalıdır. Akıllı telefonların konum özellikleri de mümkün olduğunca kapalı tutulmalıdır. Bununla birlikte askeri personelin sosyal medya hesaplarından kendilerine ve ailelerine ait kişisel bilgileri paylaşmamaları gerekmektedir. Sosyal medya hesaplarında üniformalı fotoğraflar bulundurulmamalı, birliği temsil eden işaretlere yer verilmemelidir.

Askeri personel askeri birlik giriş kartı, görev yeri ve beraber görev yaptığı arkadaşlarıyla ilgili hususları paylaşmaktan kaçınmalıdır. Görev esnasında kendinizin ya da birliğinizi kullandığı hiçbir silah, malzeme ve teçhizat sosyal medyada paylaşılmamalı, bunları kullanımına ilişkin taktik bilgiler dışarıya verilmemelidir. Düzenlenecek ya da devam eden harekâtın yeri, zamanı, kapsamı, harekât için intikale başlama tarihi gibi kritik bilginin kesinlikle sosyal medyada paylaşılmaması gerekmektedir. Sosyal medya ilr ilgili diğer bir husus tanımadığınız insanlarla sosyal medya üzerinden arkadaş olarak irtibat kurmakla ilgilidir. Nasıl sokakta gördüğünüz her insanla ilişik kurup görüşmeye çalışmıyorsanız aynı şekilde sosyal medyada gördüğünüz ancak tanımadığınız insanlarla irtibat kurmamanız önem arz etmektedir.

Son olarak özellikle TikTok isimli uygulamada asker şahıslar ve kolluk kuvvetleri mensuplarınca yapılan paylaşımlarda harekat güvenliği çerçevesinde çok daha önemli bilgiler içeren paylaşımlar olduğunu, ancak bilinçli olarak bu paylaşımların çalışma kapsamı dışında tutulduğu, örnek teşkil etmesi açısından uygun görülen ve az miktarda kritik bilgi içerdiği değerlendirilen paylaşımların çalışma kapsamına alındığını belirtmek gerekir.

Unutulmaması gereken bir diğer husus ise yaptığınız bir sosyal medya paylaşımını silseniz dahi ortadan kaldıramadığınızdır. Bu nedenle paylaşım yapmadan önce çok kez gözden geçirilmeli, içeriğinde askeri harekatı ihlal edebilecek bilgi bulunup bulunmadığı kontrol edilmelidir. Sizinle ilgili paylaşımlar yapmaması konusunda aile fertlerinin de bilgilendirilmesi oldukça önemlidir. Çalışmada yer alan sosyal medya paylaşımlarıyla ilgili olarak şu sözün sürekli tekrarlanması ve unutulmaması gerektiği değerlendirilmektedir: "*Sosyal medyada, bin kez düşün, bir kez paylaş*".

KAYNAKÇA

Army Study Guide. (2023). *An operational security (OPSEC) primer*. Erişim tarihi: 20 Aralık 2023, https://www.armystudyguide.com/content/army_board_study_guide_topics/security_and_intelligence/an-operational-security-o.shtml

Bartlett, J. ve Reynolds, L. (2015). *The state of the art 2015: a literature review of social media intelligence capabilities for counter-terrorism*. Demos.

Bejar, A. (2010). *Balancing social media with operations security (OPSEC) in the 21st Century*. Naval War College

Clark, R. M. (2013). Intelligence collection. CQ Press.

Connable, B. (2012). *Military intelligence fusion for complex operations: A new paradigm*. RAND Corporation. Erişim tarihi: 24 Kasım 2023, http://www.rand.org/pubs/occasional_papers/OP377.html.

Defence Turk [@Defence_Turk] (2019, 11 Şubat). *Yunanlı savunma sayfalarından biri Kuzey Kıbrıs Türk Cumhuriyeti'nde konuşlu üslerimizden birinde askerimizin paylaştığı fotoğraf sayesinde KKTC'ye Leopard 2A4 tanklarının sevk* [Görsel ekli] [Tweet] Twitter https://twitter.com/Defence_Turk/status/1094909046036070400

Director of National Intelligence. (2022). *OPSEC for all, protecting yourself and your critical information*, Erişim tarihi: 3 Kasım 2023, https://www.dni.gov/files/NCSC/documents/nittf/OPSEC_for_All_July2022.pdf

Erdem, A.K. (2021). *MSB'nin askerlere sosyal medyada fotoğraf paylaşmayın uyarısının ardındaki neden... İki Türk askerinin fotoğrafı Rumlara nasıl koz verdi?* Erişim tarihi: 15 Kasım 2023, https://www.indyturk.com/node/433246/haber/msbnin-askerlere-sosyal-medyada-foto%C4%9Fraf-payla%C5%9Fmay%C4%B1n-uyar%C4%B1s%C4%B1n%C4%B1n-ard%C4%B1ndaki-neden

Ergürel, D. (22 Aralık 2015). *Askeri istihbarat sosyal medyada*. Erişim tarihi: 10 Kasım 2023, https://medium.com/turkce/askeri-istihbarat-sosyal-medyada-2327f071a98d.

Erol, M.K. (2022). Açık Kaynak İstihbaratı ve Askeri İstihbarat Haşdi Şabi Örgütü Üzerinde Uygulama. Nobel Yayınevi

Eyal, P. ve Asher, T. (2015) The value of military intelligence, *Defence and Peace Economics*, 26:2, ss.179-211, DOI: 10.1080/10242694.2014.886435

Gallagher, S. (2023). *Opposite of OPSEC: Russian soldier posts selfies—from inside Ukraine. Instagram Photo Map feature shows bored Russian soldier across the border*., https://arstechnica.com/tech-policy/2014/08/opposite-of-opsec-russian-soldier-posts-selfies- from-inside-ukraine/

Gill, P. ve Phythian, M. (2018). *Intelligence in an insecure world*. New York: John Wiley & Sons.

Gudgin, P. (2000). *Military intelligence*. Sutton Publication Ltd.

Ivan, A. L., Iov, C. A., Lutai, R. C. ve Grad, M. N. (2015). Social media intelligence: opportunities and limitations. Centre for European Studies Working Papers, 7(2a): 505-510.

Johnson, L. K. (2007). *The Oxford Handbook of National Security Intelligence*. Oxford University Press

Joint Chiefs of Staff. (2013). Joint Publication 2-0: Joint Intelligence. Erişim tarihi: 10 Aralık 2023, http://www.dtic.mil/doctrine/new_pubs/jp2_0.pdf.

Ju, Y., Li, Q., Liu, H. Y., Cui, X. M., & Wang, Z. H. (2020). Study on application of open source intelligence from social media in the military. *In Journal of Physics: Conference Series* (Vol. 1507, No. 5, p. 052017). IOP Publishing. doi:10.1088/1742-6596/1507/5/052017

Kent S. (2002). Stratejik istihbarat. ASAM Yayınları.

kmando7333. [@kmndo] (2022, 20 Ağustos). [Görsel ekli] [TikTok Paylaşımı] TikTok, https://www.tiktok.com/@kmando7333/video/7133789193612037377?_r=1&_t=8ik5gh2Tbde

komando056. [@cankat] (2023, 11 Mayıs). [Görsel ekli] [TikTok Paylaşımı] TikTok https://www.tiktok.com/@komando056/video/7231861010447994118?_r=1&_t=8ik79IWP5wk

Mahood, M.E.K. (2014). Socmint: Following and liking social media intelligence. Canadian Forces College. Erişim tarihi: 08 Kasım 2023, https://www.cfc.forces.gc.ca/259/290/317/305/mahood.pdf.

Momi, R. (12 Kasım 2021). SOCMINT: Social media ıntelligence a new discipline? Erişim tarihi: 03 Kasım 2023, https://www.greydynamics.com/socmint-social-media- intelligence-a-new-discipline.

NATO (2001). *NATO Open Source Intelligence Handbook*. Brussells: North Atlantic Treaty Organisation.

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.

Omand, D. (2013). Is it time to move beyond the intelligence cycle? A UK practitioner perspective. Phythian, M. (Ed.) *Understanding the intelligence cycle* içinde (ss.136-149). Routledge.

Office of the Director of National Intelligence. (2016). *Going bright: How the internet of things could revolutionize intelligence collection and analysis*. Erişim Tarihi: 11 Kasım 2023, https://www.odni.gov/files/PE/Documents/Internet-of-Things.pdf.

Özdağ, Ü. (2015). *Açık kaynak istihbaratı*. Yılmaz, S. (Ed.) İstihbarat Bilimi. Kripto Yayınları.

Öztürk, S. [@serkanozt06] (2022, 29 Kasım). [Görsel ekli] [TikTok Paylaşımı] TikTok https://www.tiktok.com/@qruzvar/video/7304970950313938194?_r=1&_t=8ik4uJmpu4b

Rodewig, C. (8 Mart 2012). *Geotagging poses security risks*. Erişim tarihi: 27 Kasım 2023, https://www.army.mil/article/75165/geotagging_poses_security_risks.

Schogol, J. (2023). Russian soldier gave away his position with geotagged social media posts. Erişim tarihi: 10 Aralık 2023, https://taskandpurpose.com/news/russian-military-opsec-failure-ukraine

Steele, R.D. (1995). The importance of open source intelligence to the military, *International Journal of Intelligence and CounterIntelligence*, 8:4, 457-470, doi:10.1080/08850609508435298

Steele R.D. (1997). *Open source intelligence: What is it? Why is it important to the military?* Open Source Solutions, Inc.International Public Information Clearinghouse

Taha, E. [@emirhan.taha] (2023, 23 Aralık). [Görsel ekli] [TikTok Paylaşımı] TikTok https://www.tiktok.com/@emirhan.taha/video/7315736745234943238?_r=1&_t=8ik5pyUBrao

Treverton, G.F. ve Miles, R. (2014). *Social media and intelligence*. Elanders Sverige AB.

Tucker, P. (27 Ocak 2020). *Spies like AI: The future of artificial ıntelligence for the US intelligence community*. Erişim tarihi: 01 Aralık 2023, https://www.defenseone.com/technology/2020/01/spies-ai-future-artificial-intelligence-us- intelligence-community/162673.

Tudoriu, C.S. (25 Haziran 2019). Using Facebook, Twitter and other sites to combat organized crime., Erişim tarihi: 20 Aralık 2023, https://perconcordiam.com/social-media- intelligence.

Urhal, Ö. (2008). Kamu Güvenliği Açısından İstihbarat ve Örgütlü Suçlar. Adalet Yayınevi.

US Department of the Army. (2023). Field Manual 2-0 Intelligence. Erişim tarihi: 11 Aralık 2023, https://armypubs.army.mil/epubs/DR_pubs/DR_a/ARN39259-FM_2-0-000-WEB-2.pdf

US Marine Corps. (2023). Operations Security Guidance. Erişim tarihi: 20 Kasım 2023, https://www.24thmeu.marines.mil/For-the-Families/OPSEC/

Vandersmith, O. (2023). How open-source intelligence is changing warfare. Erişim tarihi: 30 Aralık 2023, https://www.usni.org/magazines/proceedings/2023/march/how-open-source-intelligence-changing-warfare

Yarkan, E. [@emirhanyarkan] (2023, 13 Haziran). [Görsel ekli] [TikTok Paylaşımı] TikTok https://www.tiktok.com/@emirhanyarkan/video/7244063291528645893?q=%C3%B6zel%20kuvvetler%20kuzey%20%C4%B1rak&t=1704472955048