ASR Journal
International Academic Social Resources Journal
Open Access Refereed E-Journal & Indexed & Puplishing
Year 2021, Vol:6, Issue:30, pp:1427-1433 E-ISSN: 2636-7637

Arrival Date : 09.10.2021
Published Date : 25.11.2021
DOI Number: 10.31569/ASRJOURNAL.312
REVIEW ARTICLE

SİBER İSTİHBARATIN GÜCÜ

THE POWER OF CYBER INTELLIGENCE

Ekrem Tuna ÖZTUNÇ
İstanbul Aydın Üniversitesi, Lisansüstü Eğitim Entitisü, Uluslararası İlişkiler ve İstihbarat İncelemeleri Anabilim Dalı, tunaoztunc@stu.aydin.edu.tr, İstanbul/Türkiye
ORCID ID: 0000-0002-9697-4250

Cite As Öztunç, E.T. (2021). "Siber İstihbaratın Gücü", International Academic Social Resources Journal, (e-ISSN: 2636-7637), Vol:6, Issue:30; pp:1427-1433

ÖZET

İstihbarat çeşitli sözlüklerde "düşünce, istihbarat, bilgi, haber, istihbarat, Hasadis, istihbarat toplama, haber alma" şeklinde geçmektedir. Ancak istihbarat açısından haber, işlenmemiş bilgiyi ifade eder. Elde edilen verilerin zeka olabilmesi için bir dizi süreçten geçmesi gerekir ve zekanın çeşitli tanımları vardır. Ülke tarafından belirlenen ihtiyaçlar. Siber istihbarat ise bir istihbarat disiplini ve bir birleştirme yöntemi olarak tanımlanmaktadır. Bu yazıda istihbarat ve siber istihbaratın gücünden bahsedilmiş, çeşitli kurum ve kuruluşlar bilgi eksikliği ve yanlış anlaşılmalar nedeniyle suistimal edilmiştir.

Anahtar Kelimeler: İstihbarat, Kamu Güvenliği, Siber İstihbarat, Siber Güvenlik, Kamu Güvenlik Politikaları, Siber Savaş

ABSTRACT

Intelligence is mentioned in various dictionaries as "thought, intelligence, information, news, intelligence, Hasadis, intelligence gathering, receiving news". But in terms of intelligence, news refers to unprocessed information. In order for the obtained data to be intelligence, it must go through a series of processes and there are various definitions of intelligence. needs determined by the country. Cyber intelligence is defined as an intelligence discipline and a unification method. In this article, the power of intelligence and cyber intelligence has been mentioned, and various institutions and organizations have been abused due to lack of information and misunderstandings.

Key words: Intelligence, Public Security, Cyber Intelligence, Cyber Security, Public Security Policies, Cyber War

1. GİRİŞ

Dünya genelinde internet kullanıcılarının artmasıyla birlikte ağa bağlanabilen cihaz sayısının artmasıyla birlikte "siber uzay" dediğimiz kavramın önemi artmaktadır. Kendi güvenliğini kontrol etme ve sağlama motivasyonu ile hareket eden insanoğlu, bu anlayışla bu amaca tam anlamıyla ulaşamayacağını anlamıştır. İnternet bilgi güvenliğinin sağlanmasında karşılaşılan sorunlar, "ağ güvenliği" gibi çalışma alanlarının ortaya çıkmasına neden olmuştur.

Zaman ve bilgi, günümüzde insanlık için en önemli argümanlardan biridir. Teknolojinin gelişmesi bilginin ömrünü kısaltmış ve artık insanlar doğru bilgiye kısa sürede ulaşma hedefini oluşturmuştur. Siber uzay, bilgi edinmek için en yaygın kullanılan yer olup, kişisel ve ulusal güvenlikle ilgili her zaman en önemli bilgi kaynağı olmuştur. Kamu güvenliği ile ilgili bilgiler korunana ve ulusal güvenliği sağlayan kurumlar arasında paylaşılıncaya kadar kullanılan altyapı sistemi kilit rol oynayacaktır.

Siber uzayın genişlemesiyle birlikte, iletişimin hızla gelişmesiyle birlikte siber uzayın askeri, siyasi ve ekonomik alanlardaki uygulaması da genişlemiştir. Siber alanda kamu güvenliğinin temelini oluşturan istihbarat faaliyetlerinin geliştirilmesi, ulusal savunma stratejilerinin bir parçası haline gelmiştir. Bu durum pek çok riski de beraberinde getirmektedir. Değerli bilgiler edinmede bir adım önde olan ülkeler, yeni bir dünya düzeni kurmada avantaj elde ediyor. Bu nedenle siber istihbarat daha da önemlidir. Çünkü her zaman olay yerinde olmayan siber istihbarat ekibi, yeni stratejilerin tanıtılması için temel oluşturan sanal ortamda kendini daha güvende hissettirmektedir.

Teknolojinin gelişmesiyle birlikte altyapı araştırmaları artmış, bu nedenle "güvenlik" kavramı önem kazanmıştır. 1970'lerde kurulan Arpanet, internet altyapısının temellerini attı ve bu süreç askeri, ulusal savunma, saldırılar, istihbarat gibi unsurlar tarafından yönetiliyor. Günümüzde giderek daha fazla sosyal medya kullanıcısı istihbarat faaliyetlerinin bu alana kaymasına neden olmuştur.

2. İSTİHBARAT KAVRAMI

15. yüzyıldan itibaren bilgi ve haber amaçlı kullanılan istihbarat, 19. yüzyılda kurumsallaşmıştır. Savaşın bir parçası olarak istihbarat, esas olarak askeri olayları ve olay bilgilerini elde etme işlevini yerine getirmektedir. Savaş dışı dönemlerde diplomatik bir araç olarak müzakerelerde de önemli bir faktördür. İstihbarat kelimesi, bilgi elde etmekten ziyade, istihbarat ve anlama gibi kavramları vurgulayan, bilginin analizini

içerir.İntelligence kelimesi haber ve bilgi almanın yanı sıra, İngilizce'deki "intelligence" kelimesi, etimolojisindeki Arapça "intelligence" kelimesinden türetilmiştir. (Özdağ, 2014). Bu nedenle istihbarat niteliğinde bilgi yapabilmek için makul bir bilimsel süreç ve analizden geçmesi gerekir.

İstihbarat amacıyla farklı araç ve yöntemlerle toplanan veriler, çeşitli ülkelerin dış politika eylemlerini desteklemeye yardımcı olabilir. II.Dünya Savaşı'ndan bu yana geleneksel yolları kullanan istihbarat araçları, son yıllarda teknolojik gelişmelerin değişmesi ve gelişmesiyle birlikte büyük değişimlere uğramıştır. Bu durumda en çok bilinen istihbarat servisi yöntemi insan zekasına dayanmaktadır. Bu yönteme ek olarak teknoloji tabanlı (sinyal zekası, ölçüm ve imza zekası (Major, 1995), jeo-uzamsal zeka ve siber zeka (Katz ve Banaski, 2018) istihbarat yöntemleri daha hızlı ve daha doğru olarak kullanılmaktadır.

En yaygın olarak kullanılan yöntem insan zekasına (HUMINT) dayanmaktadır. Kökleri antik dünyanın yöntemlerine kadar uzanabilir, II.Dünya Savaşı ve Soğuk Savaş'ın ilk günlerinde hemen hemen tüm toplumlar kritik bilgileri elde etmek, düşman eylemlerini önlemek ve dost güçlerin askeri, siyasi ve ekonomik avantajlar elde etmesine yardımcı olmak için kullanmıştır. Yabancı hedefleri, yetenekleri, güçlü yönleri, eğilimleri, taktikleri, teçhizatı ve anavatanlarını anlamak ve yaymak için bireylerden veya kurumlardan (ABD Ordusu, 2016) bilgi toplayan kişiler (casuslar) aracılığıyla kişilerarası iletişim, sorgulama, gizli fotoğrafçılık. Şirketin yetenek verileri, belgeler ve diğer materyaller aracılığıyla elde edilir. (NATO, 2008). 1950'li yıllarda yeni teknolojilerin gelişmesiyle havacılık ve uydu araçları aracılığıyla veri elde etmek kolaylaşmış ve zamanla insan temelli istihbarat yöntemlerinin etkinliği azalmıştır. Günümüzde istihbaratın teknik temeli daha etkin bir şekilde kullanılmaktadır.

Teknik zeka (TECHINT); sinyaller, fotoğraflar, uydular, radarlar ve çeşitli elektronik manyetik araçlardır (Özdağ, 2014). Bu bağlamda, karşı tarafın niyetlerini, eğilimlerini ve yeteneklerini anlamak için elektromanyetik spektrum (dalga boyu ve frekans aralığı) ve sinyal zekası kullanılır. Aslında, sinyalleri yakalayarak istihbarat toplar. Elektronik sinyalleri ifade eden iki tür sinyal zekası vardır. (USMC, 2018). Biri iletişim zekası, diğeri ise elektronik istihbarat sistemleridir. Bu nedenle iletişim zekası, aramalar, metin mesajları ve çeşitli çevrimiçi etkileşimler dahil olmak üzere bireylerin veya kuruluşların iletişiminden toplanan bilgilerdir. Bu bilgiler aktarımdaki frekans ve diğer teknik detaylar dikkate alınarak toplanır (Gökduman, 2018). Elektronik istihbarat ise doğrudan iletişimde yer almayan bilgilerin radyasyonlu radyo frekansı ve radar sistemleri aracılığıyla elde edilmesini ve gerektiğinde erken uyarı verilmesini içermektedir. Elektronik istihbarat sayesinde çeşitli ülkelerin savunması garanti altına alınmış, yabancı füzeler ve uzay araçları hakkında birçok bilgi elde edilmiştir. (Bernard, 2009).

Ölçme ve Karakteristik Zekada (MIGINT), belirli tekniklerin (metrik, açı, uzay, dalga boyu, zaman korelasyonu, modülasyon, plazma ve hidromanyetizma) kullanılmasıyla elde edilen verilerin bilimsel ve nitel analizi, herhangi bir belirgin özelliği tanımlamak için kullanılır. Teknik istihbarat bilgileri ifade edilir. Bu nedenle manyetik bilgi, yabancı nükleer, kimyasal ve biyolojik özellikler, yayılan nükleer enerji, termal enerji ve elektromanyetik enerji, yansıyan veya yeniden düzenlenmiş radyo dalgaları, ışık ve ses doğrultusunda elde edilir. Ayrıca gizli yeraltı tesisleri, keşfedilmesi zor kimyasal ve biyolojik savaş bölgelerindeki gözetleme faaliyetleri gibi devletin elini güçlendirme yeteneğine de sahiptir (Seng, 2007).

İnsan temelli istihbarat yöntemleri ile kullanılan teknik istihbaratta, çeşitli tehditler ve yabancı askeri teçhizat hakkında bilgiler toplanarak analiz edilmektedir. Küreselleşen bir dünyada, çeşitli zeka biçimleri ve teknolojileri, hızlandırılmış iletişim teknolojileri ve çeşitli bilgi işlem ve ölçüm cihazları tarafından desteklenmektedir. Gizli belgeleri çekmek ve filmi gizlemek için minyatür bir kamera ve mikrofilm kullanmak daha kolay hale gelmiştir. Uyduların casusluk amacıyla kullanılması, gizli askeri tesislerin tespiti gibi araştırmaları bu şekilde gerçekleştirir. Gizlilik gerektiren bu süreçte kablo kullanmadan telefon dinleme, kapalı ortamda veri sağlamak için elektronik dinleme ve kayıt cihazları kullanma, karanlıkta fotoğraf çekme imkanı sağlanmaktadır. (Fidan, 1999). Bu nedenle günümüz görüntüleri coğrafi bilgilerle eşleştirilmekte ve uydu, uçak, insansız hava araçları gibi teknik araçlarla konumsal veriler elde edilmektedir. Bu durumda coğrafi yöntemler de istatistiksel verilerin elde edilmesinde etkilidir (haritalama ve ölçme teknikleri, haritacılık, jeodezi gibi). (Cardillo, 2018)

Bu nedenle istihbarat departmanı amacına göre çeşitli yöntemler kullanır. Bu yöntemlerle elde edilen veriler, olayların değişikliklerine veya geçişlerine kıyasla esneklik sağlayabilen sonuçları bir araya getirir. Yani sadece mevcut tehditleri değil, fırsatları da değerlendirip geleceği şekillendirmek için bilgiyi doğru analiz etmek ve amacına göre kullanmak gerekir. Bu bağlamda, sürekli yenilik gerektiren istihbarat, gazeteler, dergiler, konuşmalar, radyo istasyonları, sosyal ağ siteleri ve hükümet raporları gibi kamuya açık bilgi kaynaklarını da kullanır.

İstihbarat yöntemleri dijitalleşme ile çeşitlenmiş olsa da kapsamları, kapsamları ve etkileri de genişlemektedir. Bu bağlamda haber ve bilgi kurumları, kültürel diplomatik alışverişler ve sosyalleşme yoluyla elde edilen bilgiler çoğu zaman motive edilse de internet ve bilgi ve iletişim teknolojilerine dayalı olarak daha çok izleyiciyi etkilemektedir. Bilginin sayısallaştırılması ağ zekası kavramını literatüre katmaktadır (Ünver, 2018). Dijital bilgilerin ağ alanında keşfedilmesiyle birlikte geleneksel istihbarat yöntemlerini aşan hız, doğruluk ve doğruluk ilkeleri ağ alanına aktarılmıştır.

3. SİBER İSTİHBARAT KAVRAMI

Her kelimenin ilk Siber istihbarat veya siber casusluk, hedefin bilgisi ve rızası olmadan ağların, bilgisayarların ve diğer ekipmanların siber uzaya girmesidir. Teknoloji penetrasyonunun kullanımı, hassas verilerin toplanması ve istihbarat çarkından geçirilmesi faaliyetidir. Ağ istihbaratı sadece teknik faaliyetlerle değil, aynı zamanda sosyal mühendislik, psikolojik savaş ve diğer unsurlarla da oluşturulabilir. Hedef kuruluşta çalışan personel, Truva atları, casus yazılımlar, virüsler ve diğer zararlı yazılımları sızdırmak veya dizüstü bilgisayarları, harici diskleri, sabit diskleri vb. çalmak için sisteme fiziksel olarak girmektedir.

Siber uzay, casusluk yöntemlerinin ("ticaret araçları" olarak ifade edilir) farklı şekillerde kullanılabildiği bir alan haline gelmiştir. Ayrıca internetin casusluğun en kullanışlı alanı olduğuna da dikkat çekilmiştir. (Wettering, 2001) Casusluk, yani casusluk, esas olarak devlete karşı gizli yollarla gizli bilgilerin elde edilmesi faaliyetidir. Ulusal veya stratejik ve askeri kurumların arşiv ve veri tabanlarındaki bilgileri "hack" ve diğer yöntemlerle ele geçirmek için internet altyapısını kullanmak mümkündür. Gerekli önlemler alınmadığı takdirde, geleneksel istihbarat yöntemlerine göre hassas verilere ağ üzerinden erişim, istihbarat amaçlı kullanılması ve karar vericilere gönderilmesi daha hızlı ve daha düşük bütçelidir. Günümüzde siber uzaya bağlı her kullanıcının nerede olduğu, kiminle konuştuğu, ne hakkında konuştuğu, arkadaşları ve akrabaları, son planları ve birçok çevrimiçi davranışı hakkında bilgi edinmek mümkündür.

Gerekli önlemler alınmazsa ağ üzerinden hassas verilere erişmek, istihbarat amaçlı kullanmak ve karar vericilere göndermek geleneksel istihbarat yöntemlerine göre daha hızlı ve ucuzdur. Günümüzde siber uzaya bağlanan her kullanıcının nerede olduğunu, kiminle konuştuğunu, ne hakkında konuştuğunu, arkadaş ve akrabalarını, son planlarını ve birçok çevrimiçi davranışını anlamak mümkündür.

Yakın gelecekte, siber saldırılar uluslararası ilişkilerde giderek daha önemli bir rol oynarken, insanlar siyasi misilleme ve diğer adımlar bağlamında saldırganın kim olduğunu anlamanın temel bir sorun oluşturacağına inanılmkatadır. Kimliği hakkında yanıltıcı ipuçları bırakan suçluların kimliklerinin aranması durumunda artması beklenmektedir. Uzmanlar tarafından tartışılan bir diğer önemli konu ise kritik altyapı ve üretim sistemlerinin özellikle jeopolitik gerilim dönemlerinde saldırganların dikkatini çekmeye devam edeceği, ayrıca, mobil cihazları hedefleyen güvenlik sektörünün, adli analiz için mobil operasyon isteklerine tam olarak erişmenin zor olması gerçeğinden yararlanacak daha fazla casusluk faaliyeti ile karşı karşıya kalacağı tahmin edilmektedir.

4. İSTİHBARATIN SINIFLANDIRILMASI

Farklı akademik çevreler ve özel kurumlar bazı yönlerden farklı istihbarat sınıflandırmalarına sahip olsalar da genel olarak belli bir sınıflandırmanın olduğu söylenebilir. İstihbarat, ulusal güç hedeflerine, toplama tekniklerine ve ölçeğe göre sınıflandırılır (Özdağ, 2013).

Alanlarına göre istihbaratlar şu şekildedir;

- ✓ Siyasi İstihbarat
- ✓ Askeri İstihbarat
- ✓ Ekonomik İstihbarat
- ✓ Sosyal İstihbarat
- ✓ Coğrafi İstihbarat
- ✓ Biyografik İstihbarat
- ✓ Ulaşım ve İletişim İstihbarat
- ✓ Bilimsel ve Teknik İstihbarat
- ✓ Siber İstihbarat ve Enformanson İstihbaratı

Strateji, taktik ve muharebe istihbaratını içeren bu alanlarda ağ istihbaratı; ekipman, kablolar, enerji üreticileri, internet servis sağlayıcıları, sunucular vb. siber uzayda hedef ülkenin altyapısını oluşturmaktadır. Teknokratlar, siber saldırılara, siber istihbarat faaliyetlerine veya siber savunmalara katılarak görevlerinin özellikleri (nitelik ve nicelik gibi) hakkında bilgi edinerek bunları değerlendireceklerdir.

Bu tanımdan, siber istihbarat araştırmasının bilgi toplama amaçlı hedeflere veya faaliyetlere yönelik siber saldırılar öncesinde yapılması gerektiği anlaşılmaktadır. Bir istihbarat disiplini olarak kabul edilen ağ istihbaratı, istihbarat toplama yöntemi olarak da kullanılmaktadır.

Toplama yöntemlerine göre ise istihbaratı şu şekilde sınıflandırmak mümkündür;

- ✓ İnsana Dayalı İstihbarat (HUMINT)
- ✓ Sinyta İstihbarat (SIGINT)
- ✓ Radar İstihbaratı (RADINT)
- ✓ Elektronik İstihbaratı (ELINT)
- ✓ Haberleşme İstihbaratı (COMINT)
- ✓ Görüntülü İstihbarat (IMINT)
- ✓ Açık Kaynaklı İstihbarat (OSINT)
- ✓ Siber İstihbarat (CYBINT)

Yukarıdaki toplama yöntemlerinden daha fazla yöntem vardır ve bazıları alt sınıfları olduğu için listede listelenmez. Ancak genel olarak istihbarat toplama yöntemleri bu şekilde sınıflandırılabilir. Görüldüğü gibi siber istihbarat artık bir istihbarat toplama yöntemidir.

5. İSTİHBARATIN TEMEL İLKELERİ

Bir disiplinde yürütülen faaliyetler sonucunda toplanan bilgiler değerli olmalıdır. Bilgi, orijinal haliyle genellikle anlamsızdır. Yüzyıllar boyunca insan zekanın öznesi olmuştur. Teknolojinin gelişmesi, bilgi toplama yöntemlerinin gelişmesi ve alternatiflerin oluşturulması ile birlikte istihbarat çalışmalarının belirli ilkeler çerçevesinde yürütülmesi gerekmektedir. Bu ilkeler şunlardır:

Kesinlik İlkesi, Elde edilen bilgiler doğru olmalıdır. Olasılıklar çerçevesinde önerilen politikaların önceliği net olarak tanımlanmalıdır. "Belki" ve "hipotez" gibi muğlak ifadeler, ülkeleri güvenliklerini sağlama konusunda tereddüte düşürüyor. Bu, istihbarat tarafından oluşturulan eylem mekanizmasını devre dışı bırakabilir. Hazırlanan raporda elde edilen bilgilerin gerçekleşme olasılığı belirtilmelidir.

Doğruluk İlkesi, İstihbarat araştırması kaçınılmaz olarak başarısız olacak ve doğruluğu teyit edilemeyecek, bu da önlemlerde gecikmelere neden olacaktır. Bunun için başlangıç noktası, elde edilen bilgilerin doğru olması gerektiğini hatırlamaktır. "Ulusal İstihbarat Kursu (NIC) Ders Kitabı, Müşterek Askeri İstihbarat Eğitim Merkezi 1999", ABD Askeri İstihbarat Kursu'nun kurs eğitmeni, "sahte istihbarat, istihbarat olmamasından daha kötüdür." Bilgi ile başlar. (Özdağ,2009)

Hızlı İstihbarat İlkesi, Elde edilen bilgilerin bir an önce ilgili birimlere iletilmesini gerektirir. Hızlı veri akışı, eylem mekanizmasından sorumlu birimlere uygun politikaları formüle etmek için yeterli zaman vermelidir. Bilginin hızlı aktarımı, kararların her zaman doğru olacağını garanti edememektedir. Bu nedenle karar alma mekanizmasını yöneten kişinin durumu doğru analiz etmesi gerekir. (Dearth, Goodden,1995).

6. İSTİHBARATIN YÖNTEMLERİ

Devletin varlığını sürdürmesinde istihbarat kavramının önemi, bu eylemin farklı şekillerde gerçekleşmesine neden olmuştur. Özellikle çeşitli ülkeler tarafından kullanılan farklı yöntemler, kamuya açık ve gizli bilgi toplama yöntemlerini de ortaya çıkarmaktadır. Ülkeler, uluslararası sahnede hareketliliklerini artırarak ve istihbarat kaynaklarını hızlı ve doğru bir şekilde kullanarak savaş alanı avantajlarını artırmayı umut etmektedirler. İstihbarat toplayan ve bu verileri analiz edebilen bir birimin olası sorunları çözmede büyük başarılar elde etmesi beklenmektedir. İstihbarat yöntemlerinden tam anlamıyla yararlanmak ve bu kaynakları etkin bir şekilde yönlendirmek başarılı operasyonlar yaratabilir. İstihbarat kaynakları, mevcut durumun detaylı analizi yoluyla bilgiyi gerçekleştiren, anlayan, kaydeden ve paylaşan sistem ve araçlardır. Sekiz ana istihbarat kaynağı vardır. İnsan Zekası (HUMINT), Sinyal İstihbaratı (SIGINT), Görüntü İstihbaratı (IMINT), Ölçüm ve Sinyal İstihbaratı (MASINT), Açık Kaynak İstihbaratı (OSINT), Teknik İstihbarat

(TECHINT), Karşı İstihbarat (CI) ve Kasıtsız Yayın İstihbaratı (RANT)) (Schleher, 2004) Bu kaynakların en önemlisi insan zekasıdır.

HUMINT konseptinin merkezindeki insanlar aslında zekaya ihtiyaç duyan insanlardır. Bu bakımdan "kişi" en önemli istihbarat aracıdır.Olayları gözlemler ve analiz eder, bilgi toplar ve bu bilgiyi değerli kılmaktadır. Temel argümanı insan olan HUMINT, bilinen en eski ve en ucuz yöntemdir ve zekanın başarısı için ana faktördür. Bilgi toplayan, bilgi ve olayların kaynağı ile doğrudan etkileşime giren ve kendini zekanın merkezinde bulan kişidir.Yetenekleri, tutum ve davranışların proaktif kullanımını ve algı yönetimini içerir. İnsanları istihbarat kaynağı olarak kullanan bu yapıya "casus" denir. Karar karşıtı sisteme girerken ve sistemin zayıf yönlerini anlarken stratejik istihbarat kavramını dikkate alınmaktadır.

Bu istihbarat faaliyetine dahil olanlar personel, casus ve ajan gibi isimler alacaklar. Hemen her sistemde insan faktörünün önündeki en büyük engel olarak yanlış bilgi aktarımı ve çifte yayın yapma ihtimali her zaman göz önünde bulundurulmalıdır. Ülke için elçilik HUMINT'in kaynağıdır ve bunu herkes bilmektedir. Bu nedenle ilgili ülkeler, elçilik personelinin niteliklerine ve güvenliğine öncelik vermelidir. Bugünkü duruma bakıldığında herhangi bir ülkede faaliyet gösteren sivil toplum kuruluşu gibi görünen düşünce kuruluşlarının da bilgi kaynağı olarak kullanıldığı görülmektedir. İnsan zekasını etkin bir şekilde kullanabilmek için organizasyonun sisteme düzgün bir şekilde nüfuz etmesi gerekir. Toplumsal ve ulusal teşkilat yapıları, sivil ve askeri bürokrasiler, öğrenci grupları ve sivil toplum kuruluşları arasında istihbarat ağları oluşturulmalıdır. Teknik alet ve ekipmanlardaki artışa rağmen HUMINT, seçeneği olmayan önemli bir kaynaktır.

Zekanın en önemli yönü, elde edilen bilgilerin "ilgili" özelliğidir. Ülkeyi yönetenlerin karşılaşacakları potansiyel tehditler ve fırsatlar hakkında bir vizyona sahip olmaları gerekir. Tehditler, askeri anlamda her zaman sıcak noktalar anlamına gelmez. İstihbarat birimleri genellikle "Cassandra kompleksi" ve siyasi ve askeri operasyonların karar vericileri ile karşı karşıyadır. Kassandra kompleksi, karar vericinin görüşlere karşı çıkması ve önyargılarına uymayan bilgi ve istihbaratı kabul etmekte tereddüt etmesidir. Bu iki konu istihbarat ve devlet ilişkisinde en önemli konulardan biridir (Özdağ,2009).

7. SİBER İSTİHBARAT TOPLAMA TEKNİKLERİ

Siber zeka bir yöntem olarak sınıflandırılsa da temel olarak güvenlik (akıllı) algısı ve akıllı (güvenlik) uygulamaları olarak ikiye ayrılabilir. Güvenlik duygusu tamamen psikolojik algıya dayanmaktadır. İstihbarat örgütleri gizli bilgileri bir tür psikolojik savaşın, yani topluma propagandalarının temelini oluşturmak için kullanırlar. Ülkenin koruma politikalarıyla güveni yönetirler. Bu yöntem özellikle Ortadoğu ve diğer inanç merkezleri olan bölgelerde etkili olup, bir nevi toplum mühendisliğidir. Psikolojik olarak hazırlanmış hedef topluluklar siber savaşta kullanılabilir. Toplanan bilgilere dayalı olarak siber saldırıların geçici veya kalıcı olarak devre dışı bırakılması, siber ortamda oluşturulan siber terör ortamında siber savaş yoluyla gerçekleştirilebilir.

Yaygın olarak kullanılan siber istihbarat yöntemleri:

- ✓ Siber Elektronik İstihbarat
- ✓ Siber Açık Kaynak İstihbaratı
- ✓ Sosyal Ağlara Dayalı Siber İstihbarat

7.1. Siber Elektronik İstihbarat

Siber Elektronik İstihbarat, kullanıcının gizli oturum açma bilgilerini içerir ve bilgisayar yazılımı müdahale etmeden sistem zayıflıklarından yararlanmayı kolaylaştırır. Burada Ulusal Güvenlik Ajansı (NSA) ve NSA kısaltması yer almaktadır. Daha sonra ABD istihbarat teşkilatı Microsoft ile işbirliği yapılarak küresel iletişimde bilgi akışı izlenerek yazılım geliştirildi. Bu nedenle Rusya, Çin ve diğer ülkeler Microsoft ürünlerini kullanmak için önlemler almıştırPROMIS, ABD savcıları için hazırlanmış bir program olan Gizli Bilgi Toplama adlı popüler bir bilgisayar yazılımıdır (Bayraktar,2015). ABD Merkezi İstihbarat Teşkilatı'nın 1990'da kullanımını açıklamasının ardından, Kanada ve İsrail'deki gizli teşkilatların da kullandığı ortaya çıkmıştır. 2000'li yıllarda ABD istihbarat teşkilatları tarafından "arka kapı" olarak yerleştirildiği ve Türkiye gibi ülkelere satıldığı bilgisi kamuoyunun kafasını karıştırmaya yetmiştr. Çünkü bu arka kapı sayesinde hain ajanların ve finans kuruluşlarının bilgileri Merkezi İstihbarat Teşkilatı ve Milli Güvenlik Teşkilatı'na iletilmiştir. "Echelon", küresel bir bilgi toplama sistemi olduğu için PROMIS gibidir. Kurulduğu günden bu yana neredeyse tüm küresel iletişim kanallarını dinleme yeteneğine sahiptir. Dinlemek için iki yöntem kullanılmaktadır. Birincisi, üye ülkelere ait uydular aracılığıyla mikrodalga sinyallerini yakalama yeteneği,

ikincisi ise okyanus ötesi kabloları dinlemek. Sözcük içeren konuşmaları yakalar, ardından izler ve izler ve istihbarat teşkilatlarına rapor etmektedir.

7.2. Siber Açık Kaynak İstihbaratı

İnternet kullanıcıları çevrim içi dünyada hareket ettiklerinde gittikleri her yerde iz bırakımaktadır. Örneğin haber sitelerine yaptığı yorumlardan siyasi görüş ve inançlarına kadar pek çok önemli bilgiye öngörüyle ulaşılabiliyor. Açık kaynak istihbarat, kamuya açık kaynaklardan bilgilere erişerek istihbarat bilgilerinin ortaya çıkarılması ve elde edilen bilgilerin analiz edilmesi olarak tanımlanmaktadır. Açık kaynak istihbarat toplama yöntemi, ağ ortamının hızla genişlemesi ile üretilen geleneksel istihbarat toplama yöntemlerinden yazılı ve görsel medya kaynaklarından biridir. Açık bir istihbarat kaynağı, hedefin ekonomik değeri hakkında yaygın olarak bulunan bilgi ve verileri içerebilir. Gri kaynaklar olarak adlandırılan kaynaklar, akademinin, devlet kurumlarının ve özel sektör birimlerinin bilgiye sınırlı erişimi ve sınırlı sayıda kopyası olan kaynakları ifade etmektedir.

Medya, gazete, dergi, radyo, televizyon ve bilgisayar gibi kaynakları içerir. Herkese açık yüksek tanımlı görüntüler (Google Earth gibi) açık kaynak istihbaratı için çok önemlidir. Akademik araştırmalar sonucunda elde edilen verilerde sahada kullanılan yöntemdir. Yasadışı faaliyet gösteren kuruluşların da açık kaynak istihbarat unsurlarını kullandığını görülmektedir.

Açık ağ istihbarat toplama yöntemlerinin etkisinden kaçınmak için, sanal ortamlar başta olmak üzere kişisel bilgilerin gizlilik ilkelerine uyulmalıdır. İnternette paylaşılan kişisel bilgilere izinsiz erişilebileceği düşüncesi çerçevesinde ağ güvenlik politikaları oluşturulmalıdır. Açık kaynak istihbaratı, eyaletlerdeki politika yapıcılara rehberlik etmenin yanı sıra, hükümet politikalarına kamu desteği sağlamak için siyasi güç tarafından da kullanılabilir.

7.3. Sosyal Ağlara Dayalı Siber İstihbarat

Sosyal mühendislik, sosyal ağlara dayalı ağ zekasının temelidir. Sosyal mühendislik; "insanların en zayıf yaratıklar olduğu" varsayımıyla hareket etmek için insan merkezinin zayıflıklarını kullanmaktadır. Sosyal mühendislik, ağ zekasının özüdür. Gizli bilgilere erişim amacını ortaya çıkarmak için insanları ve toplum eğilimlerini ve sosyal ağları kullanmaktadır. Sosyal ağlar, kitle hareketini ve bilgi akışını ateşlemede önemlidir. Sosyal medya kullanılarak organize edilen topluluklar, popüler sporların çıkış noktası olabilir. Bu nedenle istihbarat örgütlerinin faaliyet gösterdikleri ülkelerde/bölgelerde bu siber istihbarat yöntemini yoğun olarak kullanmaları beklenmektedir. 2010 yılında Arap dünyasında meydana gelen Arap Baharı, özünde bir kitle hareketiydir.

8. TÜRKİYE'NİN SİBER İSTİHBARAT VE SİBER GÜVENLİK MEVZUATI

Ne yazık ki ülkemin ulusal bilgi güvenliğinin korunmasına yönelik araştırmaları, ağ güvenliği ve istihbarat bilgi kullanımı alanlarında birçok konuda taslağı geçemiyor. Bu yasal dayanak eksikliği, siber istihbarat araştırmalarında ve siber saldırılarda koordinasyon sorunlarına yol açabilmektedir. 14 Aralık 2015 tarihinde dünyanın en tehlikeli hacker gruplarından Anonymous tarafından gerçekleştirilen siber saldırıda, ".tr" uzantılı web sitesine yaklaşık 15 gün süreyle erişim engellenmiştir. Saldırı yıkıma yol açmaktan çok işgal şeklinde gerçekleştirilmiş olsa da saldırıya verilen yanıt ilginç olmuştur. Türkiye, sözde DDoS saldırısı nedeniyle saldırıya sadece kapı olarak modelleyebileceğimiz yapıyı kapatmıştır. Saldırılara karşı önleyici tedbirler alınırken formüle edilemeyen politikalar öngörülemeyen zararlara neden olabilir. Saldırının süresine göre ekonomik kaybı hesaplamak kolay değildir. Ayrıca ulusal platformda prestij kaybetmek uzun zaman almaktadır.

9. SONUÇ ve ÖNERİLER

Siber uzayın gelişmesiyle birlikte insanlar bu alana giderek daha fazla güvenmektdir. Toplumun çoğunluğunun bu alana katılmasıyla birlikte, bu dünyanın güvenliği büyük bir sorun haline gelmiştir. Ulusal güvenlik, dünyadaki tüm ülkelerin karşı karşıya olduğu önemli bir sorundur. Amerika Birleşik Devletleri ve Rusya gibi ülkeler dünyada olup bitenlerin farkında olup, ulusal çıkarlarıyla çatıştıkları durumlarda içgüdüsel olarak müdahale etmekte ve oluşturdukları siber uzayı bu alanda bir söz olsun diye şekillendirmeye çalışmaktadırlar. ABD'nin 44. Başkanı Barack Obama, 21. yüzyılda ülkesinin zenginliğinin ağ güvenliğine bağlı olduğunu bunun en iyi kanıtı olduğunu söyledi. Siber alanda söz sahibi olan ülkeler, bu alanda yapacakları istihbarat araştırmaları ile savunma ve saldırı stratejilerini belirleyeceklerdir.

Bu noktada Türkiye'deki yerlere bakarsak siber istihbarat kavramının henüz yeni bir kavram olduğunu görmekteyiz. Türkiye gibi gelişmekte olan bir sermayeye sahip bir ülkede siber istihbarat araştırmaları, milli güvenlik politikalarını desteklemek üzere tasarlanmış donanım ve yazılımlar sağlamış, müreffeh ve barışçıl bir ortam yaratabilecek her yönüyle milliyet üretmiştir. Birincisi, kamu kurum ve kuruluşlarındaki siber olaylara müdahale ekiplerinin sayısını artırmak ve siber güvenlik mevzuatının oluşturulmasını hızlandırmak. "İyi insanlar da kötü insanlar kadar kötü bilgiye sahip olmalıdır." Felsefesi ile siber güvenlik alanında edindiği bilgileri iyi bir şekilde kullanan uzmanların sayısını artırmak gerekmektedir.

KAYNAKÇA

Bayraktar, G.(2015). "Siber Savaş ve Ulusal Güvenlik Stratejisi", Yeni Yüzyıl Yayınları, İstanbul, s. 64

Cardillo, R. (2018). "Geospatıal-Intellıgence (Geoınt) Basıc Doctrıne", Natıonal System For Geospatial Intelligence, Publication 1.0, s. 18-142

Dearth Douglas H. & Goodden R. Thomas (ed.), (1995).Strategic Intelligence:Theory and Application, Washington, Defence Intelligence Agency, Washington D.C..

Fidan, H. (1999). "Intelligence and foreign policy; A comparison of British, American and Turkish intelligence systems", Yayımlanmamış yüksek lisans tezi, Bilkent Universitesi Ekonomi ve Sosyal Bilimler Enstitüsü Uluslararası İlişkiler Anabilim Dalı

Gökduman, M.(2018). "Sinyal İstihbaratı", Rapor, Ankara, Teknolojik Düşünce Merkezi Analizi, Ankara.

Katz, R &. Banaski, J.(2018). Essentials of Public Health Preparedness and Emergency Management, Burlington, Jones & Bartleed.

Major, G, J. (1995). The Nature of Future: Intelligence Organizations:, Kansas, School of Advanced Mılıtary Studıes Monograph Approval.

North Atlantıc Treaty Organızatıon (NATO) (2008).Standardızatıon Agency (NSA). Nato Glossary of Terms and Definitions.

Özdağ, Ü. (2013).İstihbarat teorisi, 7.Naskı, Kripto Kitapları.

Özdağ,Ü. (2004). İstihbarat Teorisi, Ankara, Kripto Yayınları.

Özdağ,Ü.,(2009). "Devlet Ve istihbarat", Beykent Üniversitesi Stratejik Araştırmalar Dergisi, 2009, 33-50.

Richard L. Bernard. (2009). Electronic Intelligence (ELINT) at NSA, Cryptologic History National Security Agency, USA.

Schleher, D. C.,(2004). "Bilgi Çağında Elektronik Harp", Doruk Yayınları, s.32

Seng,A.,C., (2007). "MASINT: "The Intelligence of the Future", DSTA Horizons, s. 108-120.

United States Marine Corps (USMC) ,(2018). Signals Intelligence, Washington, Department of The Navy.

Ünver, A. (2018). Digital Open Source Intelligence and International Security: A Primer, EDAM Cyber Governance and Digital Democracy.

Wetterıng,Frederick L., (2001).The Interner and the Spy Business,International Journal of Intelligence and CounterIntelligence, 14;342.