Siber İstihbarat Tanımı ve Faaliyet Alanı

Atalay KELEŞTEMUR*

Öz

İstihbarat, çeşitli sözlüklerde "akıl, zeka, malumat, haber, bilgi, havadis, bilgi toplama, haber alma" şeklinde yer almaktadır. Ancak istihbarat terminolojisinde haber, işlenmemiş bilgiyi ifade etmektedir. Elde edilen verinin, istihbarat olabilmesi için bir takım işlemlerden geçmesi gerekmektedir. İstihbarat hakkında çeşitli tanımlar yapılmıştır. İstihbarat, devlet tarafından belirlenen ihtiyaçlara karşılık olarak, çeşitli kaynaklardan derlenen haber, bilgi ve dokümanların işlenmesi sonucu elde edilen üründür. Siber İstihbarat ise hem bir istihbarat disiplini, hem de bir toplama yöntemi olarak tanımlanmaktadır. Bu makalede, istihbaratın ve siber istihbaratın ne olduğuna değinilmekte, çeşitli kişi ve kurumların bilgi eksikliği, kavram hatası veya kasıtlı olarak yanlış kullandığına dikkat çekilmektedir.

Anahtar Kelimeler: İstihbarat, Siber İstihbarat, İstihbarat Toplama Yöntemleri, Siber Uzay, Gizli Servisler, İnternet

Definition and Scope of Cyber Intelligence

Abstract

Espionage (intelligence) takes part in some dictionaries as "intelligence, information, knowledge, news, gathering information, receiving news". But in the intelligence terminology, news states raw information. The gathered data should undergo a set of processes to be intelligence. There are several definitions of intelligence. Simply; intelligence is a product of news, information and documents which are processed in return of the requirements of government. Cyber Intelligence is one of an intelligence discipline as well as a gathering method. In this article it is covered what is intelligence and cyber intelligence. It is also attracted to misuse of intelligence notion by some people and organizations because of lack of knowledge or on purpose.

Keywords: Intelligence, Espionage, Cyber Intelligence, Intelligence Gathering Methods, Cyber Space, Secret Services, Internet

Giriş

İstihbarat, gizli ve açık faaliyetler sonucu elde edilen verilerin, bir takım işlemlerden geçmesi sonucu müşterilere (genellikle siyasi karar alıcılar) sunulan işlenmiş bilgilerdir. Gizli faaliyetlerin kimi zaman doğrudan gerçeği yansıtarak, kimi zamansa abartılı olarak romanlarda ve sinema filmlerinde işlenmesi, istihbarata olan ilginin artmasına sebep olmaktadır. Bunun neticesi olarak, bilgiye erişmek, veriye ulaşmak ve haber toplamak gibi faaliyetler, bazı kimseler tarafından istihbarat elde etmek şeklinde adlandırılmaktadır. Oysa ki istihbarat, tanım ve işlev olarak çok daha farklı ve geniş kapsamlı bir faaliyetler bütünüdür. Bugün artık bir bilim dalı olarak kabul edilen istihbarat, siber uzay üzerinden de oluşturulabilmektedir. Siber istihbarat, günümüzde bir istihbarat disiplini ve istihbarat toplama yöntemi olarak ele alınmaktadır. Bu makalede istihbaratın ve siber istihbaratın ne olduğu anlatılmakta, kavramın ne gibi sebeplerle, nasıl yanlış kullanıldığına değinilmektedir.

İstihbaratın Tanımı

İstihbarat, yüzyıllardır gizemini korumakta olan, bunun neticesi olarak da insanların ilgisini çekmeye devam eden bir nosyondur. Her ne kadar ilgi çekse de yanlış anlaşılma, yanlış bilinme, yanlış tanımlama vb. sebeplerden ötürü ne yazık ki Türk toplumu yıllardır istihbarattan uzak durmakta ve bunun neticesi olarak da istihbarat disiplini yeterince oluşamamaktadır.

Oysaki istihbarat, haber alma teknolojilerinden, kriptolojiye, yabancı dil uzmanlığından, psikolojiye kadar birçok müspet ilmi kapsamaktadır. Oldukça geniş bir çalışma/faaliyet alanına sahip olan istihbarat, dışarıdan gözlemleyen kimselerin hayal ettiğinden çok daha büyük bir bilgi akışına ev sahipliği yapmaktadır. Bu anlamda istihbarata bir bilim dalı olarak, gerekli önemin verilmesi ve istihbarata akademik açıdan bakılması, incelenmesi gerekmektedir. İstihbaratın ne olduğunu irdelemeden önce, istihbarat kelimesinin anlamına ve bu konuda yapılmış tanımlara bakmakta fayda bulunmaktadır.

İstihbarat, çeşitli sözlüklerde “akıl, zeka, malumat, haber, bilgi, havadis, bilgi toplama, haber alma” şeklinde yer almaktadır. Arapça istihbar, haber, bilgi alma kelimesinin çoğulu olan istihbarat, İngilizce ve Fransızca’da ise “intelligence” yani “akıl, zeka” şeklinde ifade edilmektedir. Türkçe’de sözlük anlamı “Yeni öğrenilen bilgiler, haberler, duyumlar” ve “Bilgi toplama, haber alma” şeklindedir.[1]

Görüldüğü üzere, farklı dillerde istihbaratın kökeni akıl ve zekaya dayanmaktayken, Türkçe'de haber toplamaya dayanmaktadır. Ancak istihbaratı kısaca tanımlayacak olursak, "toplanan haberin, akıl ve zeka yardımıyla işlenmesi faaliyeti" olarak ifade etmek mümkündür. Bu basit tanımdan yola çıkarak, istihbarat hakkında yapılmış farklı tanımları incelemek daha kolay olacaktır.

ABD Genel Kurmay Başkanlığı Askeri Terimler Sözlüğü'nde "Yabancı devletler, düşman ya da potansiyel düşman kuvvetler, öğeler ya da mevcut/potansiyel operasyon bölgeleri hakkında toplama, işleme, bütünleşme, değerlendirme, analiz ve yorumlama işlemlerinden geçen bilgilerin, üretilmesi safhasıdır" şeklinde ifade edilmektedir.[2]

CIA ise basitçe "İstihbarat, etrafımızdakilerle ilgili politika yapıcıların karar vermelerini kolaylaştıracak bilgi ve önbilgidir" şeklinde tanımlamaktadır.[3]

Bir başka ABD gizli servisi FBI'ın resmi sitesinde ise istihbarat, "Politika yapıcıların ulus güvenliğini tehdit eden unsurlara karşı doğru karar vermeleri için gerekli olan analiz edilmiş bilgidir" yazmaktadır.[4]

Michael Warner'a göre istihbarat "Güvenilir kaynaklara dayanan ve etkili yöntemlerle, devlet görevlileri tarafından, devlet için toplanan, yabancıların üzerine odaklanan -genellikle diğer devletler, bazen de yabancı şahıslar, şirketler, vb. bilginin üretilmesi ve dağıtılması ile ilgili olan süreçtir".[5]

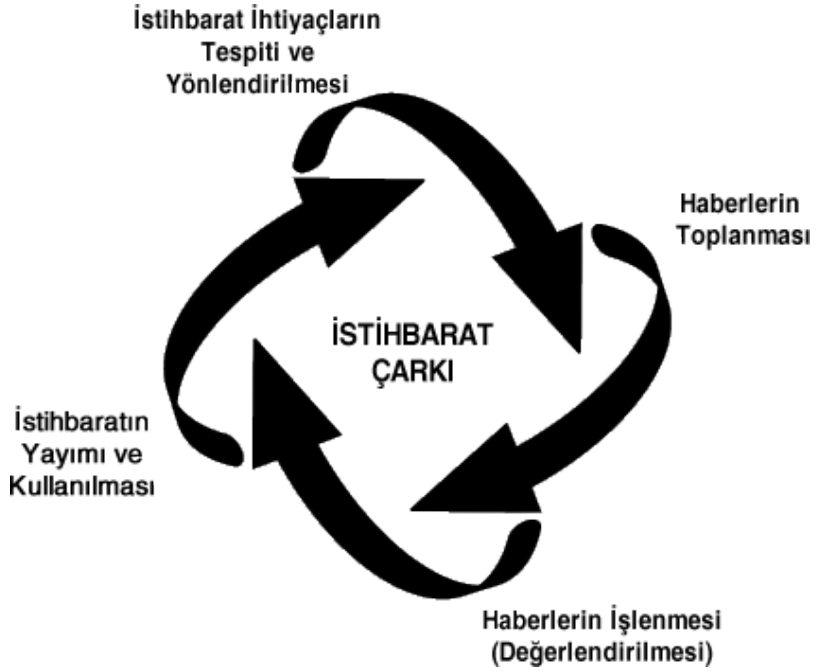
Görüldüğü üzere istihbarat kelimesinin Türkçe'de sözlük anlamı haber alma olarak geçmesine karşın, istihbarat terminolojisinde haber, sadece işlenmemiş bilgiyi ifade etmektedir. İstihbarat ise devlet tarafından belirlenen ihtiyaçlara karşılık olarak, çeşitli kaynaklardan derlenen haber, bilgi ve dokümanların işlenmesi sonucu elde edilen üründür.[6]

Devlet çapında istihbarat oluşturmakla görevli olan Milli İstihbarat Teşkilatı'nın resmi sitesinde ayrıca, istihbaratın üretilebilmesi için sadece haberin, bilginin ve belgenin toplanmasının yeterli olmadığı, elde edilen haberin, bilginin ve belgenin belli bir sistematik içerisinde işlenmesi gerektiği ifadesine yer verilmiştir.

Ham bilgilerin istihbarat haline gelebilmesi için tasnif, kıymetlendirme, yorum ve yayım aşamalarından geçerek değerlendirilmesi; bir başka deyişle işlenmesi gerekmektedir. İstihbarat faaliyetleri, kesintisiz süren bir çalışmadır ve dünya üzerindeki tüm istihbarat teşkilatları bu çalışmayı bir çarka benzetmektedir. Çeşitli istihbarat teşkilatları, bu çarkı beş,

hatta altı aşamalı olarak göstermektedir. Milli İstihbarat Teşkilatı'nın resmi sitesinde ise istihbarat çarkı, dört aşamalı olarak ele alınmaktadır. (Bkz. Çizelge 1)

Çizelge 1: İstihbarat Çarkı



Tespit ve yönlendirme; çarkın birinci evresidir. İstihbarat ihtiyaçlarının belirlenmesi, bir toplama planının hazırlanması, bilgi toplama emirlerinin yayınlanması ve haber toplama çalışmalarının yönlendirilmesi aşamalarını kapsamaktadır.

Toplama; "açık" ve "gizli" kaynaklardan yürütülmektedir. Gazete, dergi, kitap, radyo, televizyon, yayınları ve internet siteleri, açık kaynakları oluşturmaktadır. Gizli kaynaklar ise çeşitli haber toplama metotları ile birlikte, teknolojinin kullanılmasıyla belirli bir istihbarat ihtiyacı doğrultusunda haber alma ve derleme sürecidir.

İşlenme; haberin toplanmasından sonra, bilgi ve belgelerin tasnif, kıymetlendirme, yorum aşamalarından geçirilerek değerlendirilmesi, yani işlenmesi sürecidir.

Yayım ve kullanım ise değerlendirme sürecinden geçtikten sonra işlenen ve istihbarat niteliği taşıyan bilgilerin, zamanında ve en etkili şekilde ilgili makamlara ulaştırılmasıdır.

İstihbaratın Sınıflandırılması

İstihbarat, çeşitli akademisyenler ve gizli servisler tarafından kimi noktada farklı sınıflandırmalara sahip olsa da genel olarak belli bir sınıflandırma yapıldığını söylemek mümkündür. İstihbarat, milli güç hedeflerine, toplama tekniklerine ve ölçeklerine göre sınıflandırılmaktadır (Özdağ, 2013).

Alanlarına göre istihbarat:

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

Stratejik, taktik ve operasyonel istihbaratın yöneldiği bu alanlar arasında, Siber İstihbarat; hedef ülkenin siber uzaydaki altyapısını teşkil eden cihazlar, kablolar, enerji üreticiler, internet servis sağlayıcıları, sunucular vb. ile siber saldırı, siber istihbarat faaliyetlerinde bulunacak ya da siber savunma yapacak olan teknokratların, görevlilerin nitelik ve nicelik gibi özellikleri hakkında bilgi elde edilmesi ve değerlendirilmesidir.

Bu tanımdan anlaşılacağı üzere, hedefe karşı yapılacak siber saldırı ya da bilgi toplama maksatlı faaliyetler öncesinde, siber istihbarat çalışmaları yapılması gerekmektedir. Bir istihbarat disiplini olarak kabul edilen Siber İstihbarat, ayrıca istihbarat toplama yöntemi olarak da kullanılmaktadır.

Toplama yöntemlerine göre ise istihbaratı şu şekilde sınıflandırmak mümkündür:

- İnsana Dayalı İstihbarat (HUMINT)
- Sinyal İstihbarat (SIGINT)

- Radar İstihbaratı (RADINT)
- Elektronik İstihbarat (ELINT)
- Haberleşme İstihbaratı (COMINT)
- Görüntü İstihbaratı (IMINT)
- Açık Kaynak İstihbaratı (OSINT)
- Siber İstihbarat (CYBINT)

Yukarıda yer alan toplama yöntemlerinden daha fazla yöntemler olup, bunlardan bazıları alt kategoriler olduğu için listede yer verilmemiştir. Ancak genel hatlarıyla istihbarat toplama yöntemleri bu şekilde sınıflandırılabilir. Görüldüğü üzere Siber İstihbarat da artık bir istihbarat toplama yöntemi olarak yer almaktadır.

Siber İstihbaratın Tanımı

Siber İstihbarat ya da siber casusluk, hedefin bilgisi ve izni olmaksızın, siber uzaydaki ağlara, bilgisayarlara ve sair cihazlara hacking vb. teknikler kullanarak sızmak, hassas verilerin toplanarak, istihbarat çarkından geçirilmesi faaliyetidir. Siber istihbarat, sadece teknik faaliyetlerle değil, sosyal mühendislik, psikolojik harp ve sair unsurlar kullanılarak da oluşturulabilmektedir. Angaje edilmiş, hedef örgüt içinde görevli kişilerin, fiziksel olarak sisteme girmesi, trojan, spyware, virüs vb. zararlı yazılımları sızdırması ya da laptop, harici disk, sabit disk vb. depolama alanlarını çalması da siber istihbarat faaliyetleri arasında yer almaktadır.

Siber uzay, “trade craft” olarak ifade edilen, espiyonaj yöntemlerinin farklı şekillerde kullanılabileceği bir alan haline gelmiştir. İnternetin, espiyonaj için en kullanışlı alan olduğu da ifade edilmektedir (Wettering, 2001). Espiyonaj, yani casusluk, esasen devletlere karşı yöneltilen gizli bilgilerin gizli yöntemlerle elde edilmesi faaliyetidir.Devletin veya stratejik ve askeri kurumlarının arşivlerindeki, veri bankalarındaki bilgilerin internet alt yapısıyla “hacking” vs yöntemlerle ele geçirilmesi mümkün olabilir. Gerekli tedbirlerin alınmaması halinde, siber uzay üzerinden hassas verilere erişmek, bunları istihbarat oluşturmak maksatlı kullanmak ve karar alıcılara göndermek, konvansiyonel istihbarat yöntemlerine göre hızlı ve daha düşük bütçeli gerçekleştirilebilmektedir. Bugün, siber uzaya bağlı olan her kullanıcının

nerede olduğu, kiminle görüştüğü, ne konuştuğu, arkadaşları ve akrabaları, yakın zamandaki planları ve daha pek çok internet üzerindeki davranışıyla ilgili bilgi elde etmek mümkündür.

Siber istihbarat faaliyetleri, her zaman bilgi elde etmek amaçlı yapılmayabilir. Kimi zaman, hedef ülkenin e-devlet altyapılarının çökertilmesi, kurumlara ait web sitelerinin erişilemez hale getirilmesi, hacklenmesi, (prestij kaybı olabileceği gibi, çeşitli propagandaların duyurulması maksatlı da olabilir) e-ticaret siteleri, bankalar vb. altyapılara saldırı gerçekleştirerek, internet üzerinden yapılacak ticari ya da finansal işlemlerin duraklatılması, böylelikle ekonomik zarara uğratılması gibi amaçlar da taşıyabilir.

Siber uzayda, gerekli koşulların sağlanması halinde saldırı faaliyetlerinin kim(ler) tarafından yapıldığını tespit etmek neredeyse imkansız olmaktadır. Bu durum, gizli servislerin ilgisini iyice çekmekte, yatırımlarını bu alana yapmaktadır. Gerek güvenliğin alınması, gerekse de siber istihbaratçıların yetiştirilmesi gibi konular, son dönemlerde pek çok devlet tarafından masaya yatırılmış, konuya olan ilgi artmıştır. İnternet üzerinden, özellikle sosyal medya kullanımı sayesinde algı oluşturulması, dezenformasyon ve manipülasyon gibi faaliyetlerde bulunarak, örtülü operasyonlar gerçekleştirilebilmektedir.

Yakın bir gelecekte, siber saldırıların uluslararası ilişkilerde giderek daha önemli bir rol oynamasıyla birlikte, saldırıları kimin yaptığını bilmek politik açıdan atılacak misilleme gibi adımlar bağlamında temel bir sorun teşkil edeceği düşünülmektedir. Kimlik tespiti arayışı ise kimliği konusunda yanıltıcı ipuçları bırakan suçluların sayısında bir artışın da beraberinde getirilmesi beklenmektedir. Hayati önem taşıyan, kritik altyapı ve üretim sistemlerinin özellikle jeopolitik gerginlik dönemlerinde saldırganların ilgisini çekmeye devam edeceği de uzmanlar tarafından masaya yatırılmış bir başka önemli konu. Ayrıca mobil cihazları hedef alan ve güvenlik endüstrisinin adli analiz amacıyla mobil işletim sistemlerine tam erişim almakta zorlanacak olması gerçeğinden faydalanacak casusluk harekatlarıyla daha fazla karşılaşılacağı da öngörüler arasında.[7]

Sonuç

İstihbarat gizemli bir faaliyet olması, konusunda uzman kişilerin bir araya gelerek, belli bir teşkilat çatısı (devlete ait bir kurum) altında görevini gizli bir şekilde icra etmesi gibi sebepler yüzünden, ilgi odağı olmaktadır. Bugün birçok birey/kurum, faaliyet alanlarını genişletmek, rakiplerinden farklı olabilmek, geliştirmiş oldukları sistemi pazarlayabilmek vb. sebeplerle istihbarat sözcüğünün albenisini kullanma eğiliminden hareketle, istihbarat

faaliyetinde bulunduklarını dile getirmektedir. Bu kişiler/kurumlar, siber istihbaratı genel hatlarıyla; "Tehditlerin oluşmadan bilgisini alıp, gerekli savunma sistemine entegre ederek, benzer bir tehdit oluştuğunda savunma geliştirmekle uğraşmadan, savuşturma yöntemidir" vb. şekillerde tanımlamaktadır.

Bu tanım, siber saldırılara karşı önalıcı faaliyetler kapsamında yer alabilir. Dolayısıyla, siber tehditlerin önceden tespit edilmesi ve buna uygun savunma sistemlerinin geliştirilmesi, siber istihbarat değil, siber güvenlik ve/veyakoruyucu güvenlik hizmeti kapsamında ele alınabilir.

Sonuç olarak; siber güvenlik hizmeti vermekte olan kişi veya kurumların, siber istihbarat olarak tanımladıkları hizmetler, genelllikle istihbarat terminolojisindeki şekliyle kullanılmamaktadır. Önleyici teknik faaliyetlerin birçoğu, hacking/penetrasyon testinin ilk evresi olan bilgi toplama aşamalarıdır. Dolayısıyla, yapılan faaliyet ile anlatım veya sunum arasında fark bulunmaktadır. Gerçek anlamda siber istihbarat faaliyetlerinde bulunan kurumlar, bu makalede söz edilen ve siber istihbarat kavramını yanlış kullanan kişiler/kurumlardan ayrı tutulmaktadır.

SONNOTLAR

* Siber İstihbarat Analisti, sakelestemur@gmail.com, Twitter: @sakelestemur

[1] http://www.tdk.gov.tr/index.php?option=com_gts&arama=gts&guid=TDK.GTS.582a54936bc517.35868489

[2] http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf

[3] https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol46no3/article02.html

[4] https://www2.fbi.gov/intelligence/di_defined.htm

[5] https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol46no3/article02.html

[6] http://www.mit.gov.tr/isth-olusum.html

[7] http://h4cktimes.com/arastirma-ve-analiz/kaspersky-lab-2017-tehdit-ongorulerini-acikladi.html

KAYNAKÇA

ÖZDAĞ, Ümit, İstihbarat Teorisi, 7. Baskı, Kripto Kitaplar, 2013

WETTERING, Frederick L., The Internet and the Spy Business, International Journal of Intelligence and CounterIntelligence, 14:342, 2001