YEAR/YIL: 2021 | CİLT/VOLUME: 2 | SAYI/ISSUE: 2

Library, Archive, And Museum Research Journal

ISSN 2718-0832

www.lamrejournal.org

Veri ve Bilgi Güvenliği Bağlamında İstihbarat Faaliyetleri

Intelligence Activities In The Context Of Data And Information Security

Yasin ŞEŞEN*, Alpaslan Hamdi KUZUCUOĞLU**

Cite this article as: Şeşen, Y., Kuzucuoğlu, A.H. (2021). Veri ve Bilgi Güvenliği Bağlamında İstihbarat Faaliyetleri. *Lamre Journal*, *2(2)*, 93-110.

ÖZ: Yaşam, bazen kendi norm ve kurallarına uygun şekilde bazen de belirli kurallar olmadan akışta bulunurken, insanların hayatlarını da doğrudan veya dolaylı yollardan etkilemektedir. Yaşam, insanların hareket kabiliyetlerini, kendilerine olan güven, bağlılık ve beklentilerini, kullandığı araçları, kendilerini koruma aletlerini (silah vb.), teknolojik ilerleme kapasitelerini, yaşadıkları ülke ve çevreleri büyük ölçüde etkilemektedir. İnsanların yaşamlarına etki eden önemli faktörlerin çeşitli değişimleri meydana getirmesinde 'veri ve bilgiler' önem arz etmektedir. İnsanların farklı bakış açıları geliştirebilmelerine zemin hazırlayan veriler, yaşamlarına da olumlu etki ederler. İnsanlar yaşamlarında bir buluşu ortaya koyabilmek, ellerindeki araçları geliştirebilmek, hayatlarının akışlarını değiştirebilmek amacıyla veri ve bilgiyi kullanırlar. Veriler, günümüzde birçok bilgi ve belgeyi oluşturan anlamlı parçalardır. Veriler, çeşitli çalışma alanlarına ayrılabilir; teknik veri, kültürel veri, sosyal veri vb. farklı veri çeşitleri birbirleriyle kaynaşarak düzenlenebilecekleri gibi, birbirinden ayrı olarak da kullanılabilirler. İnsanlar yaşadıkça veriler de sürekli akmaya devam etmektedir. Verilerin bir araya gelmesi ve anlamlı bir bütün oluşturmasıyla bilgi ortaya çıkmaktadır. Çalışmada, dünyada her geçen gün şiddet dozunu yükselterek yaşanmaya devam eden çeşitli faaliyetlerden dolaylı veya dolaysız yoldan etkilenen devletlerin, bu duruma bağlı olarak vatandaşlarını her türlü maddi ve/veya manevi sorunlardan koruyabilmek amacıyla değiştirdikleri ulusal ve uluslararası güvenlik konseptlerinde bilgi paylaşımı, bilgi güvenliği, kültürel istihbarat vb. faktörler üzerinde durulmuştur. Araştırma verilerine katkı sağlamak amacıyla çeşitli veri kaynaklarından elde edilen bilgiler aktarılmıştır. Bireysel güvenliğe yansımaları bakımından bilgi güvenliğinin, istihbarat ile olan ilişkisi irdelenmiş ve bu ilişki bağının geliştirilmesi konusunda öneriler ortaya koyularak çalışma sonlandırılmıştır.

Anahtar Sözcükler: *Bilgi Güvenliği, Bilgi Paylaşımı, İstihbarat, Kültürel İstihbarat, Veri Güvenliği.*

ABSTRACT: While life sometimes flows in accordance with its own norms and rules and sometimes without certain rules it also affects people's lives directly or indirectly. Life greatly affects people's mobility, self-confidence, loyalty and expectations, the tools they use, the tools they use to protect themselves (weapons, etc.) their technological advancement capacity and the countries and environments they live in. Data and information is important for the important factors affecting people's lives to bring about various changes. Data, which lays the groundwork for people to develop different perspectives also have a positive impact on their lives. People use data and information in order to reveal an invention in their lives, to improve their tools and to change the flow of their lives. Data are meaningful parts that make up many information and documents today. Data can be divided into various fields of study; technical data, cultural data, social data etc. Different types of data can be organized by fusing with each other or they can be used separately from each other. As people live, the data continues to flow continuously. Information emerges as the data come together and form a meaningful whole. In the study, information sharing, information security, cultural intelligence in national and international security concepts which are changed by the states that are directly or indirectly affected by the various activities that continue to be experienced by increasing the dose of violence every day in the world in order to protect their citizens from all kinds of material and/or moral problems etc. factors are emphasized. In order to contribute to the research data, information obtained from various data sources was transferred. The relationship between information security and intelligence was examined in terms of its reflections on individual security and the study was concluded by making suggestions to improve this relationship.

Keywords: *Information Security, Information Sharing, Intelligence, Cultural Intelligence, Data Security.*

* Öğr. Gör., Hitit Üniversitesi, Rektörlük, Çorum, Türkiye.
Email: ysesen11@gmal.com ORCID ID: https://orcid.org/0000-0001-6896-0567

**Doç. Dr. İstanbul Medeniyet Üniversitesi, İstanbul, Türkiye.
Email: alpaslan.kuzucuoglu@medeniyet.edu.tr ORCID ID: https://orcid.org/0000-0003-3186-2204

Geliş/Received: 03.04.2020
Düzeltme/Correction: 19.05.2021
Kabul/Accepted: 30.05.2021

GİRİŞ

Veri, anlamlı/anlamsız bilgiler topluluğudur. *"Veri herhangi bir işleme tabi tutulmadan, gözlem veya ölçüm yöntemleri ile ortamdan elde edilen her türlü değerdir"* (Şeker, 2013, s. 3). Bu tanımdan, toplanan verilerin her zaman anlamlı bir bütünlük veya işe yarar bir bilgi taşımak zorunda olmadığı görülmektedir. Dağınık şekilde üretilen veya toplanan verilerin anlamlı biçime döndürülerek, işlevselliklerinin artırılması gerekmektedir. Yılmaz'a göre ise veri (2009, s. 7) *"tek başına anlam ifade etmeyen veya kullanılamayan, bununla birlikte enformasyona ve bilgiye temel oluşturan ilişkilendirilmeye, gruplandırılmaya, yorumlanmaya, anlamlandırılmaya ve analiz edilmeye gereksinim duyulan ham bilgi"* şeklinde tanımlanabilir. Veriler ve verilerden elde edilen bilgiler, günümüzde birçok bilgi ve belgeyi oluşturan anlamlı bütünleşmiş kalıplardır.

Veriler, çeşitli çalışma alanlarına ayrılabilir; teknik veri, kültürel veri, sosyal veri, kütüphane verisi, arşiv verisi, istihbarat verisi vb. Farklı veri çeşitleri birbirleriyle kaynaşarak düzenlenebilecekleri gibi, birbirinden ayrı olarak da kullanılabilirler. İnsanların kullanım durumlarına bağlı olarak, insanlar yaşadıkça veriler de sürekli akmaya devam etmektedir. Verilerin bir araya gelmesi ve anlamlı bir bütün oluşturmasıyla bilgiler de gelişmektedir. Veri güvenliği, bilgi teknolojisinde sürekli olarak önemli bir sorun olmuştur. Veri güvenliği ve gizlilik koruması sorunlarının çözümü açısından, donanım ve yazılımlar ön plandadır.

Bu nedenle bulut teknolojilerindeki verileri korumak için hem yazılım hem de donanım açısından farklı güvenlik teknikleri ve zorluklar gözden geçirilmelidir. Daha güvenilir bulut ortamı için veri güvenliğini ve gizlilik korumasının geliştirilmesi amaçlanmalıdır (Sun vd., 2014, s. 5). Organizasyonel kavram, stratejileri, kültürü, yapısı ve politikaları gibi bir kuruluşu temsil eden özellikler olarak tanımlanabilir.

Kurumsal yapılarda bilgi güvenliği açısından organizasyonel ve çevresel riskler bulunur. Bu organizasyon ve teknik verilerin de korunmasını gerektirir. Organizasyonlarda yönetim mekanizmaları, kurumsal güvenlik uygulamalarını ve kültürünü, güvenlik planlamasını, güvenlik politikasını ve risk azaltma stratejilerini tanımlamalıdır. Büyük verinin getirdiği güvenlik ve mahremiyet sorunlarına ilişkin organizasyon kültürü ve farkındalık, verileri insan kaynaklı ihlallerden korumada dikkate alınması gereken önemli bir faktördür (Salleh vd., 2016, s. 8). Açık kültürel ve sosyal veriler sosyal medya platformlarında ve web platformlarında yayınlanabilmektedir. Sosyal medyada bilgi yayınlamak, kişisel ve gizli bilgilerin kamusal alana sızabileceği popüler bir faaliyet durumundadır. Sonuç olarak, sosyal medya, bir kuruluşun veri ihlaline maruz kaldığına dair bir gösterge olan bilgileri de içerebilir. Son zamanlarda, tanınmış kuruluşlara yönelik siber saldırıların sayısı önemli ölçüde artmıştır. Veri hırsızlığı ve finansal hırsızlık hem müşteriler hem de kuruluşların mali kayıplarını artırabileceğinden dolayı oldukça zararlıdır.

Müşterilerin uğradığı mali kayıplar, itibarların zarar görmesine neden olabilir. İtibar zararları, müşterilerin kuruluşa olan güvenini kaybettiği için anında ve gelecekte iş kaybına neden olmaktadır (Ullah vd., 2020, s. 6).

Bilgi akışının sürekli şekilde takip edilebilmesi, istihbarat faaliyetlerini ortaya çıkarmaktadır. Çünkü bilgilerin sürekli şekilde ve çok gizli olarak (sır halinde) saklanabilmesi pek mümkün değildir. Bilgilerin yer değiştirmesi veya çeşitli teknik uygulamalarla dost-düşmanlar tarafından ele

geçirilebilmesi mümkündür. Bu nedenle veri ve bilgilerin de korunması önem arz etmektedir. Veri ve bilgi

güvenliğinin sağlanması, istihbarat çalışmalarıyla mümkündür. Var olan bilgilerin ve/veya potansiyel bilgi akışının güvenli şekilde sağlanması ve önemli verilerin korunması amacıyla, istihbarat kuruluşları çeşitli teknik yöntemlerle çalışmaktadır. Zaman geçtikçe değişen konseptlere uygun olarak, istihbarat çalışmaları da her geçen gün farklı şekiller ve içerikler kazanmaktadır. Özellikle karşı dost/düşman devletlere karşı yürütülen her türlü psikolojik ve fiziki tehditlerden korunabilmek açısından istihbarat toplama önemli bir faaliyettir.

Çalışmada literatürde belirtildiği üzere teknik veri, kültürel veri, sosyal veri gibi her türden verinin insan kaynaklı ihlaller nedeniyle gerek kurumlar gerekse devletler arasında transfer edilebileceği, bunun illegal olması nedeniyle siber suçlar kapsamında değerlendirilebileceği, bu veri ihlallerinin kültürel, askeri, endüstriyel olarak istihbari şekilde mümkün olabileceği üzerinde durulmuştur.

TEORİK ÇERÇEVE

İstihbarat faaliyetlerinin ilk örnekleri, insanlığın başlangıcı kadar geriye gidebilir. İlk çağlarda hayatını devam ettiren insanlar, hayatta kalabilmek ve yaşam kalitelerini artırabilmek amacıyla karşılarına çıkan sorunlara çözüm aramışlardır. Bu amaçlarla bilgi edinme ihtiyaçlarını giderebilmek maksadıyla, farklı yerlerden bilgi kazanmak için mücadele etmişlerdir. Avcılık, toplayıcılık, korunma ihtiyacı ve diğer rakip kabileler veya devletler tarafından asimilasyon olma tehlikeleri vb. nedenlerden dolayı istihbarat faaliyetler ortaya çıkmıştır. Antik Çağ'da çok ilkel koşullarda da olsa, istihbarat faaliyetleri hayata geçirilmiştir. Zaman içerisinde bu faaliyetler daha sistematik bir biçim almış ve geliştirilmiştir. *"Bilginin kaynağını oluşturan haber alma ve haber toplama yeteneği de bireysel çabalar ve teknolojilerden daha ileri bir seviyeye gelmiştir"* (Seren, 2017, s. 8). Bu hızlı gelişimin sonucu olarak, istihbarat faaliyetleri de hızlanmıştır.

İstihbarat kavramı çeşitli dillerde birbirinden farklı şekilde tanımlanabilir. Bu tanımların ortak noktası 'açık ve/veya gizli şekilde bilgi edinme faaliyetleridir'. Karşı taraftan öğrenilebilen her türlü bilgi ve veri önemlidir. Her ne şekilde olursa olsun öğrenilen bilgiler, gelecekte bir amaç uğruna rahatlıkla karşı tarafın aleyhine kullanılabilir ve/veya farklı devletlere de sızdırılabilerek çok kapsamlı sorunlara da yol açabilir.

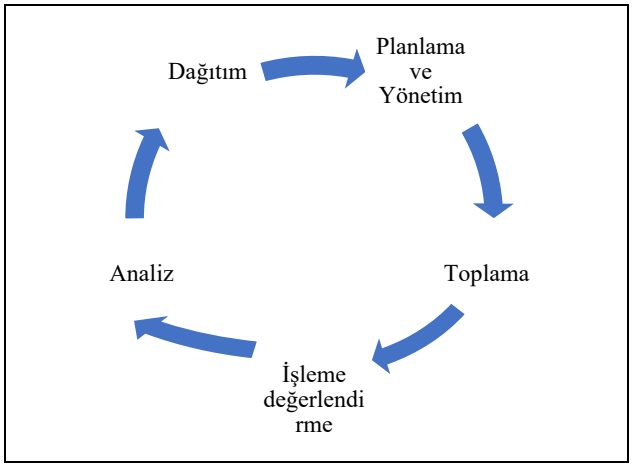
İstihbarat teriminin tanımı farklı şekillerde ele alınabilir. İstihbarat kavramı köken olarak, Arapça 'istihbar' kelimesinin çoğulu olup; 'yeni öğrenilen bilgiler, duyumlar, bilgi toplama, haber alma' anlamlarına gelmektedir. İngilizce literatürde mevcut veya muhtemel düşmanlar hakkındaki gizli bilgiler' anlamına da gelmektedir. Bir başka İngilizce sözlük olan International Dictionary of Intelligence'da istihbarat terimi; *"mevcut ve muhtemel durumlar ile yerel ve yabancı faaliyetlere ilişkin koşullar hakkında bilgi toplama ve işleme sürecinin sonucu olarak yer almaktadır"* (Türk Dil Kurumu Sözlüğü, 2021; The American Heritage Dictionary of the English Language, 2021; Carl, 1990, s. 9).

Tanımlardan anlaşılabildiği gibi, istihbari faaliyetlerin yürütülmesiyle birlikte aktif ve/veya potansiyel düşmanlar hakkında bilgiler elde edilir. Düşmanların sakladığı ve gizli tuttukları bilgiler de istihbarat faaliyetleri ile öğrenilebilir. Düşmanların her türlü faaliyetleri takip edilerek, düşmanın hareket tarzı da tahmin edilebilir. İstihbarat bir nevi satranç oyunu gibidir, sürekli stratejiler ve yön belirlemeler söz konusudur. Bu konuda ünlü filozof Sun Tzu'nun öğretileri ön plana alınabilir. Sun Tzu 'savaş aldatmadır, savaş stratejidir' demektedir. Sun Tzu'nun da ifade ettiği gibi, karşı devletleri manipüle edebilmek ve

onlara zarar verebilmek açısından istihbarat gayet kullanışlı bir çalışma alanıdır.

İstihbaratın farklı türleri de ele alınabilir. *"Batılı perspektiften 'istihbarat' profesyonel bir disiplin olarak günümüzde üç disipline bağlı olarak incelenebilir: diplomasi, askeri keşif ve iç güvenlik. Bu alanlar ve istihbarat arasındaki sınırlar oldukça belirsiz ve geçişkendir. İstihbarat tarihi ve askeri tarih ya da diplomasi tarihi kaynakları ortaklaştığı için yöntemlerde de benzerlikler olduğu kaydedilmiştir"*

(Warner, 2007, s. 11). Yabancı bir devlet hakkında gizli olan istihbaratın verimli şekilde takip edilebilmesi için öncelikle iç güvenlik protokollerinin ve uluslararası diplomasinin kurallarının dışına çıkılabilmesi önemlidir. Bu noktada askeri keşif ön plana gelmektedir. Her devlet kendi askeri gücünü saklamaya çalışırken, karşısındaki dostu veya düşmanının hakkında istihbarat toplama faaliyetlerinde bulunmaktadır. İstihbarat dünyasında gerçek anlamda dost veya düşman kavramı yoktur. Sadece çıkar ilişkileri ön plandadır. Çünkü devletler arasındaki ilişkiler, pamuk alevine benzer şekildedir ve tüm istihbarat teşkilatları asıl amaç olarak karşıdakine zarar verebilmek amacıyla kurulurlar.



Şekil1. İstihbarat Döngüsü (Akman, 2019, s. 5)

Şekil 1'de görüldüğü gibi her istihbarat faaliyeti bir döngü süreci izlemektedir. Bu döngüde, 'Planlama ve Yönetim, Toplama, İşleme/Değerlendirme, Analiz, Dağıtım' süreçleri birbiriyle bağlantılı şekilde işlemektedir. Bu süreçlerin dengeli şekilde takip edilmesi sonucunda verimli bir bilgi sağlama ağı kurulabilir. 'Toplama aşaması' çeşitli kaynaklardan verilerin toplanması faaliyetleridir. Bu süreç, işleme/değerleme aşamasıyla' devam etmekte ve diğer süreçlerle de tamamlanmaktadır. *"Bu disiplinlerin hangisinin ön planda olacağı, ele alınan vakanın özgül şartlarına ve doğasına bağlıdır. Yukarıda genel anlamda bilginin, özel anlamda bilimsel bilginin nasıl toplumla iç içe, etkileşim halinde olduğu görülmüştür"* (Akman, 2019, s. 7). 'Planlama ve Yönetim' faaliyetiyle başlatılan genel 'İstihbarat Döngüsü Süreci'; 'Analiz ve Dağıtım' sürecinin tekrar 'Yönetim' aşamasına bağlanmasıyla devam ettirilmektedir. Eğer istihbarat faaliyetinin 'Yönetim' aşamasında verimli bir şekilde bilgilenim elde edilemediği hissedilirse, süreç tekrarlanabilir ve/veya değiştirilebilir. Çünkü her şekilde asıl amaç, 'istenen bilgilere herhangi bir şekilde' ulaşabilmektir.

Devlet kurumunun ilk olarak oluşturulmasından itibaren geçen binlerce yıl içerisinde devletin güvenliğinin sağlanarak, devletin ayakta tutulması en önemli amaç olmuştur. Bu noktada 'ulusal güvenlik' terimi ön plandadır. Ulusal güvenlik, devletin kendi iç organlarının ve yurttaşlarının güvenliğini sağlamak için ön plana aldığı her türlü güvenlik uygulamasıdır. Bu uygulamalar bazen uluslararası kanunlara uygun, bazen de uluslararası hukukun kurallarına teğet geçebilen, bazen de sadece devletin iç hukukuna uygun şekilde oluşturulmaktadırlar. Ulusal güvenlik yasalarının veya uygulamalarının, toplumun genel geçer dünya görüşüne ve ulusal tehdit algısına yönelik biçimlerde oluşturuldukları görülmektedir. Ulusal güvenliğin verimli oluşturulması, takip edilmesi, devamlılığı vb. her açılardan topluma yönelik, toplumun yaşamını doğrudan etkileyen özelliklere sahiptir.

Ulusal güvenlik dış ve iç güvenlik şeklinde incelenmektedir. İç güvenlik, devletin iç tehditleri öncelikli olmak üzere, dış tehditlerle de desteklenerek kamu düzeninin bozulmasının önlenmesi çalışmalarıdır. *"Eğer anayasal çerçevede güvence altına alınan temel hak ve özgürlüklere karşı bir tehdit söz konusu ise gerekirse sıkıyönetim ve olağanüstü hâl ilan edilerek iç güvenlik sağlanır. Dış güvenlik ise yabancı devletlerin ortaya koyacağı saldırı politikalarına karşı koyma halidir"* (Özalp ve Asker, 2017, s. 18). Özalp ve Asker'in de bahsettiği gibi, ülkeler dışarıdan gelebilecek olan tehditleri askeri güçlerle karşılarken; içeriden gelebilecek sorunlarda da sıkıyönetim ve olağanüstü hâl yasaları ile (örn. 15 Temmuz 2016 Hain Darbe Girişimi sonrasında çıkarılan yasalar) çözüm bulabilmektedirler. Ulusal güvenliğin sadece silah ile savaşı içermediği, aynı zamanda asimetrik bir savaş durumunun da var olduğu görülmektedir.

Günümüzde bir savaş ve çatışma durumunda, o ülkenin tüm unsurları ile mücadele edilmektedir. Bu unsurlar içerisinde insan ve kültür faktörü de önem arz etmektedir. İstihbarat sürecinin hızlanması ve sürecin gelişmesi amacıyla internetin ve bilgisayar ağlarının toplumun tüm birimlerini inceleyebilmesi önemlidir. Topluma yayılan sistemlerden farklı olarak, toplumun sıklıkla kullandığı sistemlerden daha gelişmiş ve gizli araçlardan istihbarat örgütleri yoğun olarak yararlanmaktadırlar. Günümüzde dünyadaki birçok ülke siber saldırı tehdidi altında yaşamaktadır. Bu tehditleri bertaraf edebilmek amacıyla sürekli siber suçlarla mücadele edebilecek uzmanlara ihtiyaç vardır. Bu uzmanların hazırladığı raporlar, özel kodlama araçları, siber saldırı yöntemleri vb. aslında dünyada siber istihbaratın inanılmaz boyutlara ulaştığını göstermektedir. Tüm bu sebeplerden dolayı istihbarat kurumları günümüzde siber istihbarat çalışmaları alanında oldukça yoğun çalışmaktadırlar.

Her geçen gün istihbarat faaliyetlerinin arttırılması ve çeşitlenmesi açısından, 'kültürel istihbarat' ön plana çıkmaktadır. Tüm ülkenin ulusal güvenlik politikalarının bu felsefelere uygun şekilde düzenlemesi için çalışmalar yapılmaktadır. Kültürel istihbarat konusu geniş bir şekilde ele alınarak, dünyadaki genel istihbarat faaliyetleri ile olan bağı incelenebilir. Kültürel istihbaratın içeriği, klasik istihbarat ile bağlantılıdır. Yüzyıllardır süregelen klasik istihbarat yöntemleri, geleneksel savaşların başarısında önemli bir yer tutmakta iken, 'toplum-merkezli' çatışmaların yoğunlaşması ile 'kültür kavramı' da ön plana çıkmaya başlamıştır. *"Devlet yönetiminde ve/veya askerî harekâtlarda karar vericiler/komutanlar özellikle askeri istihbaratın varlığına önem verirlerken, istihbaratın kültürel yönünü çoğunlukla göz ardı etmişlerdir. Afganistan ve Irak harekâtlarında şu durum ortaya çıkmıştır ki, yerel halkın 'kalpleri ve zihinleri' kazanılmadan, salt askeri istihbarat teknikleri ile sağlanan tedbirler, özellikle terörizm ile mücadelenin başarısını kısa ömürlü kılacaktır"* (Özer, 2018, s. 3). Kültürel olarak bir toplumun benliği etkilenemezse, o toplumun elde tutulabilmesi ve o toplumun düşmanca tavırlarından geri durabilmek mümkün olamaz. Bu doğrultuda kültürel istihbarat çeşitli şekillerde tanımlanabilir. Özellikle yabancı literatürde kültürel istihbarat; kültürel bilginin, harekât planlamalarının, düşmanı ve harekât çevresini nasıl etkilediğini ve yönlendirdiğini analiz etmeyi hedefleyen bir istihbarat disiplini (aktaran Özer, 2018, s. 11) olarak tanımlanabilir. "Kültürel istihbarat, bir harekât bölgesine gerçekleştirilecek harekât öncesinde veya harekât esnasında, o bölgede bulunan kültürün tanınması ve anlaşılması maksadıyla toplanan kültürel bilginin tasnif edilmesi, değerlendirilmesi ve analiz edilmesidir" (Wunderle, 2007, s. 21). Kültürel istihbaratın terörizmle mücadeledeki rolü göz ardı edilemeyecek derecede önemlidir. Harekât alanında bulunan toplumun kalplerini ve zihinlerini kazanmak maksadıyla geliştirilen politikaların başarısı, doğru ve zamanında elde edilen istihbarat ile

mümkündür. *"İstihbaratın temel amacının bilinmeyene ilişkin sis perdesini aralamak ve onu görünür kılmak olduğu düşünüldüğünde; kültürel istihbarat ile bireysel ve toplumsal kültüre ilişkin bilinmeyenlerin açığa kavuşturulması sağlanmaktadır"* (Saydam, 2010, s. 6).

Kültürel istihbaratın ilk aşaması 'bilginin toplanması' aşamasıdır. Bu aşamada kültürel farkındalık ve kültürel edinim ön plandadır. Bu aşamada, karşı tarafın kültürü ve kültürel bağlantılarının çözümlenmesi gerekmektedir. Böylece karşı taraflardan ilk bilgilerin nasıl toplanabileceği üzerine fikir yürütülür. Daha sonra elde edilen bilgilerin anlaşılması ve uygulanmasına yönelik olarak 'kültürel farkların ayırt edilmesi' aşaması takip edilir. Bu takip edilen iki aşamada da kültür, henüz işlevsel hale getirilmemiştir. İki aşamada ele alınan kültürel farkındalık durumu, bir sonraki safhada 'kültürel bilginin elde edilmesi' sürecine geçiş yapar. Özellikle savaş durumlarında, harekât alanında kullanılabilir ve karar vericilerin olumlu/olumsuz kararlarını etkileyen bir süreç ön plandadır. Bu aşamada, karşı taraftan bilginin akması ve karşı tarafa karşı yapılan bir istihbarat süreci hayata geçmektedir. *"İstihbarat birimleri, düşmanın askeri imkân ve kabiliyetlerinin yanı sıra değerlerini, inançlarını, davranışlarını, bir başka ifade ile kültürünü öğrenmek ve analiz edip harekât kapsamında kullanmak durumundadır. Kültürel istihbarat eksikliği, askerî harekâtlarda düşmanın ve bölgedeki halkın yanlış algılanması ve yanlış yorumlanmasına neden olabilmektedir"* (Özer, 2015, s. 7). Günümüzde dünyanın birçok yerinde devam eden savaşların başarılı olmasına yardımcı olabilmesi açısından kültürel istihbarat faaliyetleri takip edilmektedir.

VERİ VE BİLGİ GÜVENLİĞİ KAVRAMI

Bilgi, verilerin ulaşılmak istenen hedeflere uygun biçimlerde farklı süreçlerden geçerek faydalı ve anlamlı olabilecek veriler topluluğuna dönüşmesi olarak tanımlanabilir. Bilginin gelişmesi ve bilgilenen insanların topluma adapte olabilmesi önemlidir. Bireyler, kamu kurumları, özel kuruluşlar ve devletin yapısı bilgi toplumuna dönüşürken; bilginin her türlü getirisinden etkilenmekte ve bilgiye dayalı vatandaşlar ve kurumlar olma yönünde ilerlemektedirler. Bilgi alanındaki bu gelişmeler bilginin mahiyetini, içeriğini ve anlamını da değiştirmektedir. *"Bilgi, zaman içerisinde stratejik bir kaynak olarak kurumun yenilik yaratma potansiyelini artıran bir faktör olarak önem kazanmaktadır"* (Bensghir, 2011, s. 7). Bilgi, ihtiyaç duyan herkese ulaştırılabildiği sürece anlamlıdır ve önemlidir. Bilginin üretimi, gelişmesi ve paylaşımı ön planda olmakla birlikte, bilginin korunması ve bilgi güvenliği daha ön planda olmalıdır. Çünkü bilginin gelecek kuşaklara ulaşabilmesi ve kötü niyetli tarafların eline geçmemesi açısından 'bilgi güvenliğinin' her daim ön planda olması gerekmektedir. Bu amaçla yasal mevzuat ve toplumsal yapı da uygun duruma getirilebilir. Gerektiğinde bilginin paylaşımı da kısıtlanabilir.

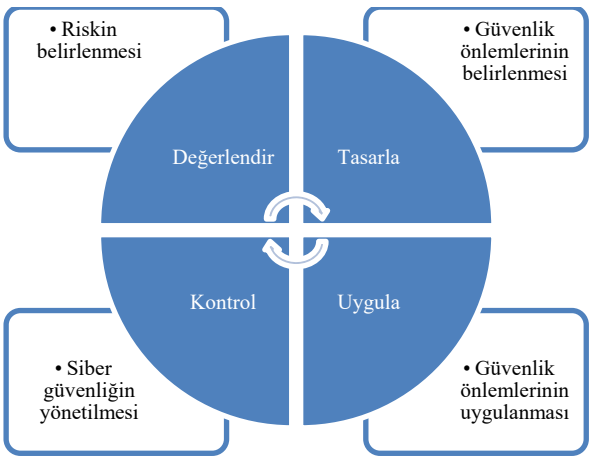
Günümüzde bilgisayar ve iletişim sistemlerinin gelişmesi, yapay zekâ, nesneler interneti, otonom araç, hibrit otomobil vb. kavramlarının günlük dile girmesi, enerji üretim ve depolama sorunlarının çözülmesi faaliyetleri beraberinde büyük teknolojik gelişmeleri de ortaya çıkarmıştır. Bu tür değişimler toplum yapısını, hukuki normları, insan-üretim ilişkilerini ve kültürel normları da değişime uğratmıştır. Bilginin üretimi, yönetimi, güvenliği ile yayımı konusunda yeni yöntemler tartışılır olmuştur. *"Bilginin tek bir merkezden üretilerek dağıtıldığı düzen artık multidisipliner bir yaklaşımla, farklı uzmanlıkların ve alanların katılımı ile üretilmekte ve birçok kanaldan dünyanın her yerine aynı anda dağıtılabilmektedir"* (Gibbons ve başkl., 1994, s. 9). Gibbons'un da ifade ettiği gibi bilginin paylaşımı ve bilginin özelleştirilerek korunması konusunda dünyada ülkeler arasında genel bir mücadele hâkimdir. Dünyada farklı ülkelerin uyguladığı askeri doktrinler, stratejik doktrinler, savaş doktrinleri vb. her

geçen gün değişime uğramaktadır. *"Artık günümüzde, kara, deniz, hava ve uzayın yanı sıra siber ortam da yeni bir mücadele alanı olarak ortaya çıkmıştır" (*Çifci, 2013, s. 12).

Bilgi güvenliğinin sağlanması günümüzde devletlerin temel hedefidir. Bu amaçla askeri, bürokratik ve sivil temelli birçok girişim ve atılım yapılmaktadır. Güvenlik, tarihi çağların en başından itibaren devletlerin dikkat ettiği önemli bir konu olmuştur. *"Güvenlik, insanlık tarihi ile birlikte ele alınan ve insanoğlunun doğa ile mücadelesinde, psikolojik yapısında, sosyal yaşamında, siyasal yapılanmasında, ekonomik ilişkilerinde, kısacası yaşamın her boyutunda davranışlarını etkileyen bir kavramdır"* (Dedeoğlu, 2003, s. 12). Güvenlik, kişisel güvenlik, kurumsal güvenlik, bilgi güvenliği, evrak güvenliği, devlet güvenliği, ulusal güvenlik, uluslararası güvenlik vb. alt ve özel alanlar içerisinde de incelenebilir. Güvenlik tanımları incelendiğinde, ortak bir tanıma ulaşabilmek zordur. Çünkü güvenliğin özel alt alanlarının kendi spesifik çalışma düzenleri vardır ve bu düzenlere uygun şekilde tanımlar da değişime uğrayabilir. Bilginin güvenlik içerisinde tutulabilmesi ve bilgi ağlarının arasında güvenli bir iletişimin devamlılığı açısından bilgi güvenliği araçlarının geliştirilmesi önem arz etmektedir. Bu araçların geliştirilmesi amacıyla öncelikle bilginin nasıl korunacağı ve bilgi güvenliğinin içeriğinin nasıl oluşturulacağı üzerinde çalışılmalıdır. Bilgi güvenliğinin içeriği incelenmek istenildiğinde, içinde yaşadığımız çağda teknolojik dönüşüme bağlı olarak hızlı bir evrimin süregeldiği ve bilginin içeriğinin de sürekli şekilde değişime uğradığı görülmektedir. Bilginin elektronik ortamlarda saklanması ve elektronik ortamların da her geçen gün geliştirilmesi mümkün olmuştur. Zaman içerisinde uygulama yazılımları ve internetin hızının da artışıyla birçok teknolojik alet artık daha çoğunlukla taşınabilir şekilde oluşturulmakta ve taşınabilir platformlarda hizmet vermektedir. Teknolojik aletlerin taşınabilir ve içeriğinin kolay kopyalanabilir olması beraberinde çeşitli güvenlik zafiyetlerini de getirmiştir. Tüm bu durumlar bilgiye gereğinden hızlı ve kolay ulaşılabilmesiyle birlikte, bilginin içeriğinin ve bazı durumlarda gizliliğinin de korunmasını güçleştirmiştir.

Bilgi önemli bir güçtür ve kesinlikle yetkin kişilerin elinde bulunmalıdır. Bazı durumlarda bazı bilgilerin uygun olmayan ve/veya yetersiz kişilerin eline geçmesinin önlenmesi gerekmektedir. Bu gibi durumların önlenebilmesi amacıyla çeşitli güvenlik önlemleri, güvenlik yazılımları, güvenlik araçları vb. kurum ve kuruluşlarda önem kazanmaya başlamıştır. Alınan tüm güvenlik önlemlerinin birinci basamağını daima 'insan faktörü' oluşturmaktadır. İnsanların eksikliklerinin giderilebildiği ölçüde, sistemden daha verimli hizmetler alınabilecektir. *"Yapılan birtakım araştırmalarda bilgi güvenliği risklerini gidermede insan faktörünü göz ardı ederek oluşturulacak sistemsel bir takım güvenlik çemberlerinin çok etkili ve yararlı olmadığı görülmektedir"* (Kandemir ve Şahinaslan, 2009, s. 5).

İlk adım, temel risk ve güvenlik seviyelerini belirlemektir. İkinci adım, uygun güvenlik ölçümlerini kullanarak sistemi tasarlamaktır. Üçüncü adım, işletmenin işletimi üzerinde minimum olumsuz etkiyi elde etmek amacıyla güvenlik ölçümlerini ve prosedürlerini uygulamaktır (Dazahra vd., 2018, s. 3).



Şekil 2. Siber Güvenlik Döngüsü (Dazahra vd., 2018, s. 7)

Bilgi güvenliği tehditleri incelendiğinde 'iç ve dış tehdit unsurlarının' var olduğuna ulaşılmaktadır. İç tehdit unsurlarına bakıldığında kurum bünyesinde çalışan kişilerin oluşturabileceği bilinçli veya bilinçsiz tehditler sayılabilir. *"Bilinçli tehditler iki kategoride ele alınabilir: İlk kategori, kurumda çalışan kötü niyetli bir kişinin kendisine verilen erişim haklarını kötüye kullanması; ikinci kategori ise bir kişinin başka birine ait erişim bilgilerini elde ederek normalde erişmemesi gereken bilgilere erişerek kötü niyetli bir aktivite gerçekleştirmesidir"* (Baykara, Daş, Karadoğan, 2013, s. 6). Bilinçsiz tehditler ise, birçok kurum için bilinçli tehditlerden daha büyük risk teşkil edebilmektedir. Çünkü öngörülemezdir ve geniş ölçekte yaşanabilirler.

Bilginin korunmasında görüldüğü gibi öncelikli konu, insan faktörüdür. Tüm sistemleri 'ortaya koyan, takip eden, denetleyen, gerektiğinde değiştiren' insanlardır. İnsanların her türlü hatası veya dikkatsizliği en iyi şekilde kurulmuş bir sistemi bile etkileyebilir. Bu nedenle bilgi güvenliğinin içeriği ortaya koyulurken, sistemin yöneticisi olacak olan bilgi yöneticilerinin özelliklerine uygun şekilde bir sistemin oluşturulması öncelikli konu olmalıdır. Sistem yöneticisinin yetersiz olduğu konularda, kişiyi yönlendirecek ve ona donanımsal katkı sağlayacak her türlü eğitimin planlanması gerekmektedir. Bu amaçla bilgi yöneticilerine verilmesi gereken eğitimlerin içeriğinde temel bilgi kavramları, bilgilerin bulunduğu ortamların geliştirilme araçları, bilginin nitelikleri, bilgi güvenliğine ilişkin güncel tehditler ve saldırıların bertaraf edilme yöntemleri de bulunur. Bu faktörlerin hayata geçirilmesinin kolaylaştırılması için de çeşitli hukuki, bürokratik ve kurumsal işlemler işlevsel duruma geçirilmelidir. Kişisel bilgi güvenliğinin sağlanabilmesi amacıyla, teknolojik ve siber saldırılardan korunabilmek önemli konulardır. Bu konuda, bireysel bilinç ve farkındalıktan istifade edilmelidir.

Kişisel bilgi güvenliği önlemi olarak aşağıda maddeler halinde verilen siber saldırı türlerine karşı çeşitli güvenlik önlemlerinin alınması tavsiye edilebilir. Bu önlemler ve yapılması gereken çalışmalar şunlardır:

- Program manipülasyonunun önlenmesi,
- Sahtekârlık ve taklite önlem,
- Erişim araçlarının çalınmasının önlenmesi,
- Kimlik çalmanın önlenmesi,
- Ticari bilgi çalmadan korunma,
- İstihbarat amaçlı faaliyetlerin hayata geçirilmesi,
- Takip ve gözetleme faaliyetleri,
- Virüsler, solucanlar (worms), ajan yazılım (spyware), truva atlarından korunma,
- Spam mailden korunma,
- Hizmeti aksatan veya durduran (D-Dos) saldırılarını bertaraf edebilmektir (Baykara, Daş, Karadoğan, 2013, s. 9).

Yukarıda verilen saldırı türleri ve her geçen gün geliştirilen siber saldırı türleri bilinmeli ve bilgi güvenliği bilinci açısından bu konulara dikkat edilmelidir. Bu tür saldırılardan korunabilecek şekilde oluşturulmuş yazılımsal ve donanımsal destek üniteleri inşa edilmelidir. İnşa edilen destek ünitelerinin devamlılığının sağlanması ve geliştirilmesi için teknolojik yatırımlar hiç soluk kesmeden devam ettirilmelidir. TS ISO/IEC 27001, TS ISO/IEC 15408 vb. önemli standartlara uygun şekilde inşa edilen ve devam ettirilen arşiv binaları ve bilgi merkezlerinde; gerçek ve/veya tüzel kişilerce uyulması gereken kurallar zaman içerisinde güncellenmektedir. Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı'na[1] uygun şekillerde, her türlü hizmetin yürütülmeye

[1] https://www.btk.gov.tr/uploads/pages/2-1-strateji-eylem-plani-2013-2014-5a3412cf8f45a.pdf

devam ettirilmesi bilgi güvenliği açısından hayati bir unsurdur. Bunun yanında herhangi bir olağanüstü durumda ürün işleme, dağıtım, kritik altyapıların korunması, devlet-endüstri ortak projelerinin korunması

vb. unsurlar açısından, özel sektöründe bilgi güvenliği önlemlerine uyması gerekmektedir. Bu amaçla ister teknolojik ister eski usul basılı şekilde her türlü belge, bilgi, doküman, haber vb. birinci elden korunabilmeli ve elde edilebilmelidir. Bu amaçla, bilgi edinme yöntemi olarak istihbarat ön plana çıkmaktadır.

İstihbarat, devletin uğrayabileceği her türlü maddi ve manevi saldırı ve zararın önceden öğrenilerek bertaraf edilebilmesini sağlamaktadır. Bu amaçla istihbarat teşkilatları oluşturulmakta, devletin haber alma ve haber saklama gücü de üst düzeylere çıkarılabilmektedir. İstihbarat faaliyetleriyle birlikte, gelecekte izlenmesi gereken bilgi güvenliği politikaları belirlenebilir. Bu politikalara göre, bilgi güvenliği mekanizmaları inşa edilebilir. Burada amaç, güvenlik konularında ileride devleti yönlendirecek, devlete kendisini savunma içgüdüsü oluşturabilecek her türlü yasal veya gizli savunma politikalarının kazandırılmasıdır. Tüm bunların yanında savunma süreçlerinin nasıl geliştirileceğine dair idari uygulamaların da kurumsallaştırılmasıdır.

SİBER İSTİHBARAT

Günümüzde bilgi, her alanda devletlerin belirleyici güç potansiyeli durumuna gelmiştir. Bilginin kullanılması ve istihbarata dönüştürülmesi için birçok alanda çalışmalar ortaya koyulmaktadır. İstihbaratın amacı, bilgiyi yani gücü maddi/manevi anlamda elde etmektir.

Yarım yüz yıldır önemli bir faaliyet alanı olan istihbarat kavramı; oluşum yapısı ve faaliyet alanları açısından tehdit algılamalarındaki değişime paralel olarak sürekli gelişmiştir. İstihbarat ilk günden itibaren haber toplayabilmek için en güncel teknolojiyi kullanmaktadır. Bu nedenle istihbarat, bilgi teknolojilerinin sunduğu imkânlardan sonuna kadar yararlanmakta ve bu durumla bağlantılı olarak siber uzayı etkili bir şekilde

kullanmaktadır. Siber uzayın kullanılması sayesinde istihbarat bir taraftan yeni yönler kazanırken, bir taraftan da yeni mücadele alanları ile karşı karşıya kalmaktadır. Bu açıdan bakıldığında önümüzdeki dönemlerde savaşların kaderini klasik savaş cephelerin yerine, asimetrik bir etki oluşturan ve harbin beşinci boyutu olarak kabul edilen siber uzayda yaşanan savaşlar belirleyecektir. Artık devletler salt çok iyi korunan askerî üstler, okyanuslarda donanmalar veya yüksek teknolojiye sahip uçan savaş aletleri yapmakla uğraşmayacaklardır. Çünkü bu aletlerin korunması açısından, yapay zekaya bağlı olarak siber taarruz kabiliyetlerinin de geliştirilmesi zaruri duruma gelmiştir.

Siber taarruz kabiliyetlerinin geliştirilmesi ile her zaman fiziksel donanımın geliştirilmesi gerekliliği ortadan kalkmamaktadır. Siber güvenlik ve harp, yeni bir alan açarken konvansiyonel olana entegre edilir ve konvansiyonel olan da siber gelişmelere göre adapte edilmektedir.

Tüm bu gelişmeler geleceğin harp ortamında siber savaşların önemini göstermekte ve siber savaşların başta modern devletler olmak üzere bilgi teknolojilerine bağımlılıkları yüksek olan devletlerin ulusal güvenlikleri için gerçek bir tehdit oluşturduğunu ortaya koymaktadır. Ulusal güvenliğin devamlılığı, dünyanın her coğrafyasında her güçlü-güçsüz devletlerin temel problemidir. Dünyada olup bitenden haberdar olup, ulusal çıkarları ile çatışan bir durum söz konusu olduğunda duruma müdahale etme refleksi ile hareket eden askerî açıdan güçlü ülkeler (ABD, Rusya, Çin vb.) bu alanda söz sahibi olma adına alt yapısını

kurdukları siber uzayı şekillendirmek için çalışmalar yürütmektedirler. Siber alanda söz sahibi olan devletler bu alanda yürüttükleri istihbarat çalışmaları ile savunma ve saldırı stratejilerini geliştireceklerdir. Gelişmiş ülkeler, artık toplu mücadele için Siber Güvenlik Ajansları kurmaya başlamışlardır. Güvenlik stratejilerin geliştirilmesi ve daha fazla hukuksal zemin kazanabilmesi için, uluslararası siber pazarlar bile kullanabilmektedirler. *"Siber güvenlik ve savunma problemini çok ciddiye alarak siber güvenlik pazarı ile kalkınmayı bile hedefleyen ülkeler gelişmiştir. ABD, Kore, Umman, Çin, Estonya, Malezya, Danimarka, Singapur ve Almanya bunun son örneği olarak verilebilir"* (Canbek, Sağıroğlu, 2006, s. 8). Bu noktada asıl amaç, siber dünyadaki suç, terör, savaş ve saldırılara karşı mücadelede başarılı olmak, farkındalığı artırmak, kümelenmeyi sağlamak ve siber ekonomi sektörünü geliştirmektir. Bunun için insan kaynağı yetiştirme, koordinasyon, işbirliği geliştirme, yetenek ve kapasite artırma, ar-ge çalışmaları gibi unsurlar da ön plana alınmaktadır.

Siber istihbarat faaliyetleri tarihçesi son yirmi yıl içerisinde gelişmeye başlamıştır. *"Siber istihbarat, istihbarat faaliyetleri yürütülürken devletin kontrol fonksiyonundan ötürü tehdidin seviyesine göre yakın ve uzak tehlikelerin engellenmesi amacıyla karar vericilere bilgi desteği sağlamak, propaganda, psikolojik harekât gibi örtülü operasyon yöntemleri ile olayları yönetmek ve düşman veya muhtemel düşmanın istihbarat faaliyetlerini engelleme faaliyetlerinin bütünüdür"* (Bayraktar, 2014, s. 16). Bu faaliyetler, istihbarat servislerinin yoğunlukla üzerinde durduğu alanlardır. Bunun yanında istihbarat servisleri, yalnızca açık kaynaklardan internet aracılığıyla yararlanmak için değil; aynı zamanda ağa bağlı bilgisayar sistemlerine gizlice girerek aleni olmayan bilgileri de bulabilmek için çalışmaktadırlar (Lewis, 2002, s. 17).

İstihbarat servisleri siber istihbarat oluştururken kendi yetiştirdiği personelini kullanabileceği gibi aynı zamanda daha zahmetsiz bir yol olarak bilgisayar korsanlarını da kendi casusları ve haber toplama elemanları gibi kullanabilmektedirler. *"Nitekim 1986 ile 1989 yılları arasında Doğu Almanya'daki bilgisayar korsanları ABD, Batı Avrupa ve Japonya'daki birçok askerî, bilimsel ve endüstriyel kurumun bilgisayarlara girerek parola, yazılım ve diğer bilgileri çalmış ve Sovyet gizli servisine satmıştır"* (Cordesman, 2001, s. 13). Bu açıdan siber istihbaratın günümüzde değer verilmesi gereken bir alan olduğu görülmektedir. Aslında siber istihbaratın kullanım alanı, saldırıların önlenmesi sürecinde de gerekli bir faaliyettir. Siber istihbari faaliyetlerin işleyişinin mükemmel olabilmesi, daha sonraki süreçlerin de düzgün ilerlemesini sağlar. Fakat her zaman her hizmet yüzde yüz verimle çalışamamaktadır. Bazı durumlarda yapılan bütün saldırılar en baştan önlenmiş olmaktadır. Fakat hiçbir güvenlik önlemi ve/veya ürünü kusursuz veya eksiksiz değildir. Ayrıca, hemen hemen her gün, işletim sistemleri, internet servisleri ve güvenlik uygulamalarında çeşitli açıklar tespit edilmektedir. Bu açıdan bakıldığında saptama ve karşılık verme süreçlerini verimli kullanmak önemlidir.

Türkiye gibi gelişmekte olan bir sermayeye sahip bir ülkede, ulusal güvenlik politikalarını destekleyici, her yönüyle milli olacak şekilde üretilmiş donanım ve yazılımları ile sağlanan siber istihbarat çalışmaları, refah ve barış ortamını oluşturabilir. Öncelikle kamu kurum ve kuruluşlarının bünyesinde oluşturulacak olan Siber Olaylara Müdahale Ekiplerinin sayısının arttırılarak, siber güvenliğe yönelik yasal mevzuat geliştirilmesi çalışmaları hızlandırılmalıdır. 'İyiler de en az kötüler kadar, kötü amaçlı bilgiye sahip olmalıdır' felsefesi ile siber güvenlik alanında edindikleri bilgileri iyi yönde kullanan uzman sayısının arttırılması gerekmektedir.

Siber istihbaratın yöntemleri bir taraftan kazanılan yetenekler doğrultusunda ülkeden ülkeye göre farklılıklar

gösterirken, bir taraftan da bilgi teknolojilerinin her geçen gün ilerlemesi sayesinde yeni yeni yöntemler keşfedilmektedir. Bununla beraber bu yöntemlere yönelik yeni siber savunma taktikleri de geliştirilmektedir. Siber istihbarat yöntemleri sistematik olarak siber uzayda bulunan aleni olmayan elektronik bilgilerin toplanmasını, değiştirilmesini ve engellenmesini içeren 'Siber Elektronik İstihbaratı da' içerir. Siber elektronik istihbarat, öncelikle devletlerin maruz kalabilecekleri siber tehditlere karşı durumsal farkındalıklarını arttıracaktır. Etkili bir siber istihbarat ile siber tehditlerin oluşturacağı riskler azalacak, siber saldırıları etkisizleştirecek yetenekler geliştirilebilecek ve inşa edilecek siber güvenlik yapılanmasında doğru ve zamanında bilgilendirilmiş istihbarat ile verimli ve maliyete olumlu etki edebilecek kararlar alınabilecektir. Etkili bir siber istihbarat ile siber tehditlerin oluşturacağı riskler azalacak, siber saldırıların etkilerini azaltacak yetenekler geliştirilebilecek ve inşa edilecek siber güvenlik yapılanmasında doğru ve zamanında bilgilendirilmiş kararlar alınacaktır.

DÜNYADA İSTİHBARAT FAALİYETLERİ

Globalleşen dünyada kurum ve kuruluşların ürettikleri mallara yönelik bilgi güvenliklerinin sağlanması konusu son yıllarda giderek önem kazanmaktadır. Kuruluşlar birbirlerinden izinsiz olarak verilerin aktarılması konusunda değişik yöntemler uygulamaktadırlar. İşletmelerde güvenilir olarak operasyonel faaliyetlerini sürdüren bilgi güvenliği konusu, genellikle riskleri ve tehditleri tespit etmenin çabukluğuna dayanır. Sistem açısından sorun teşkil eden tehlike ve risklerin önceden belirlenip bertaraf edilmesi ile veri kayıpları ile sistemin çökmesi vb. riskler de önlenmiş olur. Bununla birlikte, işletmenin faaliyetleri için kritik hale gelebilecek ciddi zaman kayıpları da söz konusu olabilir. Bu kayıpların önlenebilmesi için çok sayıda danışman firmalar ürettikleri yazılımlar ile piyasada hizmet vermektedirler. Görevleri ve bilgi raporlama formatı bakımından farklılık gösteren çok sayıdaki güvenlik sistemini kontrol etmek ve birbirleriyle entegre etmek neredeyse imkansızdır. Bankalar, iletişim işletmeleri ve değişik sektörlerdeki kurum ve kuruluşlar genellikle bu sorunla karşı karşıyadırlar. İşletmelerde bilgi güvenliğini sağlamak için çeşitli sistemler kullanılmaktadır. Bunların çoğu iş odaklı yani işle ilgili bilginin temin edilmesi, kullanılması, saklanması ve işin sürekliliğini sağlamaya yarayan verilerin depolanması ile ilgilidir. Bu çalışmaların ne ölçüde başarıldığına dair performans göstergelerine ihtiyaç vardır. Bu göstergeler de her kurum açısından gizli yani rakip işletmeler tarafından bilinmemesi gerekli olan istihbari bilgidir. İşle ilgili teknik, idari tüm göstergelerin verilerin sayısal değerlerini gösteren metrik verilerle ifade edilmesi gerekir. Metriklerin değerlendirilmesi ve analitik bilgilerin toplanması sistemler sayesinde otomatik olarak gerçekleştirilir. Metrik değerlerin doğru değerlendirilmesi kilit öneme sahiptir. Değerlendirmeler raporlamalar şeklinde düzenlenir ve karar vericilere sunulur. Bilgi güvenliğini sağlamak amacıyla yapay zekâ sistemleri de kullanılmaktadır. Bu tür sistemler yazılımlar vasıtasıyla daha verimli ve doğru veri seçimleri nedeniyle işletmenin yönetimsel kararlar alması konusunda yüksek avantajlara sahiptir. Raporlamalarda kullanılan grafikler, görselleştirmeler, çizelgeler, tablolar, infografiklerle anlaşılması kolay bir biçimde üst yönetim kademesine sunulabilir. Sonuç olarak, bilgi güvenliği süreçleri daha şeffaf ve daha anlaşılabilir hale gelir.

İşletmelerin istihbarat amaçlı birbirlerinin sistemlerine müdahale etmesi, yasa dışı olarak veri veya bilgisayar programlarının girilmesi, değiştirilmesi, silinmesi, işletmenin ekonomik zararı ile sonuçlanacak veri kayıpları ile açıklanabilir. Bu müdahalelerin temel nedeni serbest piyasa koşullarında birbirlerine karşı üstünlük kazanıp ekonomik fayda elde etmektir. İşletmelerin teknolojik bir ürüne ait teknik detayları izinsiz olarak ele geçirmesi ve üretmesi bu konuya örnek olarak verilebilir. Bir ürünün

yasadışı çoğaltılması, ürünün ticari amaçla kullanımı suç teşkil etmektedir. Bu suç durumu, 'endüstriyel rekabetçi istihbarat' kavramı ile de açıklanabilir.

Ülkeler ekonomilerinin gelişmesi ve diğer rakiplerinin önüne geçebilmesi amacıyla ekonomik önleyici tedbirlere başvururlar. Ekonomik açıdan ülkenin büyümesi, vatandaşlarının refah içinde yaşaması, bunun için de gerekli büyüme koşullarının oluşturulması önem kazanmaktadır. Bu koşullardan bazılarına yolsuzluğun azaltılması, bürokrasinin azaltılması, verimliliğin artırılması, dijital ekonomik modellerin geliştirilmesi, dünya ile rekabet edebilir inovasyon sistemlerinin geliştirilmesi bu şekilde de ulusal ekonominin rekabet gücünün artırılması örnek olarak verilebilir. İşlemlerde hız ve dakikliğin beklendiği bir çağda sorunların da çözümünün hedeflendiği politikaların geliştirilmesi gereklidir. Vatandaşların kişisel ve işletmelere yönelik güvenlik sistemlerinde de iyileştirmelere gidilmelidir.

Global ölçekte rakip firmalar, mevcut olan faaliyetlerinde kullanmak üzere diğer firmalardan bilgi ve veri alabilirler. Birbirlerinin iş süreçleri ve geliştirdikleri ürünleri hakkında bilgi toplamak yasalara aykırı bir eylem olup, rekabetçi istihbarat tanımına girmektedir. İşletmelerde genel olarak ekonomik ve teknolojik veriler daha önemli görülmektedir. Dolayısıyla, işletmeler rekabetçi durumları arttırabilmek açısından ekonomik ve teknolojik yatırımlar yapmaktadırlar. *"Ayrıca, işletmeler rakiplerine ilişkin verilerden en çok satış politikaları, satış fiyatları ve üretim maliyetlerine ilişkin verileri önemli bulmaktadırlar. Bu tür veriler elde edilmesi halinde, rakibe finansal olarak en çok zarar verebilecek veriler arasındadır"* (Seviçin, 2005, s. 7). Farklı kaynaklardan verilerin toplanması ve işlenmesinde rakiplerin faaliyetlerini incelemek, rakiplerin zayıf yönlerinin belirlenmesi, rakiplerin olası eylemlerini tahmin etmek, yeni pazarların araştırılması ve değerlendirilmesi, piyasalardaki değişiklikleri tahmin etmek vb. verileri elde etmek önemlidir. Bilgi güvenliği için bilimsel desteğin gerekli bir unsuru olarak, hedeflenen temel ve uygulamalı araştırma sisteminin oluşturulması, devlet desteğinin teşvikler sayesinde sağlanması, araştırma ve eğitim kurumları ağının ve yapılacak ortak çalışmaların genişletilmesi önemlidir. Bununla beraber, alan profesyonellerin eğitimi, modern dijital teknolojilerin ve gelecek vaat eden bilimsel yoğun modellerin geliştirilmesi de öncelikle ele alınması gereken konulardır.

Modern dijital teknolojilerin günümüzde dünyanın en büyük sorunu durumuna gelen Covid-19 pandemisinde de önem kazandığı görülmektedir. Özellikle 2021 yılı içerisinde 'aşı çalışmaları' konusunda ciddi bir rekabet baş göstermiştir. Çin ve Rus istihbarat ajanlarının, ilaç şirketlerinin peşine düşmek yerine; daha kolay hedef olabilmesi açısından salgın konusunda verimli araştırmalar yapan Kuzey Carolina Üniversitesi ve diğer eğitim kurumlarında dijital keşif yaptığı belirtilmektedir. New York Times'ın haberine göre istihbarata yakın bazı yetkililer Çinli internet korsanlarının, Dünya Sağlık Örgütü'nün (DSÖ) geliştirilen aşılara dair topladığı verileri de gizlice kullandığını öne sürmektedir. Rusya'nın önde gelen istihbarat servisi S.V.R ise ABD, Kanada ve İngiltere'deki aşı araştırma ağlarını hedef almıştır. Rusya'nın faaliyetleri ilk olarak uluslararası fiber optik kabloları izleyen bir İngiliz casus teşkilatı tarafından tespit edilmiş ve İngiliz, Amerikan ve Kanada istihbarat servislerinin açıkladığına göre Rus istihbaratı öncelikli olarak, Oxford Üniversitesi'nin ve eczacılık partneri Astra Zeneca'nın araştırmalarına odaklanmıştır. Öte yandan ABD ise, kendi istihbarat servislerinin çalışmalarının tamamen savunma amaçlı olduğunu söyleyerek diğer ülkelerin koronavirüs araştırmalarına yönelik herhangi bir casusluk girişiminde olmadığını savunmuştur. Ancak yetkililer, Amerikan istihbarat ajanlarının Rusya, Çin ve İran'ın herhangi bir bilgi çalıp çalmadığını araştırırken bu ülkelerin araştırmalarına ulaşmış olabileceğini kaydetmiştir ("Covid Aşısı", 2021).

Bunun yanında Covid-19 aşılarının teknik bilgilerine çeşitli yöntemlerle ulaşabilecek olan devlet dışı unsurların da dünyadaki barış açısından tehlikeli olacağı açıktır. Örneğin Filistin'de silahlı mücadele içinde olan Hamas'ın destekçilerinden olan Muhammet Dahlan'ın destekçilerinin Gazze'de insani yardım ve yardım projeleri yürüttüğü bilinmektedir. Bu durum, bölgelerindeki rakip gruplara oranla daha fazla şiddet suçları işleyebilmesi açısından teşvik edici bir durum haline gelmiştir. Hamas'ın politikaları ve kaynakların kaba yanlış yönetimi nedeniyle bölge zaten yoksulluk içindedir. Filistin lideri Abbas, halkı için aşı temin etmek için mücadele etmeye devam ederken, aşıların beklenen teslimatı Dahlan'ın bölgedeki konumunu daha da artırabilecek unsurları içerisinde barındırmaktadır ve durum bu açıdan da tehlikeli bir hal almaktadır ("Muhammet Dahlan", 2021).

Günümüz itibariyle ise, siber güvenlik uzmanları çok daha tehlikeli gelişmelerin baş gösterebileceğini ön görmektedirler. Biyoterörist olarak adlandırılan kişilerin, virüsler üzerinde çalışma gerçekleştiren biyologların bilgisayarlarına sızarak saldırı gerçekleştirebileceği açıklanmıştır. Uzmanlar, bu saldırıların gerçekleşmesi durumunda dünyada korona virüs salgınından daha tehlikeli durumlar oluşabileceği ihtimali üzerinde durmaktadırlar. ABD Sağlık ve İnsan Hizmetleri Bakanlığı, potansiyel açıdan zararlı DNA'ları tarayarak tespit etmek için bazı protokoller uygulamaktadır. Ancak araştırma ekibi, gizleme yoluyla bu protokolleri atlamayı başarmış ve gizlenmiş 50 DNA örneğinden 16'sının tespit edilemediğini ortaya koymuştur. Araştırmacılara göre bu tür zayıflıklar başka etkenlerle de birleşince, kötü amaçlı yazılımın, kurbanın laboratuvarındaki biyolojik süreçlere müdahale etmesine neden olabilme ihtimali vardır. Siber saldırıya uğrayan ve durumun farkında olmayan bir bilim insanının, gelecekte korsanlarca değiştirilen DNA'yı diğer dizilerle bir araya getirdiği farz edilebilir. Bunun ardından, örneğin gen düzenleme işlemlerinde sıklıkla kullanılan Cas9 gibi bir proteinin kötü amaçlı diziden gRNA'yla bir araya gelerek, sentetik virüsler veya toksik kimyasallar dahil olmak üzere bir dizi tehlikeli madde oluşturabileceği belirtilmiştir. Sentetik DNA tedarik zincirini siber saldırganlara karşı korumak gerekmektedir ("Biyoterörizm", 2021).

Türkiye de de aşı çalışmalarında önemli çalışmalar ortaya koyulmuştur. 2021 yılının başında aşı çalışmaları geliştirilmiş ve tüm ülkede öncelikle sağlık personelinin aşılanması çalışmaları yapılmış (1 milyona yakın sağlık çalışanı) ve 2021 yılı içerisinde tüm Türkiye vatandaşlarının aşılanması için gereken uygulanmaların da hızlandırılacağı ön görülmektedir.

Aşı çalışmalarının diğer ülkelerin istihbarat teşkilatları tarafından zarar görmemesi için her türlü istihbarat ve güvenlik önlemleri alınmalıdır.

Türkiye Cumhuriyeti, dünya jeopolitiğinde güncellenen ve belirlenen versiyonuyla İç ve Dış Güvenlik Esasları'nı ön plana alan yeni bir milli istihbarat sistemi oluşturmalıdır. Bu sistem, ülkemizdeki tüm istihbarat kuruluşlarının stratejik ve yönetimsel liderliğini, genel güç konfigürasyonu aracılığıyla gözlemciliğini yapma misyonunu yürütebilir. Zira, Covid-19 salgını göstermiştir ki, çok yakında su yüzüne çıkacak olan yeni dünya dengelerinde sürprizler ve ezber bozan gelişmeler her zamankinden daha fazla olacaktır. Bu tür ani ortaya çıkabilecek olan olumsuz durumlardan ülkelerin korunabilmesi için istihbarat faaliyetlerinin sadece fiziki terörizmi değil; biyoterörizm tehlikelerini de bertaraf edebilecek çalışmaları ön plana alması gerekmektedir.

SONUÇ ve ÖNERİLER

Global dünyada ülkeler arası ticaret açısından işletmeler arası rekabete dayanan bir piyasa ekonomisi yaşanmaktadır. Tüm işletmeler rakiplerine göre daha

ileride olmak için çaba harcamaktadır. Sadece işletmeler arasında değil, ülkeler arasında da askeri ve politik amaçlı istihbarat toplanarak toplumların değerleri, kültürleri ve talepleri değiştirilmeye çalışılmaktadır. Bilgiye sahip olan işletmelerin, ülkelerin diğerlerine nazaran daha önde olduğu gözlemlenmektedir. Herhangi bir işletme için rakipleri hakkında güvenilir bilgilere sahip olmak son derece önemlidir. Birbirlerinden bilgi ve veri elde etme yöntemleri farklı ve yasal ya da illegal yöntemler olabilir.

Kanunla korunan ticari, resmi veya sair sır teşkil eden bilgilerin yasa dışı alınması, kullanılması, ifşa edilmesi, ticari faaliyetlerde menfaat elde edilmesi, emek, zaman ve paradan tasarruf etme gibi amaçlarla yapılan endüstriyel istihbarat ile rekabetçi istihbarat işletmeler tarafından tercih edilen yöntemlerdir. Bu haksız rekabet biçiminin yasal mevzuata göre suç teşkil eden kriminolojik yönlerinin açığa çıkarılması gerekmektedir. Çalınan bilgi birikimi ile mağdur durumda olan işletmelerin hakları yasal düzenlemelerle korunmalıdır. Buna ilaveten savunma sanayinde meydana gelen endüstriyel istihbarat konularında devletin ulusal güvenliğini tehdit etmesi açısından uluslararası hukuka giren konular bulunmaktadır. Bu istihbaratı sağlayanlar yabancı devletlerin istihbarat aracı olup, o ülkelerin çıkarlarına hizmet etmektedirler. Endüstriyel istihbarat, kamuya açık olmayan ve kanunla korunan bilgileri elde etmeyi amaçlarken, rekabetçi istihbarat çoğunlukla açık kaynakları kullanır. Bu açık kaynak bilgileri internet, medya kuruluşları, derecelendirme kuruluşları, işletme raporları ve analizleri gibi bilgileri kullanabilir. Bilginin korunması açısından yasal tedbirler üzerinde durulmalı, yüksek teknolojiler alanında genel sosyal suç önleme politikaları geliştirilmelidir. Bilgi güvenliği için sadece ulusal değil, ikili ve çok taraflı devletler arası anlaşmalar da yapılmalıdır. Suçla mücadelede kolluk kuvvetlerinin faaliyetlerini engelleyen yasal engellerin giderilmesi; mevcut mevzuatın uygulanmasındaki problemler ve iyileştirmeler/güncellemeler, kriminolojik açıdan mevcut sorunların incelenmesi ve sorunların bertaraf edilmesi için mekanizmaların oluşturulması, bilgi güvenliğine yönelik suçlara karşı mücadelenin en etkin şekilde yapılmasını sağlayacaktır. Tüm bu olumlu/olumsuz potansiyellerden korunabilmek amacıyla bilgi güvenliğine önem vererek çalışmalarına devam eden devlet kuruluşları ve/veya özel işletmelerde, özellikle yerli ve milli güvenlik yazılımı programları kullanılmalı, veri güvenliği açısından yerli kriptolama programlarının sürekli güncelleştirilmesi sağlanmalıdır. Bu doğrultuda 'Türkiye Cumhuriyeti Cumhurbaşkanlığı Dijital Dönüşüm Ofisi Bilgi ve İletişim Güvenliği Rehberi'ne (Temmuz 2021)[2] uygun şekilde hizmetler sürekli takip edilmelidir.

Rakiplerine göre herhangi bir avantaj elde etmek, daha ileride olmak amaçlı yapılan bu tür faaliyetlerde yürürlükte olan yasalar da ihlal edilebilir. Gelişen internet teknolojileri ile de ticari sırların saklanması giderek zorlaşmaktadır. Rekabetçi istihbarat teknikleri konusunda işletmelerin eğitilmesi ile bu ihlallerin önüne geçilebilecektir. Kontrol, izleme, denetim gibi güvenlik stratejilerinin ciddiyetle uygulanması gerekir. Sızıntıların kaynağı işletme içindeki personelden de kaynaklı olabilir. Oldukça uzun ve zahmetli süreçlerle oluşturulan patentlerin tecili, ticari sırların korunması için işletme içinde de sıkı bir denetim sistemi getirilmelidir. Rekabetçi istihbarat kapsamında taleplerin toplanması, rakiplerin, iç ve dış paydaşların belirlenmesi, amaç ve hedeflerin tanımlanması ve diğer tüm konularla ilgili bilginin kullanılması ve yönetilmesi zorunludur. Ancak bu yönetim sırasında çalışma kapsamında da belirtildiği üzere bilginin güvenliği ön planda değerlendirilmelidir. Uzun vadeli stratejilerin oluşturulması, dış çevre hakkında belirli bilgilerin kullanılmasını zorunlu kılar. Kaynakların kıt olduğu veya örgütün ağırlıklı olarak çevreye bağımlı

[2] https://cbddo.gov.tr/SharedFolderServer/Genel/File/bg_rehber.pdf

olduğu durumlarda, istihbarat toplama, yorumlama vb. faaliyetlerin işlevine daha fazla kaynağın tahsis edildiği görülecektir. Dolayısıyla dış çevreye ilişkin bilgilerin sağlanması, işlenmesi, analizi ve dağıtılması ise daha bütüncül bir yaklaşım öneren rekabet istihbaratı ile mümkündür. Küresel fırsatları takip etmede rekabet istihbaratına önem vermeyen ve bu alanda başarısız olan işletmeler güçlü küresel rekabet tarafından kenara itileceklerdir.

ÇIKAR ÇATIŞMASI BEYANI

Yazarlar ve/veya herhangi bir akademisyen grubuyla, herhangi bir çıkar çatışması bulunmamaktadır.

ETİK KURUL VE İNTİHAL TAKİBİ

Bu çalışma, insanlardan veri ve örnek toplamayı gerektiren, anket, inceleme, alan çalışması ve deney içeren araştırmalar kapsamına girmediğinden ‘etik kurul onay belgesi’ gerektirmemektedir.

Makalenin intihal takibi yapılmıştır.

KAYNAKÇA

Akman, K. (2019). "Bilgi sosyolojisi açısından istihbarat kaynaklarının tasnifi ve değerlendirilmesi". *Ankara Üniversitesi Sosyal Bilimler Dergisi*, *10*, 24- 42.

Baykara, M., Daş, R., Karadoğan, İ. (2013). "Bilgi güvenliği sistemlerinde kullanılan araçların incelenmesi". *1. Uluslararası Dijital Adli Tıp ve Güvenlik Sempozyumu (ISDFS'13) 20-21 Mayıs 2013.* Elâzığ: Elâzığ Üniversitesi.

Bayraktar, G. (2014). "Harbin beşinci boyutunun yeni gereksinimi: Siber istihbarat". *Güvenlik Stratejileri Dergisi*, *10*(20), 118-148.

Bensghir, T. K. (2011). "Bilgi sistemleri ve bilgi yönetimi". *TODAİE E-Devlet Merkezi Bilgi Yönetimi Semineri.* Ankara: TODAİE Yayınları.

Biyoterörizm, (2021) Uzmanlar dünyayı bekleyen koronadan daha beter yeni tehlikeyi açıkladı. https://www.yenicaggazetesi.com.tr/koronadan-bile-daha-beter-uzmanlar-dunyayi-bekleyen-yeni-tehlikeyi-acikladi-319369h.htm (04.04.2021)

Carl, L. D. (1990). *International Dictionary Intelligence*. V.A.: Maven Books.

Canbek, G., Sağıroğlu, Ş. (2006). "Bilgi, bilgi güvenliği ve süreçleri üzerine bir inceleme". *Politeknik Dergisi, 9*(3), 165-174.

Cordesman, A. H. (2001). "Cyber-threats, information welfare and critical infrastructure protection: Defending the U.S. homeland". *Praeger Connecticut*, *1*(18),18.

Covid-19 Aşısı, (2021). Aşıda istihbarat savaşları soğuk savaş dönemindeki uzay yarışına döndü. https://www.yenisafak.com/koronavirus/asida-istihbarat-savaslari-ortalik-soguk-savas-donemindeki-uzay-yarisini-dondu-3556135 (05.03.2021)

Çifci, H. (2013). *Her yönüyle siber savaş*. Ankara: TÜBİTAK Popüler Bilim Kitapları.

Dazahra, M. N., Elmariami, F., Belfqih A., Boukherouaa J., (2018). "A defense-in-depth cybersecurity for smart substations". *International Journal of Electrical and Computer Engineering (IJECE)*, *8*(6), 4423-4431.

Dedeoğlu, B. (2003). *Uluslararası güvenlik ve strateji*. İstanbul: Derin Yayınları.

Gibbons, M. vd. (1994). *The new production of knowledge: The dynamics of science and research in comtemporary societies*. London: Sage Publications.

Kandemir, R., Şahinaslan Ö. (2009). "Bilgi güvenliği farkındalık eğitim örneği". *Akademik Bilişim'09 - XI. Akademik Bilişim Konferansı Bildirileri 11-13 Şubat 2009*. Şanlıurfa: Harran Üniversitesi.

Lewis, J. A. (2002). *Assessing the risks of cyber terrorism, cyber war and other cyber threats*. Washington: Center for Strategic and International Studies. https://csis-website-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/media/csis/pubs/021101_risks_of_cyberterror.pdf (08.03.2021)

Muhammet Dahlan, (2021). *Abbas rival woos Gazans With corona vaccines*. https://worldisraelnews.com/abbas-rival-woos-gazans-with-corona-vaccines/ (08.04.2021)

Özalp, A.N., Asker, A. (2017). "Devletin güvenlik politikalarında siber istihbaratın rolü ve önemi". *19. Akademik Bilişim Konferansı 8-10 Şubat 2017.* Aksaray:

Aksaray Üniversitesi.

Özer, Y. (2015). "Terörizmle mücadelede istihbaratın rolü: Kültürel istihbarat konsepti". *İGÜSBD*, *Nisan 2(1)*, 51-80.

Özer, Y. (2018). "Yeni bir istihbarat paradigması: Kültürel istihbarat". *21. Yüzyıl Türkiye Enstitüsü Dergisi*, *Nisan 2(1),* 60-70.

Salleh, K.A., Janczewskia, L. (2016). "Technological, organizational and environmental security and privacy issues of big data: A literature review". *Conference on ENTERprise*

Information Systems / International Conference on Project Management / Conference on Health and Social Care Information Systems and Technologies, CENTERIS / ProjMAN / HCist 2016. Porto: Procedia Computer Science.

Saydam, A. (2010). *İletişimin akıl ve gönül penceresi algılama yönetimi*. İstanbul: Rota Yayınları.

Seren, M. (2017). *Stratejik istihbarat ve ulusal güvenlik*. Ankara: Orion Kitabevi.

Seviçin, A. (2005). "Türkiye'de ilk 500'e giren işletmelerde rekabetçi istihbarat sistemi uygulamalarına ilişkin bir araştırma". *H.Ü. İktisadi ve İdari Bilimler Fakültesi Dergisi*, *23*(2), 181-205.

Sun Y., Zhang J., Xiong Y., Zhu G. (2014). "Data security and privacy in cloud computing". *International Journal of Distributed Sensor Networks*, *6*(50), 1-9.

Şeker, Ş. E. (2013). *İş zekâsı ve veri madenciliği*. İstanbul: Cinius.

The American Heritage Dictionary of the English Language, (2021). *Intelligence*.

Türk Dil Kurumu Sözlüğü, (2021). *İstihbarat terimi*.

Türkiye Cumhuriyeti Cumhurbaşkanlığı Dijital Dönüşüm Ofisi Bilgi ve İletişim Güvenliği Rehberi (2021), *Rehber*. https://cbddo.gov.tr/SharedFolderServer/Genel/File/bg_rehber.pdf (28.02.2021)

Ullah I., Lane C., Buda S., Drury B., Mellotte M., Assem H., Madden M. (2020). "Classification of cybercrime indicators in open social data". *Conference: 7th International Conference on Information Management and Big Data.* Peru: Lima.

Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı (2021). Plan. https://www.btk.gov.tr/uploads/pages/2-1-strateji-eylem-plani-2013-2014-5a3412cf8f45a.pdf (18.03.2021)

Warner, M. (2007). *Sources and methods for the study of intelligence*. ABD: Johnson Sons Limited.

Wunderle, W. (2007). *Through the lens of cultural awareness: A premier for US Armed Forces deploying to Arab and Middle Eastern Countries*. Kansas: Combat Studies Institute Press.

Yılmaz, M. (2009). "Enformasyon ve bilgi kavramları bağlamında enformasyon yönetimi ve bilgi yönetimi". *Ankara Üniversitesi Dil ve Tarih-Coğrafya Fakültesi Dergisi*, *49*(1), 95-118.

Extended Abstract

Providing information, processing, analyzing, obtaining results, designing future plans according to results etc. the main goal that important transactions want to achieve is to get any advantage over competitors and to be further ahead. In some cases, these laws may be violated as the laws in force in such activities are used. With developing internet technologies, it is increasingly difficult to keep trade secrets. By training businesses on competitive intelligence techniques, these violations can be prevented. Security strategies such as control monitoring, audit need to be implemented seriously.

The source of the leaks may also be from personnel within the enterprise. A strict audit system should also be introduced within the enterprise in order to defer patents created by fairly long and laborious processes and to protect trade secrets. As part of competitive intelligence, it is mandatory to collect requests, identify competitors, internal and external stakeholders, define goals and goals, select data sources and use and manage information related to all other issues. But during this administration, as stated in the scope of the study the security of information should be evaluated at the forefront. In order to ensure corporate information security, joint work should also be carried out with expert stakeholders. In order to ensure sustainable profitability, businesses should follow the market, recognize the competitive environment in which they are located, and become active players in this environment by developing appropriate strategies.

Monitoring the competitive environment is an essential component in strategy development as a strong strategic path requires realistic assumptions about the behavior of competitors and their reactions to the strategic moves of the enterprise.

The creation of long-term strategies obliges the use of certain information about the external environment. Where resources are scarce or the organization is heavily dependent on the environment, intelligence gathering, interpretation etc. it remains to be seen that more resources are allocated to the function of the activities. Therefore, the provision, processing, analysis and distribution of information about the external environment is possible with competition intelligence, which suggests a more holistic approach. Businesses that do not care about competitive intelligence in pursuing global opportunities and fail in this area will be pushed aside by strong global competition.

With this research, it was observed that the relationship between intelligence and information security and information access is intertwined and that they are also positively influenced by technological developments. From this point of view, a valuable contribution has been made to his literature on intelligence.