

BİLGİ YÖNETİM SİSTEMLERİ VE SİBER GÜVENLİK

*Ahmet Naci ÜNAL**

Makale Geliş Tarihi-Received: 29.05.2018
Makale Kabul Tarihi-Accepted: 12.11.2018

ÖZ

Bilgi; düşünme, yargılama, akıl yürütme gibi işlemler sonucunda elde edilen kapsamlı bir sürecin ürünüdür. Yoğun veri ortamında karar vermek güçleşerek, karmaşıklaşmaktadır. Genelde uzman sistemlerin, özelde ise Yönetim Bilgi Sistemleri'nin etkin kullanımı insan kaynaklı hataların en aza indirilmesini sağlamaktadır. Bu sistemler kullandıkları veriyi siber uzaydan toplamaktadır. Bu çalışmada siber güvenlik kavramına dikkat çekilerek, siber uzayda güvenli bilgi kullanımı ile alınması gereken önlemler üzerinde durulmaktadır.

Anahtar Kelimeler: Bilgi Sistemleri, Uzman Sistemler, Yönetim Bilgi Sistemleri, Karar Destek Sistemleri, Siber Güvenlik.

JEL Kodları: L86, M15, O32

375

IJSI 11/2
Aralık
December
2018

* Dr. Öğr. Üyesi, Bahçeşehir Üniversitesi, Mühendislik ve Doğa Bilimleri Fakültesi, Yazılım Mühendisliği Bölümü, İstanbul/Türkiye.
ahmetnaci.unal@vs.bau.edu.tr

KNOWLEDGE MANAGEMENT SYSTEMS AND CYBERSECURITY

ABSTRACT

Information; is a comprehensive product of a process obtained from thinking, judging, and reasoning. Deciding in an intensive data environment becomes difficult and complicated. The effective use of expert systems in general and management information systems in particular reduces human errors. These systems collect data from cyberspace. In this study, attention is paid to the concept of cyber security, and the precautions to be taken regarding safe information use in cyber space are emphasized.

376

IJSI 11/2
Aralık
December
2018

Keywords: Information Systems, Expert Systems, Management Information Systems, Decision Support Systems, Cyberspace, Cyber Security.

JEL Codes: L86, M15, O32

GİRİŞ

Yönetim kavramı; insanların yaşam döngülerinde yer alan önemli etkenlerden biri olarak karşımızda çıkmaktadır. Bu kavram; insanlık için önemli bilim dallarından biri olmanın yanı sıra gelişen teknolojiyi kullanan disiplinlerarası bir yapı olarak da gelişimini sürdürmektedir. Bu gelişim en küçük organizasyon olarak gösterebileceğimiz aile yapısından, uluslararası şirket yapılarına kadar oldukça büyük ve birbirlerinden farklı alanlardaki faaliyetleri de kapsamaktadır.

Ülgen, Mirze (2014: 23) “Yönetim; bir işletmenin veya örgütün amaçlarını gerçekleştirmek için sahip olduğu üretim kaynaklarını (doğal kaynaklar, insan kaynakları, sermaye, hammadde, makineler vs.) etkili ve verimli olarak kullanması süreci olarak tanımlanmaktadır.”

Koçel (2010: 59) ise “başkaları vasıtasıyla iş görme” diye kısa tanımını vermektedir. Her iki kaynaktan yönetim sürecini; plânlama, organize etme, uygulama, koordine etme ve kontrol etme şeklinde belirtmektedirler.

Yönetici ise “kâr ve riski başkalarına ait olmak üzere, üretim faktörlerinin bilinçli ve sistemli olarak birleştirilmesini sağlayan ve bunların belli bir ihtiyacı karşılamak amacıyla yönelten kişi” olarak tanımlanmaktadır (Efil, 2002: 5-7).

Bu tanımlardan yola çıktığımızda her tür işletmede yönetim sürecinin gerçekleştirilmesinin yönetici iradesine ya da başka bir ifadeyle yönetici tarafından alınan karara bağlı olduğunu görmekteyiz. Bu kapsamda karar; Yarman, Ünal (2015: 11) tarafından “herhangi bir alanda sonuca bağlanması gereken bir iş veya bir meseleyi, ferdi ya da grup olarak tartışmak suretiyle varılan kesin hüküm olarak” tanımlanmaktadır. Karar verme ise Harrison’a (1995: 4) göre “belirlenen bir amaca ulaşabilmek için, yerine getirilmesi söz konusu olabilecek birçok eylemli seçenekler içinden birini seçme işlemine karar verme” şeklinde tanımlanırken, Holsapple (2008: 26) tarafından da “n tane alternatif hareket tarzının tespit edilmesi ve içlerinden birinin karar olarak seçilmesi eylemidir” şeklinde tanımlanmaktadır. Tüm bu tanımlamalardan yola çıkıldığında ise karar vermenin özellikleri “karar veren kişi veya kişilerin olması, karar verici(ler)

tarafından belirlenecek bir amaç olması, karar vericiyi bu amaca ulaştırabilecek çok eylemli seçenekler kümesi olması, seçenekler kümesi içinden seçme işleminin yapılabilmesi için ölçütlerin olması ve sistematik bir seçme yönteminin olması" şeklinde özetlenebilmektedir (Yarman, Ünal, 2015: 13).

Yönetim süreci ile karar verme olgularını; sağlıktan, eğitime, enerjiden, ulaşım, finanstan güvenliğe kadar pek çok alanda ve sektörde kullanabilmek mümkündür.

Günümüzde artan bilgi üretimi ve giderek karmaşıklaşan yönetimsel veriler düşünüldüğünde karar verebilmek için veri, enformasyon ve bilgi gibi kavramlar öne çıkmaktadır.

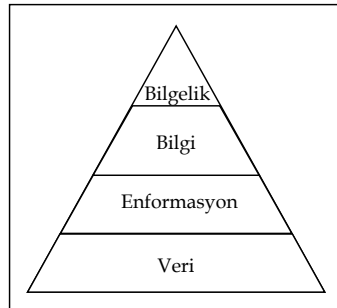
378

IJSI 11/2
Aralık
December
2018

1. VERİ VE VERİNİN EVRİMLEŞME SÜRECİ

İnsanoğlu ürün yetiştirmeye başladığı andan itibaren ürününü depolamak zorunda kalmış, depoladığı ürüne sağlam olarak erişmek istemiş ve eriştiği ürünü dönüştürerek çeşitli mamuller elde etmiştir. Bu süreç "Tarım Toplumu" olarak adlandırdığımız süreçte gerçekleşmiştir. Günümüz bilgi toplumunda ise veri, enformasyon ve bilgi gibi terimler ön plâna çıkmaktadır. Vercellis (2009: 6) veriyi; bir olgunun yapısal kodu olarak ifade ederken, Stair ve Reynolds (2009: 4); düzenlenmiş niteliklerin (verilerin) toplamını "enformasyon" olarak tanımlamakta ve Holsapple (2008: 22) da bilgiyi kararların verilmesinde kullanılan ana madde olarak ifade etmektedir.

Şekil 1: Bilginin Oluşum Süreci

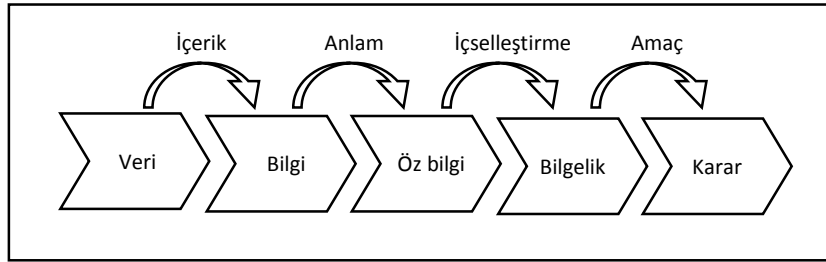


Kaynak: (Sanders, 2016: 2)

Şekil 1’de gösterildiği gibi veriler belirlenmiş amaç ya da amaçlar için işlenerek enformasyona, enformasyon geliştirilerek bilgiye ve bu bilgi de kullanılarak bilgeliğe dönüştürülmektedir. Bu dönüşüm kapsamında; bilgiye erişilmesi, bilginin işlenmesi ve bilginin depolanması (saklanması) süreçleri ön plana çıkmakta ve mevcut bilgi bizzat kullanılmakta ya da kullanılmak üzere başka alanlara iletilmektedir.

Özellikle 20’nci yüzyılın son çeyreğinde bilgi sistemlerinin aktif kullanılmaya başlaması ve 1990’larda internetin ticarileşerek sivilleşmesi; verinin evrimleşerek dönüşmesine sebep olmuştur. Bu dönüşüm süreci Şekil 2’de gösterilmiştir.

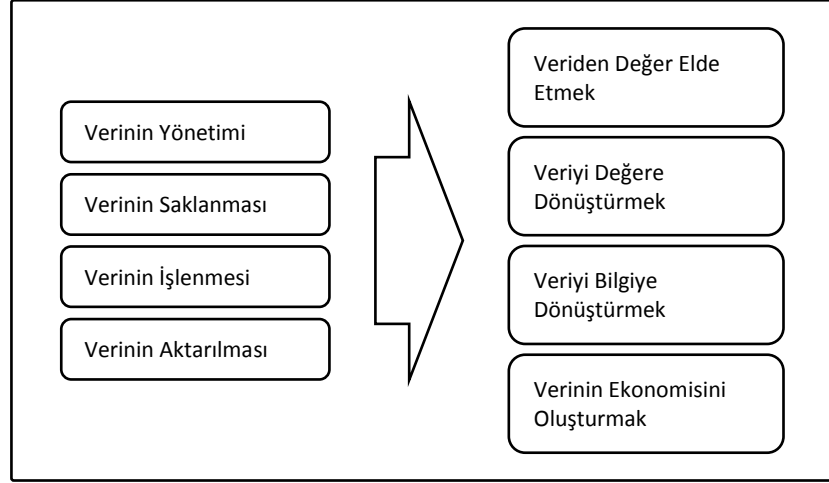
Şekil 2: Verinin Evrimleşerek Dönüşümü



Kaynak: (Terzi vd.,2017: 15)

Şekil 2’de verinin evrimleşme sürecine yönelik sistem mimarisi görülmektedir. Burada veri; bilişim teknolojisi açısından, anlamlı hale dönüştürülmemiş bitleri ifade etmektedir. Verinin belli bir anlam ifade edecek şekilde işlenip, belirsizliğinin azaltılmasıyla da bilgi elde edilmektedir. Bilginin, tecrübe veya öğrenme ile algılanmasıyla öz bilgi oluşurken, öz bilginin nasıl kullanılacağını kavramak bilgelik olarak tanımlanmaktadır. Amaca ulaşabilmek için elde edilen çözümün elemanlarını içeren seçeneklerin seçilerek uygulanması da kararı oluşturmaktadır (Terzi vd., 2017: 15). Tüm bu süreç incelendiğinde ise Şekil 3’te gösterilen girdilerin sebep olduğu çıktılar elde edilmektedir.

Şekil 3: Verinin Evrimleşmesinin Sonuçları



380

IJSI 11/2
Aralık
December
2018

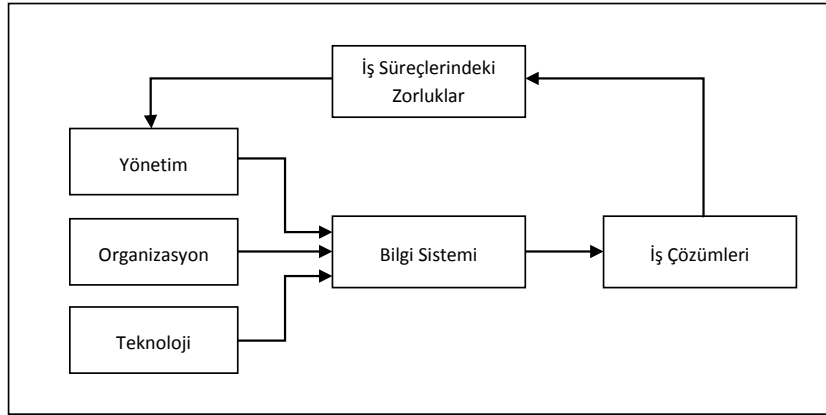
Bu evrimleşme sürecinde verinin; yönetimi, saklanması, işlenmesi ve aktarılması gibi girdilere bağlı olarak mevcut veriden değer elde etmek, veriyi değere dönüştürmek, veriyi bilgiye evirmek ve veriyi ekonominin bir parçası haline getirmek amaçlanmaktadır (Terzi vd., 2017: 14).

Günümüz teknolojik gelişim ve dönüşüm süreçlerinin de etkisiyle üretilen bilgi katlanarak artmaktadır. Dolayısıyla bilginin yönetimi için bilişim teknolojilerinde yoğun olarak kullanılmak gerekmektedir.

2. BİLGİ SİSTEMLERİ VE GELİNER BOYUT

Bilgi Sistemi (BS) dediğimiz kavram; Şekil 4'te de gösterildiği gibi tüm yönetim süreçlerinde yer alan yönetim, organizasyon ve teknoloji bileşenleriyle doğrudan ilişkili olan ve bu sayılan faktörler arasında doğrudan koordinasyon sağlayabilen, örgütün işleyişine yardımcı olan sistemlerdir.

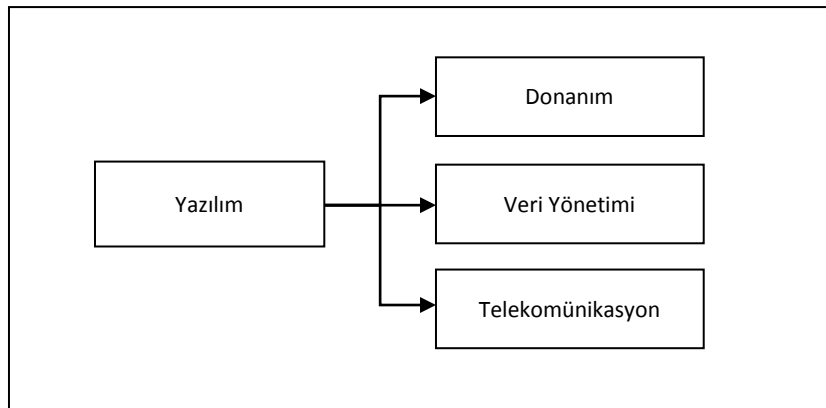
Şekil 4: Bilgi Sistemi Temel İşleyiş Mimarisi



Kaynak: (Laudon, Laudon, 2014: 22)

Bu temel işleyiş mimarisi incelendiğinde; yönetim, organizasyon ve teknoloji bileşenleri BS'nin girdilerini oluşturmaktadır. Sistem çıktıları ise iş çözümleri olarak karşımıza çıkmaktadır. Bu süreçte, çıktıların niteliksel değerlerinin artırılması ise yönetime yapılan geri besleme ile sağlanmaktadır.

Şekil 5: Bilgi Sistemi Temel Sistem Mimarisi



Kaynak: (Laudon, Laudon, 2014: 43)

BS'lerin temel sistem mimarisi ise Şekil 5'de gösterilmiştir. Bu mimari yapı incelendiğinde; donanım, veri yönetimi ve iletişimin yazılım tarafından yönetildiği görülmektedir. Yazılımın karakteristik özellikleri ise kullanıcının BS'yi kullanım amacına göre şekillenmektedir. Bu kapsamda, en çok kullanılan BS'ler; Uzman Sistemler (US), Yönetim Bilgi Sistemleri (YBS) ve Karar Destek Sistemleri (KDS) olarak özetlenebilir. Bu sistemleri incelediğimizde:

2.1. Uzman Sistemler

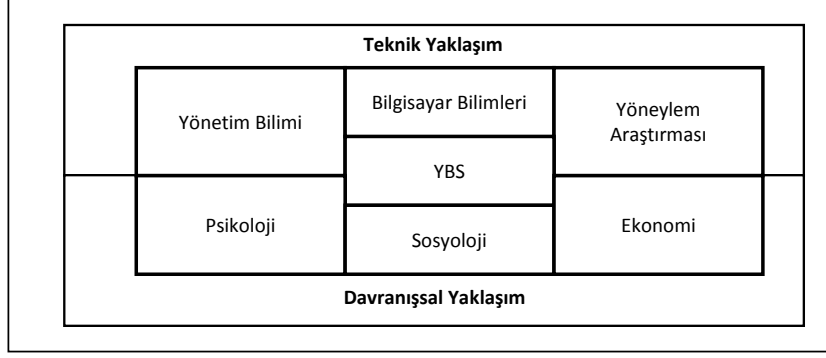
US; bir alana ait uzmanlık bilgisini, yazılım aracılığı ile bilgisayar ortamına aktarma işlemidir. Sistem mimarisi olarak uzman sistemleri diğer sistemlerden ayıran en önemli özellik US'lerdeki "Bilgi Tabanı" ve "Çıkarım" sistematiğidir. Bu yüzden sistem tasarımında ve çalıştırılmasında alan uzmanı ile bilgi mühendisinin koordineli çalışması gerekmektedir.

US; dil, turizm, arkeoloji veya coğrafya danışmanlığı, makine tasarımı, finansal tahminler, hava durumu tahminleri veya tıbbi teşhis faaliyet alanları gibi özel alanlarda, ilgili bilgi veya tanımlayıcı cümleler üreten bir bilgi sistemidir. US içinde bulunan bilgi ve modeller, yardımcı olduğu alandaki uzman kişilerce toplanmakta ve oluşturulmaktadır. Sistem, kullanıcıları tarafından tasarlanan modellerle, sorulan sorulara yanıtlar verebilmektedir (Shimizu vd., 2006: 299).

2.2. Yönetim Bilgi Sistemleri

Yukarıda genel hatları ile açtığımız BS'ler günümüz iş dünyasında istenilen verim ve etkinlik değerine ulaşabilmek için dönüşmüş ve Şekil 6'da gösterilen ve birbirinden farklı bilim disiplinlerini etkinlikle kullanan Yönetim Bilgi Sistemleri (YBS) ortaya çıkmıştır.

Şekil 6: Yönetim Bilgi Sistemi Temel Sistem Mimarisi



Kaynak: (Laudon, Laudon, 2014: 59)

Şekil 6'da gösterilen yapı incelendiğinde YBS'lerin teknik yaklaşım altında; yönetim bilimleri, bilgisayar bilimleri ile yöneylem araştırmasını, davranışsal yaklaşım altında ise psikoloji, sosyoloji ve ekonomiyi kullanmakta olduğu saptanmaktadır.

Özellikle günümüz dünyasında yaşanan teknolojik gelişmeler ve siber uzay ortamının etkin kullanımı YBS'lerin de siber uzay tabanlı olarak kullanılmalarını beraberinde getirmektedir.

2.3. Karar Destek Sistemleri

Karar Destek Sistemi (KDS) çalışması, diğer disiplinlerin bilgisini ve özellikle teorisini kullanan tatbiki bir disiplindir (Power, 2007). KDS, doğru kararlar için doğru zamanda, uygun maliyette, uygun sunumlarla doğru bilgileri elde eden teknolojilerdir (Holsapple, 2008: 25). Bu tanımlamalardan yola çıkılarak, KDS; bilişim teknolojilerini araç olarak kullanan, veri, model ve kullanıcı arabirimlerinden oluşan ve karar vericilere danışmanlık hizmeti veren çok kapsamlı yazılımlar olarak da tanımlanabilir.

KDS'yi diğer BS'lerden ayıran temel özellikler; etkililiği, matematik modele sahip olması ve karar verme süreciyle bütünleşmesi olarak sayılabilir (Vercellis, 2009: 37). Bu özellikleri sağlayabilmek için KDS tasarımında; güçlü bir veri tabanı; doğru bir bilgi tabanı ve

çözümleme önerileri geçerli bir model tabanının olmasına dikkat edilmelidir (Forgionne, 2003: 14).

Bu kapsamda özetlenen US, YBS ve KDS'lerin özellikleri arasındaki temel farklar Tablo 1'de gösterildiği gibidir:

Tablo 1: US, YBS ve KDS Karakteristikleri.

Özellikler	US	YBS	KDS
Problem türü	Yapısal olmayan	Yapısal	Yarı-yapısal, Entegre edilmiş
Kullanım Maksadı	Özel	Verimlilik	Etkinlik, Mükemmelleştirme
Zaman	Şimdi	Geçmiş ve Şimdi	Şimdi ve Gelecek
Hedefi	Sonuç	Bilgi	Karar
Maliyet	Orta ve Yüksek	Orta	Yüksek
Uygulamalar	Teşhis, Eğitim	Envanter, Muhasebe, Tahmin	Bütünleşik Karar

Kaynak: (Shimizu, vd., 2006: 316)

Tablo 1 incelendiğinde US, YBS ve KDS gibi BS'nin de günümüz dünyasında önemini artırarak devam ettirdiğini ve artık siber uzay ortamında ve gerçek zamanlı bilgileri kullandıkları görülmektedir.

3. SİBER UZAY VE KAVRAMSAL BİR YAKLAŞIM

Siber Uzay; "internet, iletişim ağları, bilgisayar sistemleri, gömülü işlemciler ve denetleyiciler de dâhil olmak üzere bilgi teknolojisi altyapılarının birbirlerine bağlı olduğu ağdan oluşan küresel bir ortam"¹ ya da "bilgisayar ağları üzerinden iletişimi sağlayan ortam"² olarak tanımlanmaktadır.

¹ Department of Defense Dictionary of Military and Associated Terms. https://fas.org/irp/doddir/dod/jp1_02.pdf pg.44 [18.01.2018]

² <https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Introduction%20to%20the%20Concept%20of%20IT%20Security.pdf> pg.18 [17.01.2018]

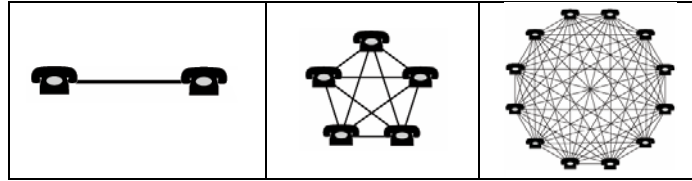
Siber uzay³; hava, kara, deniz ve uzaydan oluşan dört boyuta ilave beşinci boyut olarak adlandırılmakta ve bu boyutların her birinin bağımsız olmasına rağmen, siber uzay bağlantı noktalarının her bir boyutla irtibatlı olduğu da ayrıca belirtilmektedir. Bu bağlantı noktalarının oluşturacağı bilgisayar ağlarının değeri ile ilgili bir öngöründe bulunan Metcalfe bilişim ağlarının değerinin, bu ağlara bağlı sistemlerin (düğüm noktalarının) karesiyle doğru orantılı olduğunu belirtmiştir. Kısaca bir bilişim ağına ne kadar çok katılan (bağlanan) olursa; ağın değeri, katılımcı sayısının karesiyle doğru orantılı olarak artmaktadır (Kocovic, 2008: 139-140).

$$\frac{N(N-1)}{2}$$

(1)

Denklem (1)'de gösterilen N katılımcı sayısı arttıkça ortamda oluşan ağ sayısı da artmaktadır. Bu durum Şekil 7 yardımıyla daha iyi anlaşılabilir.

Şekil 7: Farklı Sayıda Katılımcının Oluşturduğu Ağ Yapıları



Kaynak: (Kocovic, 2008: 140)

Günümüz teknolojisi düşünüldüğünde bilgi ağlarının yapısı sadece bilgisayarlarla sınırlı kalmamakta, çeşitli sensörler ve gömülü elektronik sistemler de siber uzayın bir paydaşı olarak ortaya çıkmaktadır. Bunun en güzel örneklerinden biri internete bağlı olan hat sayılarından anlaşılmaktadır. 31 Aralık 2017 tarihli verilere göre internet⁴; 4.156.932.140 kişi tarafından aktif olarak kullanılmaktadır. Dünya nüfusunun 7.634.758.428 kişi olduğu düşünüldüğünde bu

³ <http://www.fas.org/irp/doddir/army/pam525-7-8.pdf> [17.01.2018]

⁴ <https://www.internetworldstats.com/stats.htm> [25.05.2018]

nüfusun % 54,4'ünün internet bağlantısına sahip olduğu görülmektedir.

Türkiye'de ise bilişim teknolojilerinin girişimlerde ve hanelerde kullanım oranları Tablo 1 ve Tablo 2'de gösterildiği gibidir.

Tablo 2: Girişimlerde Bilişim Teknolojileri Kullanımı.

Yıllar	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017
Bilgisayar kullanımı	90,6	90,7	92,3	94,0	93,5	92,0	94,4	95,2	95,9	97,2
İnternet erişimi	89,2	88,8	90,9	92,4	92,5	90,8	89,9	92,5	93,7	95,9

386

IJSI 11/2
Aralık
December
2018

Kaynak: (TÜİK, 2017)

(TÜİK, 2017) verilerine göre Türkiye'de faaliyet gösteren girişimlerdeki bilgisayar kullanım ve internete erişim oranları Tablo 2'de görüldüğü gibidir. Bu değerler incelendiğinde son on yıllık dönemde bu oranların artış eğiliminde olduğu gözlenmektedir. Türkiye'deki girişimlerde internet erişimi 2017 verilerine göre % 95,9, bilgisayar kullanımı %97,2'dir. Sadece bu tabloda belirtilen veriler bile neredeyse tüm girişimlerde bilgisayar kullanılmakta olduğunu ve bu bilgisayarların neredeyse tamamının internet bağlantısına sahip olduğunu göstermektedir.

Bireysel erişimler incelendiğinde ise Tablo 3'teki değerlere erişilebilir.

Tablo 3: Hanelerde Bilişim Teknolojileri Kullanımı.

Yıllar	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017
Bilgisayar kullanımı	38,0	40,1	43,2	46,4	48,7	49,9	53,5	54,8	54,9	56,6
İnternet kullanımı	35,9	38,1	41,6	45,0	47,4	48,9	53,8	55,9	61,2	66,8

Kaynak: (TÜİK, 2018)

Tablo 3'te sunulan değerler incelendiğinde hanelerde 2015 yılına kadar bilgisayar kullanım oranları ile internet kullanım oranlarında benzerlikler görünmesine rağmen, 2015 yılı ve sonrasında internet kullanım oranlarının hanelerdeki bilgisayar kullanım oranlarını geçtiği görülmektedir. Bunun sebebi, internete erişmek için bilgisayara olan bağımlılığın azalması ve akıllı cep telefonu kullanımlarının artışı olarak gösterilebilir.

Küresel anlamda yaklaşık 4,1 milyar kişiye ilave olarak çevremizdeki teknolojik cihazların ürettiği, tespit ettiği, kullandığı ve ürettiği bilgileri de göz önüne aldığımızda sayısını hayal bile edemeyeceğimiz boyutta bir bilgi yığınıyla karşı karşıya olduğumuzu da görmekteyiz. Bu yığının varlığını ve içeriğini korumak ya da bu yığından bize gelebilecek zararlı yazılımlardan korunmak önemli bir güvenlik problemi olarak karşımıza çıkmaktadır. Bu kapsamda Uluslararası Telekomünikasyon Birliği (ITU-International Telecommunication Union) tarafından; "siber çevre, organizasyonlar ve kullanıcının varlıklarını korumak için kullanılabilir araçlar, politikalar, güvenlik konseptleri, güvenlik önlemleri, kurallar, risk yönetimi, eylemler, eğitimler, uygulamalar ile teknolojiler bütünü" olarak tanımlanan "siber güvenlik" kavramı ön plana çıkmaktadır. Siber uzayın, daha önce de belirtildiği gibi çok farklı sektörler tarafından aktif olarak kullanılması, bu sektörlerle ait bilgi sistemlerinin etkin olarak korunması ihtiyacını beraberinde getirmektedir. Bu sistemler "kritik alt yapılar" olarak adlandırılmaktadır. Kritik alt yapılar tanımı; Türkiye'de de ilk kez 20 Haziran 2013 tarihli ve 28683 sayılı Resmi Gazete'de yayımlanarak yürürlüğe giren "Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı"⁶nda yer almıştır. Bu plana göre kritik alt yapılar; "işlediği bilginin gizliliği, bütünlüğü veya erişebilirliği bozulduğunda, can kaybına, büyük ölçekli ekonomik zarara, ulusal güvenlik açıklarına veya kamu düzeninin bozulmasına yol açabilecek bilişim sistemlerini barındıran altyapıları" şeklinde ifade edilmiştir. Bu tanımlamadan da anlaşılacağı gibi bu noktada "siber güvenlik" kavramı devreye girmekte ve siber uzayı paylaşan tüm süreçlerde etkinlikle kullanılmasına gereksinim duyulmaktadır.

⁵ <https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Introduction%20to%20the%20Concept%20of%20IT%20Security.pdf> pg.43 [19.02.2018]

⁶ http://www.udhb.gov.tr/doc/siber/SOME_2013-2014_EylemPlani.pdf [19.02.2018]

4. SİBER GÜVENLİK SÜRECİ

(ITU-T Rec.) tarafından siber güvenliğin sağlanmasındaki temel hedefler; “erişebilirlik”, “bütünlük” ve “gizlilik” olarak belirtilmektedir. Bu hedefler Carnegie Mellon University tarafından yayınlanan Security 101⁷ isimli çalışmada şu şekilde tanımlanmaktadır:

- Erişilebilirlik; bilgi ve bilgi sistemlerinin yetkisiz bozulmalara karşı korunması anlamına gelmektedir. Kısaca, bilgi ve bilgi sistemlerine zamanında ve güvenilir bir şekilde erişilmesini sağlamaktır.
- Bütünlük; bilgilerin yetkisiz düzenleme veya yok edilmeden korunması anlamına gelmektedir. Amacı bilgi ve bilgi sistemlerinin doğru, tam ve bozulmamış olmasını sağlamaktır.
- Gizlilik; bilginin yetkisiz erişime veya açıklanmaya karşı korunması anlamına gelmektedir. Bilgiye erişme hakkına sahip olanların bunu yapabilmelerini ve yetkilendirilmemiş kişilerin bunu yapmalarını engeller.

Ancak, “siber” ön ekinin getirildiği tüm kavramlar toplumun tüm katmanlarını etkilemekte ve belirtilen hedefler tüm toplum katmanları için bir tehdit algısı oluşturmaktadır. Özellikle siber uzaya kolay ulaşım desteği veren akıllı telefonlar, tablet bilgisayarlar ve siber uzayla irtibatlı tüm sensörler bu tehditleri sıradanlaştırmaktadır. Belirtilen bu tehdit algısını Tablo 4’te gösterildiği gibi özetlemek mümkündür:

Tablo 4: Siber Tehdit Kaynakları.

Siber Tehditler	
Yazılım Kaynaklı Tehditler	İnsan Kaynaklı Tehditler
Zombi/Hayalet Sistem yazılımları	- Organize Suç Grupları
Yemleme yazılımları	- Yabancı İstihbarat Örgütleri
İstemdışı e-posta yazılımları	- Hacker’lar
Casus/Kötü amaçlı yazılımlar	- BİS'lere Erişebilen Çalışanlar
	- Teröristler

Kaynak: (Ünal, 2015: 115)

⁷ Security 101, <https://www.cmu.edu/iso/aware/presentation/security/101-v2.pdf>, [22.01.2018].

Tablo 4’te belirtilen siber tehditlerin kaynakları yazılım desteğindeki insanlardan oluşmakta ve yine insanları hedef olarak almaktadır. Bu tehditler sosyal ağlar ve kişisel web sayfalarına yapılan saldırılarla bireyleri, kritik altyapı tesisleri, kurumsal web sayfaları, e-devlet, e-banka, e-sağlık gibi akıllı ağlar ile toplumu ve devlet yapılarını etkileri altına almaya çalışmaktadır.

Bu etki; toplumun değişik seviyelerdeki (yaş, eğitim, yönetici, çalışan,vb.) tüm katmanlarını kapsayabilir ve bu yeni durum da toplumun tüm katmanlarını etkiler.

SONUÇ

Bilişim teknolojisinin hızlı gelişimi ile birlikte hemen her sektörde bilgi üretimi artmış, hatta bilgi kirliliği olarak ifade edebileceğimiz bilgi yığınları oluşmaya başlamıştır. Bu yığının içinden doğru bilginin tespit edilmesi ve bu bilgiye erişim ise büyük önem taşımaktadır. Bu erişimin ardından karşılaşılan en önemli sorun ise bu bilginin işlenmesidir. İşte tam da bu noktada devreye BS’ler girmektedir. BS’ler sayesinde geçerli olduğu belirlenen bilgiler işlenmekte ve girişimlerin doğru, etkili ve verimli işleyişine katkı sağlamaktadır.

Ancak tüm bu süreç kapsamında göz ardı edilmemesi gereken en önemli husus sahip olunan ya da araştırılan bilginin güvenlik altına alınmasıdır. Siber uzayın kullanımı ile birlikte yaşanan güvenlik dönüşümü sonucunda ortaya çıkan siber güvenlik olgusu bir anda fiziksel şartların ötesine geçerek; sosyal ağlar, web siteleri, kritik altyapı tesisleri, e-devlet, e-banka, e-sağlık gibi akıllı ağlar ile toplumu ve devlet yapılarını etki alanına almıştır. Bu alan; toplumun tüm katmanlarını (yaş, eğitim seviyesi, yönetici, çalışan, ev hanımı, vb.) kapsamaktadır. Kapsamın bu kadar etkili ve geniş olması, sadece iş ortamında değil, toplumun her katmanında siber güvenlik bilincinin oluşturulmasını ve gerekli önlemlerin alınmasını zorunlu kılmaktadır.

Bu kapsamda aşağıda belirtilen hususların dikkate alınmasının uygun olacağı değerlendirilmektedir:

- Girişimlerin siber güvenlik stratejilerini ve siber güvenlik uygulama politikalarını güncel tutmaları,

- Üretilen politika ve stratejiler kapsamında kısa, orta ve uzun vadeli siber güvenlik uygulama planlarını oluşturmaları,
- Mevcut bilgi sistemleri merkezlerine ilave olacak şekilde “Siber Güvenlik Merkezi” yapılanmasına geçilmesi,
- Siber Güvenlik Merkezi çalışanlarının her türlü tehdit algılamasına uyum sağlayacak şekilde, esnek ve bilimsel öngörüye sahip olmaları ve niteliklerini korumaya yönelik güncel eğitimler almalarının sağlanması,
- Günümüz siber saldırılarının -çoğunlukla- yapay zekâ yazılımları yardımıyla gerçekleştirilmesi, bu sızma faaliyetlerinin hedef bilgi sistemleri tarafından zamanında saptanamamasına sebep olmaktadır. Bu kapsamda hedef bilgi sistemi korumasında da yapay zekâ yöntemleri kullanımına öncelik verilerek “tehdit belirleme hızı”nın artırılması yönünde projeler geliştirilmesi,
- Siber güvenliğe yönelik mevzuatın, gelişen bilişim teknolojisini yakından izleyerek, önleyici tedbirleri de içerecek şekilde, kişi hak ve özgürlüklerini de gözeterek ulusal ve uluslararası düzeyde yapılandırılarak, güncel tutulması.
- Kritik alt yapı yazılımları başta olmak üzere, gerekli tüm yazılımların milli kaynak kodları içermesi ve mevcut yazılım oluşturma standartlarına uygun bir şekilde yazılması,
- Toplumun tüm katmanlarında; siber güvenlik farkındalığı ile siber güvenlik bilinci oluşturacak şekilde ve katmanlar arasında da etkileşimli olacak şekilde değişik seviyelerde eğitimler tasarlanarak, uygulamalı bir şekilde gerçekleştirilmesi.

KAYNAKLAR

Department of Defense Dictionary of Military and Associated Terms. https://fas.org/irp/doddir/dod/jp1_02.pdf pg.58 (Erişim Tarihi 25.05.2018).

Efil, İsmail (2002). *İşletmelerde Yönetim ve Organizasyon*. İstanbul: Alfa Yayınları.

Sanders, John (2016). "Defining Terms: Data, Information and Knowledge". 2016 SAI Computing Conference (SAI 2016), 13-15 July 2016, London, 223-228.

Forgionne, Guisseppi A. (2003). "An Architecture For the Integration of Decision Making Support Functionalities". *Decision Making Support Systems Achievements and Challenges for the New Decade*, Manuel Mora, Guisseppi A. Forgionne (Eds.), London: Idea Group Publishing, 1-19.

Harrison, E. Frank (1995). *The Managerial Decision Making Process*. Boston: Houghton Mifflin Company.

Holsapple, Clyde W. (2008). "Decisions and Knowledge". *Handbooks on Decision Support Systems 1: Basic Themes*, Frada Burstein, Clyde W. Holsapple (Eds.), Berlin: Springer, 21-53.

<http://www.fas.org/irp/doddir/army/pam525-7-8.pdf> (Erişim Tarihi 17.01.2018).

<https://www.internetworldstats.com/stats.htm> (Erişim Tarihi 25.05.2018).

[https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Introduction %20to%20the%20Concept%20of%20IT%20Security.pdf](https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Introduction%20to%20the%20Concept%20of%20IT%20Security.pdf) pg.43 (Erişim Tarihi 19.02.2018).

<https://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx> [07.11.2018]

ITU-T Rec. X.1205 (2008) "Overview of cybersecurity", <https://www.itu.int/rec/T-REC-X.1205-200804-I>, (Erişim Tarihi 22.01.2018).

Kocovic, Petar (2008). "Four Laws for Today and Tomorrow". <http://www.scielo.org.mx/pdf/jart/v6n3/v6n3a1.pdf>, (Erişim Tarihi 19.02.2018).

Koçel, Tamer (2010). *İşletme Yöneticiliği*. İstanbul: Beta Basım Yayım.

Laudon, Kenneth C.; Laudon, Jane P. (2014). *Management Information Systems Managing the Digital Firm*. Boston: Pearson.

Power, Daniel, J. (2007). "A Brief History of Decision Support Systems". <http://DSSResources.COM/history/dsshistory.html> (Erişim Tarihi 09.04.2018).

Resmi Gazete (2013). Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı, http://www.udhb.gov.tr/doc/siberg/SOME_2013-2014_EylemPlanı.pdf (Erişim Tarihi 19.02.2018).

Security 101, <https://www.cmu.edu/iso/aware/presentation/security101-v2.pdf>, (Erişim Tarihi 22.01.2018).

Shimizu, Tamio; de Carvalho, Marly Monteiro; Barbin, Laurindo Fernando Jose (2006). *Strategic Alignment Process and Decision Support Systems: Theory and Case Studies*. London: IRM Pres.

Stair, Ralph M; Reynolds, George Walter (2009). *Fundamentals of Information Systems*. UK: Course Technology.

Terzi, Ramazan; Sağıroğlu, Şeref; Demirezen, M. Umut (2017). "Büyük Veri ve Açık Veri: Temel Kavramlar". Büyük Veri ve Açık Veri Analitiği: Yöntemler ve Uygulamalar, Şeref Sağıroğlu, Orhan Koç (Eds.), 13-29. http://bigdatacenter.gazi.edu.tr/wp-content/uploads/buyuk_veri_ve_acik_veri_analitigi.pdf (Erişim Tarihi 01.03.2018).

TÜİK (2017). http://www.tuik.gov.tr/PreTablo.do?alt_id=1028. (Erişim Tarihi 14.02.2018).

Ülgen, Hayri; Mirze, S. Kadri (2013). *İşletmelerde Stratejik Yönetim*. İstanbul: Beta Basım Yayım.

Ünal, Ahmet Naci (2015). *Siber Güvenlik ve Elektronik Bileşenleri*. Ankara: Nobel Akademik Yayıncılık.

Vercellis, Carlo (2009). *Business Intelligence: Data Mining and Optimization for Decision Making*. West Sussex: John Wiley & Sons Ltd.

Yarman, Bekir, Sıddık, Binboğa; Ünal, Ahmet Naci (2015). *Stratejik Karar Verme Boyutunda Bilgi Toplama/İşleme Amaçlı Karar Destek Sistemleri*. Ankara: Nobel Akademik Yayıncılık.

SUMMARY

Information is the product of an extensive process obtained by excogitation, judgement and reasoning. This process made progress along with human history and became one of the fundamental elements of today's world. Particularly with the development of information technology, it constitutes the concept of "decision" which is one of the most important outputs of management science. In today's world, the variation of the problem fields including the interdisciplinary studies causes the complexification of the solution options which forms the basis of decision and makes it harder for the decision makers to make the appropriate choice. At this point Information Systems (IS) are designed for decision makers. IS; Systems which are in relation with management, organization and technology components as being the part of all management processes, which enables direct coordination with these factors and which supports the operation of the organizations are developed.

IS is separated into functional subdivisions such as; Expert Systems (ES), Management Information Systems (MIS), Decision Support Systems (DSS) with the effect of continuously transforming technological opportunities. The main input or starting material of each IS is "information". In the first decade of the 21st century, the increase in the quantity of data which creates the information and utilization of this data in various compositions significantly enhances the value and the quantity of information. "Cyberspace" which is defined as "A global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.⁸" or "The environment in which communication over computer networks occurs."⁹ plays an important role in this increase. "Cyberspace" includes not only our personal world but also many social areas that differ from one another. Most of the business processes take place under scope of cyberspace and cyber security is highly important. In this context, "cyber security is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's

⁸ Department of Defense Dictionary of Military and Associated Terms. https://fas.org/irp/doddir/dod/jp1_02.pdf pg. 58 25.05.2018.

⁹ <https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Introduction%20to%20the%20Concept%20of%20IT%20Security.pdf> pg.18, 25.05.2018.

assets.¹⁰ Although cyber security is a virtual concept, it has physical impacts. Cyber threats are generated by malicious software and their targets are humans and organizations. For this reason, cyber security concept is particularly significant for IS.

In this study the evaluation process of data, the dimensions of IS, cyberspace and cyber security process is analyzed. In the conclusion part emphasis is laid on the precautions to be taken in order to provide an effective cyber security environment.

394

IJSI 11/2
Aralık
December
2018

¹⁰ <https://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx> [07.11.2018]