Kamu Yönetimi ve Teknoloji Dergisi
Journal of Public Administration and Technology

DERLEME MAKALESİ

Geliş Tarihi: 1 Mayıs 2020
Kabul Tarihi: 25 Haziran 2020

TÜRK KAMU SEKTÖRÜNDE BİLGİ VE BİLİŞİM GÜVENLİĞİ*

Tuba ÖZBİLEN[1]

ALİ ÇAĞLAR[2]

Öz

Bu çalışmanın ana amacı, Türk kamu sektöründe bilgi ve bilişim güvenliğinin mevcut durum tespitini yaparak, buradan hareketle birtakım analiz, değerlendirme ve önerilerde bulunmaktır. Belirtilen amaca varmak için öncelikle siber güvenlik kavramı başta olmak üzere, Türkiye'de bilgi ve bilişim güvenliğiyle ilintili kurum ve kuruluşlara yer verilmiştir. Aynı zamanda bu kurum ve kuruluşların sorumlulukları ve görev alanları değerlendirilmiştir. Daha sonra içeriden ve dışarıdan, rekabete ve saldırılara karşı koyabilecek bir bilgi ve bilişim sektörüne sahip olmamız için neler yapılması gerektiği açıklanmıştır. Çalışmanın verileri, ikincil kaynaklara ve ilgili güncel literatüre dayanmaktadır. Diğer bir deyişle, çalışma için gereksinim duyulan veriler, özellikle alanda faaliyet gösteren yetkili ve sorumlu kamu kurumlarından -Ulaştırma ve Altyapı Bakanlığı (UAB), Bilişim Teknolojileri ve İletişim Kurumu (BTK), Siber Güvenlik Kurulu (SGK), Ulusal Siber Olaylara Müdahale Merkezi (USOM), Ulusal Kamu Entegre Veri Merkezi (KEVM), Cumhurbaşkanlığı Dijital Dönüşüm Ofisi (CB-DDO) vb.- web sayfaları, yasal mevzuat, raporlar ile alanda yapılmış akademik yayınlardan derlenmiş ve daha sonra çalışmanın amaçları doğrultusunda analiz edilerek kullanılmıştır. Çalışma, bu alanda ülkemizde önemli adımlar atılmış olmakla birlikte, özellikle ileri düzeyde karşı koymalara hazırlıklı olunması gerektiğini tespit etmiş ve bu konuda hem ilgili profesyonellerde ve hem de toplumda bir farkındalık yaratmanın gerekliliği sonucuna varmıştır.

Anahtar Kelimeler: Bilgi, Bilişim, Güvenlik, Bilgi ve Bilişim Güvenliği, Siber Güvenlik, Türkiye

Abstract

The aim of this paper is to determine the current situation of information and informatics security in the Turkish public sector. In order to achieve the aim, firstly, starting with the concept of cyber security, the main institutions which are in charge of information and informatics security are defined and explained. Later, it is discussed that how Turkey can challenge and confront the cyber competitions and attacks come from both inside and outside. The data needed were gathered from the secondary data related to these intsitutions, mainly the institutions which are in charge of the information and informatics security, i.e., Ministry of Transportation and Infra-structure (UAB), The Institution of Informatics Technologies and Communication (BTK), Cyber Security Board (SGK), National Center for Counteracting to Security Attacks (USOM), National Public Data Integrated Center (KEVM), Presidency Digital Transformation Office (CB-DDO) and their web sites, and reports. The collected data are evaluated and analysed in order to achieve the aims of study. The study is concluded that although there are important improvements, the informatics security in Turkey still does need further and counter works to be done, and also to create an awareness for both institutional professionals and citizens in society.

Keywords: Information, Informatics, Security, Information and Informatics Security, Cyber Security, Turkey.

I. GİRİŞ

Güvenlik, tüm canlılar için en temel gereksinim olmakla birlikte, küresel anlamda herkesin üzerinde mutabık olduğu bir güvenlik kavramı tanımı yapmak pek olanaklı değildir. Sosyal bilimlerdeki hemen hemen her kavramın tanımlanmasında görülmekte olan bu farklılıklara rağmen, güvenlik kavramı, anlam olarak genelde; "tehditlerden, korkulardan ve tehlikelerden uzak olmak anlamına gelmektedir" (Akbulut, 2015: 7). Bu açıdan bir bireyin ya da bir kurumun güvende olması durumu temelde iki koşula bağlıdır: "Eldeki değerlere yönelik bir tehdidin olmaması ve eğer böyle bir tehdit

* Bu makalenin yazımı aşamasında, çok değerli görüş ve değerlendirmeleri ile katkıda bulunmuş olan "Bilgi Teknolojileri ve İletişim Kurumu" İnternet Daire Başkanı Sayın Bahadır Aziz Sakin ile "Bilgi Teknolojileri ve İletişim Kurumu" Siber Güvenlik Uzmanı Sayın Onur Aktaş'a çok teşekkür ederiz.

[1] Dr. Öğrencisi, Hacettepe Üniversitesi, SBE, Siyaset Bilimi ve Kamu Yönetimi ABD, ORCID: 0000-0003-2303-9381

[2] Prof. Dr. Ali Çağlar, Hacettepe Üniversitesi İİBF Siyaset Bilimi ve Kamu Yönetimi Bölümü, e-posta: acaglar@hacettepe.edu.tr, ORCID: 0000-0003-0101-655X

varsa tehdide maruz kalanın rasyonel bir maliyetle bu tehdidi savuşturma kapasitesine sahip olması" (Miller, 2001: 16). Bilgi ve bilişim güvenliği konusuna gelindiğinde ise günümüzde en değerli güç unsurlarının başında geldiğini söylemek olanaklıdır. Bilgi ve iletişim teknolojilerinin hızla gelişmesi ile birlikte daha çok bilginin depolanması, taşınması ve işlenmesi olanaklı hale gelmiştir. "Bilgi ve teknoloji önemli bir güç çarpanı olarak insan, malzeme ve finanstan daha önemli bir kaynak olarak" (Bayazıt, 2005:20) değerlendirilmektedir. Teknolojik ürünler yardımıyla, her gün daha fazla bilgi ve belge veri tabanlarına aktarılmakta, buralarda depolanmakta ve analiz edilerek kullanılmaktadır. Hatta gerektiğinde çok kolaylıkla bir yerden başka bir yere bu bilgi transfer edilmektedir. Buna bağlı olarak, ülkeler tarafından vatandaşlara sunulan birçok hizmet, gelişen bilgi teknolojileri bünyesinde internet üzerinden sağlanmaktadır.

Söz konusu sistemler, kamu kurumlarının yanı sıra enerji ulaşım, haberleşme gibi kritik altyapı sektörlerinde yaygın bir şekilde kullanılmaktadır. Bu sistemler gerek sunulan hizmetlerin kalitesine gerekse ilgili kurum/kuruluşun daha verimli çalışmasına katkıda bulunmaktadır. Kurum ve kuruluşların uhdesinde bulunan bilgi-verinin tam güvenliği sağlanmış şekilde korunması gerekmekte olup söz konusu sistemlerin güvenliğinin sağlanması ulusal güvenlik açısından büyük bir önem oluşturmaktadır. Günümüzde özellikle zararlı yazılımlar, oltalamalar, hedef odaklı saldırılar, botnet[3]vb. gibi tehditlerle sıklıkla karşılaşılmaktadır. Dolayısıyla bahsi geçen sistemlerin güvenliğinin sağlanmaması durumunda, ulusal boyutta güvenlik risklerinin oluşması, can kayıplarının yaşanması, kamu düzeninin bozulması, sistemlerin hizmet dışı kalması ve ülkeler açısından itibar kaybı gibi durumlar ile karşılaşılabilecektir. Bu bağlamda, çalışmada; Türkiye'de siber güvenlik organizasyonu, bilgi güvenliği ve siber güvenlik alanında gerçekleştirilen çalışmalar, kritik altyapıların güvenliği ve siber güvenlik ekosistemi temel konu olarak ele alınmıştır.

Bu çalışma, ikincil verilere dayalı bir araştırmadır. Çalışmanın gereksinim duyduğu veriler, konuyla ilgili mevzuat, yazılı, görsel dokümanların yanısıra akademik literatür ve alanın ilgili, sorumlu ve yetkili kurumlarının - UAB, BTK, SGK, USOM, KEVM, CB-DDO vb. - web sayfaları ile raporlarından derlenmiştir. Toplanmış olan veriler, çalışmanın amacı doğrultusunda, birim – kurum bazında sınıflandırılmış ve daha sonra analiz edilerek değerlendirilmiştir.

Çalışmada öncelikle, alanın temel kavramı olan "siber güvenlik" konusuna yer verilmiştir. Her ne kadar, literatürde, zaman zaman "dijital güvenlik" veya "online güvenlik" vb. kavramlar kullanılıyor olsa da "bilgi ve bilişim güvenliği" dendiğinde, en kapsayıcı kavram olarak "siber güvenlik" kavramıyla karşılaşıldığını söylemek olanaklıdır.

1. Siber Güvenlik

Kavramsal olarak bakıldığında; *siber* kelimesinin anlamı, bilgisayar ağlarına veya internete ait olan anlamına gelmektedir. Dolayısıyla 'siber güvenlik' dendiğinde, bilgi ve bilgisayar güvenliğinden, dijital ortamdaki veri ve operasyon güvenliğine kadar çok genişçe bir alan akla gelir. Bu nedenle siber güvenlik konusu; "'bilgi silahları' ve 'bilgi savaşı veya siber savaş' gibi yeni kavramların güvenlik literatürüne girmesine sebep olmuştur" (Atıcı, 2005: 791 ve O'Brien, 2004: 132). "Siber güvenlik farklı hedef kitleleri için farklı anlamlara gelmekle birlikte bireyler açısından, güvenli hissetmek, kişisel verileri ve gizliliği korumak demektir" (Yılmaz, 2017: 718). İlgili kurumlar açısından siber güvenliğin temel hedefi, ifa edilen görevle ilgili çok özel öneme sahip bilgi ve verilerin kullanılabilir olması ile

[3] Çok sayıda bilgisayarın bir IP'ye saldırması – büyük bir zombi PC ağı.

gizli verilerin korumasını sağlamakken, "hükümetler açısından ise vatandaşların, kurumların, kritik altyapının ve devlete ait bilgisayar sistemlerinin çökertilmesi amaçlı saldırılara ya da verilerin çalınmasına karşı korunması anlamına" (Yılmaz, 2017: 718) gelmektedir.

Bilişim dünyasında internetin gelişimi insanlara birçok kolaylık sağlamaktadır. İnsanlar birçok hizmete, o hizmetin üretildiği ya da sunulduğu yere gitmeden bilgisayar ya da mobil cihazlarıyla ulaşabilmektedirler. Alışveriş merkezine gitmeden internetten alışveriş yapabilme, fatura ödeyebilme, banka işlemleri yapabilme gibi pek çok hizmet internet üzerinden gerçekleştirilebilmektedir. Enerji dağıtım alt yapıları, banka alt yapıları, telefon hatları, hastane sistemleri, trafik lambaları gibi hizmetlerin neredeyse tümü internet alt yapısını kullanmaktadır (Akyıldız, 2017: 1). Siber güvenlik konusu ile ilgili düzenlemelere bakıldığında; *"Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna ilişkin Bakanlar Kurulu Kararı*" ve "5809 sayılı Elektronik Haberleşme Kanunu gereğince siber güvenliğin sağlanmasına ilişkin politika, strateji ve eylem planlarını hazırlamak ve koordinasyonu sağlamak görevi Ulaştırma, Denizcilik ve Haberleşme Bakanlığı'na verilmiştir" (Resmi Gazete, 20 Ekim 2012).[4]

Bu çerçevede, siber uzay güvenliğinin amaçları şu şekilde sıralanmıştır[5]:

1) Ulusal kritik altyapının siber saldırılardan korunması,
2) Siber saldırılara karşı ulusal hassasiyeti arttırmak,
3) Siber saldırı oluştuktan sonra kurtulma zamanını ve zararı asgari düzeyde tutmak*.

Bu kapsamda, söz konusu karar gereğince, "Siber Güvenlik Kurulu" oluşturulmuş ve siber güvenlikle ilgili olarak UAB'na görev, yetki ve sorumluluklar verilmiştir. Ayrıca, siber güvenlik ile ilgili çalışma grupları ve geçici kurulların oluşturulabileceği karara bağlanmıştır. Siber Güvenlik Kurulu, "siber güvenlikle ilgili kamu kurum ve kuruluşları ile gerçek ve tüzel kişiler tarafından alınacak önlemleri belirlemek, hazırlanan plan, program, rapor, usul, esas ve standartları onaylamak, (politika, strateji ve eylem planlarını onaylamak) ve bunların uygulanmasını ve koordinasyonunu sağlamak amacıyla 'Ulaştırma, Denizcilik ve Haberleşme Bakanı' başkanlığında kurulmuştur" (UDHB, 2019 ve www.btk.gov.tr, 2019). Kurulun temel görevleri, Resmi Gazete'de şu şekilde verilmiştir:

"1. Siber güvenlik ile ilgili politika, strateji ve eylem planlarını onaylamak ve ülke çapında etkin şekilde uygulanmasına yönelik gerekli kararları almak.

2. Kritik altyapıların belirlenmesine ilişkin teklifleri karara bağlamak.

3. Siber güvenlikle ilgili hükümlerin tamamından veya bir kısmından istisna tutulacak kurum ve kuruluşları belirlemek.

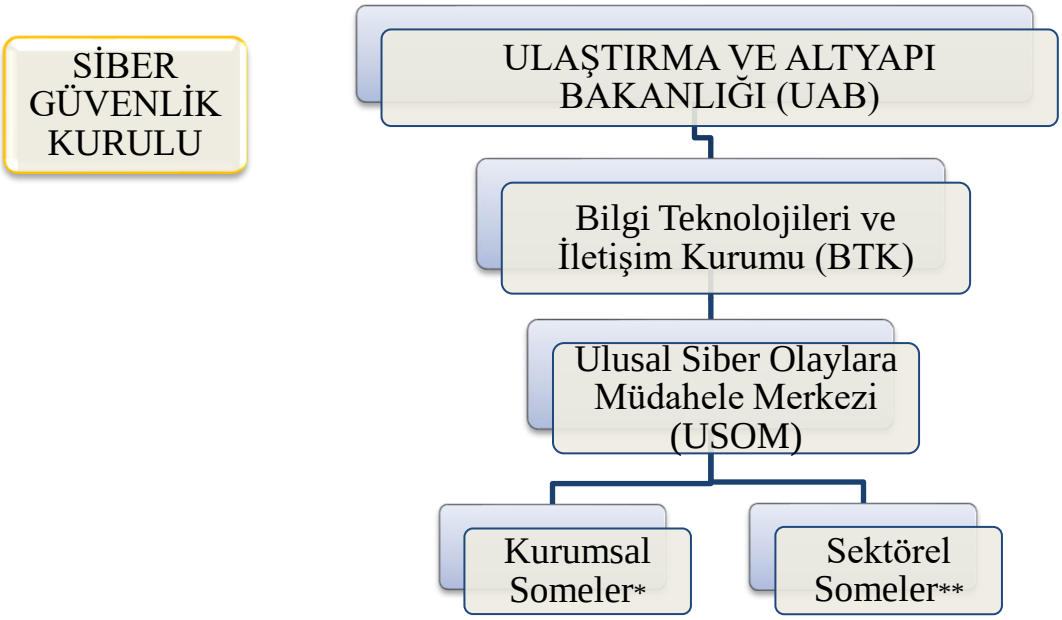
4. Kanunlarla verilen diğer görevleri yapmak".

[4] Bkz. 28447 Sayılı Bakanlar Kurulu Kararı "Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Karar" **Resmi Gazete**, 20.10.2012. Bakanlığın adı, Cumhurbaşkanlığı Hükümet Sistemi ile birlikte "Ulaştırma ve Altyapı Bakanlığı" olarak değiştirilmiştir.

[5]Geniş bilgi için bkz.(The White House, 2003).

* Kurumsal SOME: "Temel görevleri tebliğde yer alan kurumunda bulunan siber güvenlik risklerini azaltan ve siber olay meydana geldiğinde görev tanımında yer alan çalışmaları yapan Kurumsal Siber Olaylara Müdahale Ekibi" (UDHB, 2019).

**Sektörel SOME: "Temel görevleri tebliğde yer alan ve düzenlemekle yükümlü olduğu sektörde bulunan kritik altyapı veya kamu sistemlerini siber olaylardan korumak için çeşitli çalışmalar yapan Sektörel Siber Olaylara Müdahale Ekibi" (UDHB, 2019).



5809 sayılı Elektronik ve Haberleşme Kanunu'na eklenen Ek Madde 1 de "Siber Güvenlik Kurulunda yer alacak bakanlık ve kamu kurum ve kuruluşları ile üyelerinin temsil düzeyi Bakanlar Kurulu tarafından belirlenir" denilmektedir. Söz konusu Kanun ile işaret edilen 11/6/2012 tarihli ve 2012/3842 sayılı Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Bakanlar Kurulu kararına göre Siber Güvenlik Kurulu, Ulaştırma ve Altyapı Bakanı'nın başkanlığında şu üst düzey yöneticilerden oluşturulmuştur[6]:

- Dışişleri Bakanlığı Müsteşarı,
- İçişleri Bakanlığı Müsteşarı,
- Milli Savunma Bakanlığı Müsteşarı,
- UAB Müsteşarı,
- Kamu Düzeni ve Güvenliği Müsteşarı,
- Milli İstihbarat Teşkilatı Müsteşarı,
- Genelkurmay Başkanlığı Muhabere Elektronik ve Bilgi Sistemleri Başkanı,
- Bilgi Teknolojileri ve İletişim Kurumu Başkanı,
- TÜBİTAK Başkanı,
- MASAK Başkanı ile UDH Bakanı tarafından belirlenecek diğer Bakanlık ve kamu kurumlarının üst düzey yöneticileri" (BTK, 2019).[7]

[6] Cumhurbaşkanlığı Hükümet Sistemi'nin kurulmasıyla birlikte 'Siber Güvenlik Kurulu' ile ilgili düzenlemelerde bir boşluk oluştuğu anlaşılmaktadır. Kurul halihazırda kanunen yerini ve görevlerini korumaktadır. Ancak kurulda olması gereken bazı organlar bugün lav edilmiştir. Bunlardan biri Telekomünikasyon İletişim Başkanlığı'dır. Ayrıca yeni hükümet sisteminde Cumhurbaşkanlığına bağlı 'Dijital Dönüşüm Ofisi' kurulmuştur. Bu durumda, esasında, en son 2016 Şubat ayında toplanan ve sonrasında toplanmayan Kurul'un fiili olarak boşta durduğu; lav edilen ve ihdas edilen kamu organizasyonlarıyla birlikte ise rol ve görev paylaşımında yeniden bir yapılandırmanın ihtiyaç olarak ortaya çıktığı anlaşılmaktadır. Bugün, Siber Güvenlik Kurulu ile karara bağlanması gereken hususların ağırlıklı olarak Ulaştırma ve Altyapı Bakanlığı ve Bilgi Teknolojileri ve İletişim Kurumu uhdesindeki kararlarla yürütüldüğü görülmektedir. Detaylı bilgi için bkz. https://www.btk.gov.tr/siber-guvenlik-kurulu - https://www.memurlar.net/haber/761188/tum-mustesar-kadrolari-kaldirildi-mustesarin-gorevini-bakan-yardimcisi-yurutecek.html

[7] Detay için bkz. https://www.btk.gov.tr/tr-TR/Sayfalar/SG-SIBER-GUVENLIK KURULU/

Bu organizasyonel yapının yanı sıra siber güvenliğe yönelik tehdit yöntemleri sürekli çeşitlenmektedir ve kapsamı değişmekle beraber bu tehditler şu şekilde özetlenebilir (Stolfo, 2008: 63-72):

- "Virüs; izinsizce bilgisayara yüklenen ve çalışan, ufak ama etkili bir bilgisayar programı veya koddur.
- Solucan (worm) virüs; e-posta üzerinden bir bilgisayardan diğerine kendini kopyalayan, daha sonra da bulaştığı bilgisayarın olanaklarını kullanarak amaçlarını gerçekleştiren bir virüstür.
- Truva atı; doğrudan "bir saldırı veya bir virüs vasıtasıyla hedeflenen sistemlere yerleştirilen, kötü niyetli" (www.afyonluoglu.org, 2019) yazılımlardır.
- Hizmet dışı bırakma (denial of service) saldırıları; internet üzerinden müşterilere hizmet sağlayan bilgisayara yönelik yapılan saldırılardır.
- Aldatma (IP spoofing) saldırısında saldırganlar; saldırganın kendisinden değil saldırıya uğrayanın güvendiği bir bilgisayardan geliyormuş gibi görünen internet mesajları yaratan yazılım araçları kullanırlar.
- Gizlilik ihlali (sniffers); e-posta ve diğer bilgiler, bir bilgisayardan diğerine ağın bir bölümüne bağlanan bir kimse tarafından kolaylıkla okunabilecek bir formda gönderilir. Paket korsanı.
- Phishing; "e-posta veya bunun gibi bilgi girilmesi gerektiren bir kuruluşun web sayfasının bir kopyasını yapıp kullanıcının hesap bilgilerini çalmayı" (www.afyonluoglu.org, 2019) amaçlayan programlardır. Oltalama, e-dolandırıcılık yapan programlar, spam.
- Spam; internet üzerinden aynı mesajın yüksek sayıdaki kopyasının, talepte bulunmamış kişileri, zorlayıcı şekilde gönderilmesidir. İstenmeyen e-posta".

1.1.1. Türkiye'de Siber Güvenlik Çalışmaları

Siber Güvenlik Kurulu 21 Aralık 2012 tarihinde dönemin UDHB Bakanı Başkanlığında ilk toplantısını gerçekleştirilmiştir. Kurul kararında, "*Siber Güvenlik Kurulunun Görevleri, Çalışma, Usul ve Esasları ile Yönergesi*" ve "*Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı*"[8] kabul edilmiştir. Kurul, ikinci toplantısını ise, 20 Haziran 2013 tarihinde gerçekleştirmiştir. Bu toplantı sonucunda, *"Ulusal Siber Olaylara Müdahale Merkezi (USOM)"* kurulmuş ve 15 Mayıs 2013 tarihinde de faaliyete geçmiştir. Kurulun üçüncü toplantısı, 19 Aralık 2013, dördüncü toplantısı ise 10 Haziran 2016 tarihinde gerçekleştirilmiştir. Ayrıca, 2013 yılında Türk Silahlı Kuvvetleri bünyesinde de Siber Savunma Komutanlığı kurulmuştur[9].

"28447 Sayılı Bakanlar Kurulu Kararı" gereğince, ulusal düzeyde siber güvenliğin eksiksiz bir şekilde sağlanması amacıyla gerekli politika, strateji ve eylem planlarının hazırlanması ve SGK'nın sekretarya hizmetlerinin yürütülmesi görevleri UAB'na verilmiştir. UAB'na siber güvenlik konularında ayrıca; politika, strateji ve eylem planlarının hazırlanması, usul ve esasların belirlenmesi, kamu kurum ve kuruluşlarındaki teknik alt yapının oluşturulmasının sağlanması ve bu yapıların doğruluğunun test edilmesi, Siber Olaylara Müdahale Organizasyonu'nun oluşturulması, farkındalık yaratma ve

[8] https://www.btk.gov.tr/tr-TR/Kurumdan-Haberler/Siber-Guvenlik-Kurulu-Toplandi/ (Bilgi Teknolojileri ve İletişim Kurumu).

[9] Detaylı bilgi için bkz.(Sabah Gazetesi, 05.06.2016).

bilinçlendirme amacıyla eğitim faaliyetlerinin yürütülmesi görevleri verilmiştir[10]. Bu kapsamda 2013 yılında, dönemin UDHB koordinasyonunda ilgili kuruluşlar ile STK'ların katkılarıyla "*Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı*" hazırlanmış ve bu plan SGK'nda kabul edilmiştir. Söz konusu Eylem Planı, Bakanlar Kurulu Kararı ile 20 Haziran 2013 tarih ve 28683 sayılı Resmi Gazete'de yayımlamış ve yürürlüğe girmiştir [11]. "*Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı"*, "7 ana başlık altında, 29 ana eylem maddesi, 86 alt eylem maddesi ve 31 sorumlu/ilgili kurum, kuruluş, organizasyonu kapsamaktadır" (www.afyonluoglu.org 2019). Bunun yanında, artan siber güvenlik gereksinimi doğrultusunda 2016 yılında, "*2016-2019 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı*"; aralarında "kamu kurumları, kritik altyapı işletmecileri, bilişim sektörü, üniversiteler ve sivil toplum kurumlarını temsilen toplam 73 kurum ve kuruluştan uzmanların katkıları ile oluşturulmuştur" (UDHB, 2019)[12].Ulusal güvenliğin olmazsa olmazı olarak kabul edilen siber güvenliğin öneminin ülkedeki tüm kişi ve kuruluşlarda yerleşmesi, "ulusal siber uzayda bulunan sistem ve paydaşların tamamının güvenliğini sağlamak üzere idari ve teknolojik önlemlerin alınmasını sağlayacak yetkinliğin eksiksiz bir şekilde kazanılması" amacıyla hazırlanan eylem planı;

- "Siber Savunmanın Güçlendirilmesi ve Kritik Altyapıların Korunması,
- Siber Suçlarla Mücadele,
- Farkındalık ve İnsan Kaynağı Geliştirme,
- Siber Güvenlik Ekosisteminin Oluşturulması,
- Siber Güvenliğin Milli Güvenliğe Entegrasyonu" (www.cybermagonline.com, 2019) olmak üzere 5 ana maddeden oluşmaktadır.

Ayrıca, "*Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı*" kapsamında "*Ulusal Siber Olaylara Müdahale Merkezi*" (USOM) kurulmuştur. Keza aynı "eylem planı çerçevesinde, kamu kurum ve kuruluşları bünyesinde Siber Olaylara Müdahale Ekiplerinin (Kurumsal ve Sektörel SOME) oluşturulması öngörülmüştür" (UHDB, 2019).

Bununla birlikte 64 üncü Hükümet Eylem Planı'nın "Siber güvenliğe ilişkin yasal düzenlemeler hayata geçirilecek" adlı 35 inci eylem maddesi ile ulusal siber güvenliğin sağlanması amacıyla birincil mevzuat hazırlama çalışmaları UAB Bakanlığı tarafından yürütülmektedir. Bu kapsamda, ilgili bakanlık tarafından "siber güvenlik ve e-devlet faaliyetlerine ait tüm konu başlıklarını içeren bir kanun taslağı çalışmasının tamamlandığı belirterek"[13], söz konusu taslağın yasalaşması beklenmektedir.

Diğer taraftan TUBİTAK da siber güvenlik konusunda bazı çalışmalar sürdürmektedir. "TÜBİTAK-BİLGEM Siber Güvenlik Enstitüsü (SGE) siber güvenlik alanında araştırma ve geliştirme faaliyetleri yürütmekte; askeri kurumlara, kamu kurum ve kuruluşlarına ve özel sektöre çözüme yönelik projeler gerçekleştirmekte, rehberlik sağlamaktadır"[14].

Bütün bu çalışmaların yanı sıra, siber güvenlik farkındalığının artırılması, kurumların siber saldırı anında ve sonrasında kurum içi ve kurum dışı koordinasyonun sağlanması, siber saldırılara karşı koyma yeteneklerinin geliştirilmesi amacı ile siber tatbikatlar düzenlenmiş (3 ulusal, 1 uluslararası) olup belirtilen "tatbikatlarda UDHB ile koordinasyon konularında, TÜBİTAK, BTK ve ITU-IMPACT ile

[10] Detaylı bilgi için bkz. https://www.hgm.ubak.gov.tr/sayfa/16/ (UDHB Haberleşme Genel Müdürlüğü)

[11]Detaylı bilgi için bkz. 28683 Sayılı Bakanlar Kurulu Kararı, (Resmi Gazete, 20.06.2013), www.resmigazete.gov.tr/eskiler /2013/06/20130620-1.htm

[12] Detaylı bilgi için bkz. "Ulusal Siber Güvenlik Stratejisi ve 2016-2019 Eylem Planı", www.udhb.gov.tr/doc/siberg/2016-2019 guvenlik.pdf

[13]https://www.aa.com.tr/tr/politika/siber-guvenlik-kanun-taslagi-calismasini-tamamladik/984785

[14]https://www.dijitalakademi.gov.tr/wp-content/uploads/2016/12/TUBITAK-BILGEM-YTE-Turkiyede EDevletGenelGorunumRaporu2017.pdf

teknik konularda iş birliği"[15] gerçekleştirilmiştir. Söz konusu tatbikatların sonuncusu, 29 Kasım 2017 tarihinde gerçekleştirilmiştir. Öte yandan "Ulaştırma ve Altyapı Bakanlığı ile Bilgi Teknolojileri ve İletişim Kurumu (BTK) tarafından Uluslararası Telekomünikasyon Birliği'nin (ITU) desteğiyle düzenlenen uluslararası siber güvenlik tatbikatının, 'Siber Kalkan 2019'"[16], 19-20 Aralık 2019 tarihlerinde Ankara'da yapılması planlanmıştır.

1.1.1. Kamu Sanal Ağı (KamuNET) Projesi

Kamu güvenli ağı, "kamu kurum ve kuruluşları tarafından içerik güvenliği sağlanan veri iletişiminin, kurumlar arası internete kapalı olan daha güvenli sanal bir ağ üzerinden gerçekleştirilerek risklerin en aza indirilmesi, ortak uygulamalar için uygun altyapının tesis edilmesi", oluşturulması "ve planlanan ortak veri merkezlerinin dâhil edilmesi amacıyla"[17] oluşturulmuştur. KamuNET ağına dâhil olunması amacıyla "*Kamu Kurum ve Kuruluşlarının KamuNET'e Dahil Edilmesi ile İlgili 2016/28 Sayılı Başbakanlık Genelgesi*", 03.12.2016 tarih ve 29907 sayılı Resmi Gazete'de yayımlanarak yürürlüğe girmiştir[18]. Bu çerçevede, KamuNET ağı kurulmasına yönelik dönemin "UDHB" ile "Türk Telekomünikasyon A.Ş." arasında "KamuNET İşbirliği Protokolü" imzalanmıştır. Kamu kurumlarında siber güvenlik risklerinin en aza indirilebilmesi ve KamuNET ağına dâhil olunabilmesi amacıyla dönemin UDHB tarafından belirli kriterler yayımlanmıştır. KamuNET projesine hâlihazırda 53 kamu kurumu dâhil edilmiştir.[19]

1.1.2. Kamu Entegre Veri Merkezi

"Ulusal Kamu Entegre Veri Merkezi (KEVM)", kamusal bilgi kaynak ve verilerinin kontrol edilmesi ve organizasyonu, verilerin depolanması, işlenmesi ve tek merkezden sunulması amacıyla oluşturulmuştur. KEVM projesi ile kurumlar bünyesinde kurulması planlanan veya kurulan veri merkezleri için ayrı ayrı harcama yapılmasının önüne geçilmesi, yatırımlarda ve operasyonlarda verimliliğin sağlanması hedeflenmiştir. Söz konusu projeye ilişkin 2017 tarihinde yüklenici firma ile sözleşme imzalanmış ve mevcut durum analizi gibi faaliyetleri içeren 1. Faz çalışmalarına başlamış olup söz konusu projenin ikinci fazında ise; veri merkezi tasarımı, arazi etüt çalışması ve mimari projelerin hazırlanması faaliyetleri yer almaktadır.[20] "Son fazda ise Yaklaşık Maliyet Belirleme ve Yapıma İlişkin Teknik Şartnameler"[21] hazırlanacaktır.

1.1.3.Cumhurbaşkanlığı Dijital Dönüşüm Ofisi (CB-DDO)

Özellikle 'Cumhurbaşkanlığı Hükümet Sistemi'ne geçişle birlikte, "gelişen teknolojiler, toplumsal talepler ve kamu sektöründeki reform eğilimleri doğrultusunda, farklı kurumlar

[15] https://www.btk.gov.tr/siber-guvenlik-tatbikatlari

[16] https://www.aa.com.tr/tr/bilim-teknoloji/siber-tatbikat-icin-turkiyeye-gelecekler/1660435

[17] Detaylı bilgi için bkz. https://www.udhb.gov.tr/doc/siberg/KamuNetweb.pdf/

[18] "Kamu Kurum ve Kuruluşlarının KamuNET'e Dâhil Edilmesi ile İlgili 2016/28 Sayılı Başbakanlık Genelgesi", https://www.tbb.gov.tr/www.tbb.gov.tr/basin-ve-yayin/mevzuat-duyurulari/20161205-kamu-kurum-ve-kuruluslarinin-kamunete-dahil-edilmesi-ile-ilgili-201628-sayili-basbakanlik-genelgesi

[19] Detaylı bilgi için bkz. https://www.udhb.gov.tr/doc/kamunetliste.pdf/

[20] http://hgm.udhb.gov.tr/en/sayfa/47

[21] Detaylı bilgi için bkz. http://hgm.udhb.gov.tr/en/sayfa/47

altında ayrı ayrı sürdürülen dijital dönüşüm (e-Devlet), siber güvenlik, milli teknolojiler, büyük veri ve yapay zekâ ile ilgili çalışmaların tek çatı altında toplanması amacıyla, 10 Temmuz 2018 tarihli ve 30474 sayılı Resmi Gazete'de yayımlanarak yürürlüğe giren 1 Sayılı Cumhurbaşkanlığı Kararnamesi kapsamında, T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi kurulmuştur". [22] Bu kapsamda özellikle şu alanlarda çalışmalar yapılması amaçlanmıştır:

"-Yerli ve millî yenilikçi teknolojileri üretmek kadar, bu teknolojilerin kullanımına imkân tanıyacak alt yapıların oluşturulması,

-Bu alt yapı üzerinden iletilen verinin kendi sınırlarımız içinde kalarak yorumlanması,

-Yapay zekâ ile yorumlanan büyük veriden değer ekonomisine geçiş için ihtiyaç duyulan iş süreçlerinin planlanması,

-Siber hâkimiyet alanımız içerisinde güvenliğimizin sağlanmasına kadar birçok alanda faaliyetler yürütülmesi"[23].

Sanal ortamda kurulan her sistem, yeni ve ciddi güvenlik risklerine açıktır. Her ne kadar geçmişte, daha basit, karmaşık olmayan biçimlerde ve çoğunlukla sıradan insanlar tarafından gerçekleştirilse de siber saldırılar günümüzde daha kompleks, profesyonel kişi ve kurumlarca, yapay zekâ algoritmaları ve teknolojileriyle gerçekleştirilmektedir. Dolayısıyla bu saldırılar, başarıya ulaştıklarında çok önemli yıkıcı sonuçlara yol açabilmektedirler. Bu nedenle ülkelerin tıpkı kendi sınır güvenliklerini koruma önlemleri gibi kritik hizmet ve alt yapıları ile onlara ait verileri koruma zorunlulukları bulunmaktadır. Özellikle haberleşme sistem ve alt yapıları, su, elektrik, doğal gaz, akıllı şebekeler, ulaşım sistemleri, barajlar, e-posta, e-ticaret, e-devlet, bankacılık hizmetleri vb. her zaman için potansiyel saldırı hedefleridirler. Bunların kısmen veya tamamen devre dışı kalması demek, o ülkenin bir nevi felç edilmesi anlamına gelir. Bu nedenledir ki "siber güvenlik kara, deniz, hava ve uzaydan sonra beşinci harekât alanı olarak ülkeler için ulusal güvenliğin ayrılmaz ve en önemli bileşeni durumundadır"[24].

Bu temel gerçeklik ve gereksinimden hareketle, Cumhurbaşkanlığı'na bağlı, *"Dijital Dönüşüm Ofisi",* sanayi, özel sektör, üniversite ve STK iş birliğiyle hayata geçirilmiştir. Tüm bu paydaşların aynı amaç çerçevesinde birleşerek, Türkiye'nin siber saldırılara karşı korunmasını sağlamaya çalışmaları büyük önem arz etmektedir

1.1.4. Kişisel Verilerin Korunması Yasası

"*Ulusal Siber Güvenlik Stratejisi*" kapsamında, "kişisel verilerin işlenmesinde kişilerin temel hak ve özgürlüklerinin korunması ve kişisel verileri işleyen tüzel kişilerin yükümlülükleri ile usul ve esasların düzenlenmesi amacıyla 6698 sayılı Kişisel Verilerin Korunması Kanunu, 24/03/2016 tarihinde kabul edilerek 07/04/2016 tarihinde yürürlüğe girmiştir"[25]. Söz konusu yasada yer alan istisnalar dışında, kişisel veriler, ilgili kişinin onayı olmaksızın işlenemez, üçüncü kişilere verilemez veya yurt dışına aktarılamaz. Bununla birlikte, siber saldırıları ve bilgi güvenliği ihlallerini azaltmak adına caydırıcı etken olarak bazı diğer kanun maddelerinden de bahsetmek olanaklıdır. Örneğin, TCK 243, 244 ve 245.

[22]Detaylı bilgi için bkz. https://cbddo.gov.tr/dijital-donusum/
[23]Detaylı bilgi için bkz. https://cbddo.gov.tr/dijital-donusum/
[24]https://cbddo.gov.tr/siber-gvenlik/
[25]"6698 sayılı Kişisel Verilerin Korunması Kanunu", 24 Mart 2016, https://www.mevzuat.gov.tr/MevzuatMetin/1.5.6698.pdf

2. Türkiye'de Bilgi Güvenliği Çalışmaları

Bilgi, iş sürekliliğinin sağlanması sürecinde, bir kurumun en önemli değerlerinden birisidir. "Özellikle internet kullanımının hayatın her alanına yayılmasıyla bilgi, küreselleşen iş dünyasının en ciddi rekabet silahı haline gelmiştir. Bilgi güvenliği, iş sürekliliği, felaket durumlarında kaybın en aza indirilmesi, firmaların yapı taşları sayılan kaynakların her koşulda gizliliğinin, kullanılabilirliğinin ve bütünlüğünün korunması amaçlarını taşır" (lostar.com.tr, 2019). Bilgi güvenliği, çok ciddi bir mesele olup özel bir yapı şeklinde örgütlenmeyi gerektirmiştir. "Dünyada gelişmiş ve gelişmekte olan ülkelerin çoğunda bu konularla ilgili faaliyet gösteren bilgi güvenliği teşkilatları kurulmuş ve faaliyet göstermektedirler" (Yılmaz ve Olay, 2008: 113).

Tüm kurum ve kuruluşlarda bilgi ve veri güvenliğinin tam anlamıyla sağlanması amacıyla kullanılan bilgi teknolojilerinin güncel olması ve bu güncellemelerin güvenlik gereksinimlerini karşılayacak biçimde yapılması gerekmekte olup şu hususların bilgi güvenliği açısından zaafiyet oluşturduğu göz önünde bulundurulmalıdır:

"-Güncel olmayan altyapı öğelerinin kullanılması,
- Uygulama güvenliği önlemlerinin yetersiz olması,
- Varsayılan kullanıcı hesaplarının kullanılması,
- Parola ve güvenlik politikalarının yetersiz olması,
- Güvensiz kabul edilen servislerin kullanılması,
- Sunucularda yapılandırma ve güvenlik sıkılaştırmasının yeterli seviyede yapılmaması,
- Şifreleme anahtar ve algoritmalarının yetersiz olması,
- Ağ yapılandırmasının güvenlik seviyesinin yetersiz olması" (www.lostar.com.tr, 2019).

Bunların yanı sıra, OWASP (Open Web Application Security Project)'ın en kritik 10 Web uygulaması güvenlik zayıflıklarını da göz ardı etmemek gerekir ki bunları başlık olarak şu şekilde vermek olanaklıdır:

"- Siteler arası betik yazma (XSS),
- Enjeksiyon açıkları,
- Zararlı dosya çalıştırma,
- Emniyetsiz doğrudan nesne referansı,
- Siteler ötesi istek sahteciliği (CSRF),
- Bilgi sızıntısı ve uygunsuz hata işleme,
- İhlal edilmiş kimlik doğrulama ve oturum yönetimi,
- Güvensiz kriptografik depolama,
- Güvensiz iletişimler,
- URL erişimini kısıtlamada bozukluk"[26].

2.1 Bilgi Varlıklarının Sınıflandırılması

Yapılan çalışmada, bilgi varlıklarının, "bilginin niteliğine, tutulduğu ortama, saklanmasına, sunulmasına, işlenmesine ya da aktarılmasına ilişkin hususlar göz önünde bulundurularak 6 başlık" (Yılmaz, 2005) altında sınıflandırılmaktadır. Bunları şu şekilde vermek olanaklıdır:

a. "Fiziksel/Elektronik Bilgi Varlıkları: Sunucu ve bilgisayarlar, Depolama ortamları (*manyetik, optik, sabit disk, harici disk gibi*), Haberleşme cihazları (*telsiz, telefon, faks,*

[26] http://csirt.ulakbim.gov.tr/dokumanlar/Ceviri_OWASP_ilk10_2007.pdf ve https://www.cloudflare.com/learning/security/threats/owasp-top-10/

sayısal mesaj iletim cihazları gibi), Girdi/çıktı cihazları (*yazıcı, tarayıcı gibi),* Basılı veya elektronik doküman/belge (*yazışmalar, e-posta, sözleşmeler, ihale dosyaları gibi*), Sosyal medya paylaşımları.

b. Yazılım Bilgi Varlıkları: Veri tabanları - veri dosyaları, İz ve işlem kayıtları, Yazılımlar (*Sistem, uygulama gibi*), Yazılım kaynak kodları ve yazılım yan ürünleri (*Algoritma gibi*).
c. Personel
d. Hizmete dönük varlıklar (Bilgisayar ve iletişim hizmetleri gibi)
e. Soyut değerler (İtibar gibi)
f. Projeler - Kamu ve özel sektör projeleri" (Yılmaz, 2005).

2.2. Kamu Kurumlarının Uyması Gereken Asgari Bilgi Güvenliği Kriterleri

"*Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı", "Kamu Bilgi Güvenliği Programı maddesi"* kapsamında, "bilgi ve iletişim sistemlerinde bulunan güvenlik zaafiyetleri, sistemlerin hizmet dışı kalması ve kötüye kullanılmasının engellenebilmesi amacıyla UDHB tarafından '*Kamu Kurumlarının Uyması Gereken Asgari Bilgi Güvenliği Kriterleri*'"[27] dokümanı hazırlanmıştır. Söz konusu kriterler, ülkemizdeki tüm kamu kurumlarını kapsamakta olup şu durumları içermektedir:

- Yasal gereksinimlere uyum,
- Bilgi güvenliği politikası (*Bir bilgi güvenliği politikası dokümanın yayımlanması*),
- Bilgi güvenliği sorumluluklarının atanması (*Eğitim almış bir uzmanın atanması, USOM ve SOME ile gerekli koordinasyonun sağlanması*),
- Bilgi güvenliği eğitimleri (*Düzenli olarak eğitimlerin verilmesi*),
- "Fiziksel ve çevresel güvenlik,
- Erişim kontrolünün yönetilmesi,
- Yazılım uygulamalarında güvenlik" (www.memurlar.net, 2019),
- Teknik açıklık yönetimi ("*En az iki yılda bir açıklık ve sızma testleri"nin yaptırılması, test neticesinde verilen tavsiyelere uyulması,*)
- İş sürekliliğinin yönetilmesi ("*Kurumsal bilgi ve kayıtların düzenli olarak yedeklenmesi"*),
- Bilgi güvenliği olaylarının yönetilmesi ("*Olayların bilgi güvenliği sorumlusuna bildirilmesi"*),
- Bilgi güvenliği süreci ("*Bilgi güvenliği sorumlusunun yöneticiye düzenli olarak bildirimde bulunması, tavsiyeler üretmesi"*).

Kamu kurumları için minimum bilgi güvenliği ölçütleri belirlenirken, ISO/EIC 27001 ve ISO/EIC 27002 bilgi güvenliği standartlarından yararlanılmıştır. ISO/EIC 27001 standardı, bilgi güvenliği yönetim sürecini tanımlarken, ISO/EIC 27002 ise ISO/EIC 27001'de yer alan önlemlerin detaylı açıklamaları ve uygulamaları yer almaktadır. Bilgi güvenliği ihtiyaçlarını tanımlayan ve uluslararası denetlenebilir bir standart olan *"ISO/27001 Bilgi Güvenliği Yönetimi Sistemi (ISMS)"* ise bilgilerin daha etkin korunması, izinsiz ve yasa dışı yollardan bilgiye erişilmesinin önlenmesi amacıyla oluşturulmuştur.

Söz konusu standardın uygulanması; kamu, "finans, sağlık ve bilgi teknolojileri sektörleri gibi bilginin korunmasının büyük öneme sahip olduğu alanlarda" (www.diamondvision.com.tr, 2019)

[27]"Kamu Kurumlarının Uyması Gereken Asgari Bilgi Güvenliği Kriterleri" (UDHB, 2019).

özellikle gerekmektedir. "*ISO/27001 Bilgi Güvenliği Yönetimi Sistemi*" (BGYS)'nin kurum/kuruluşlarca kurulmasının kurumlara şu konularda katkı sağlayacağı düşünülmektedir:

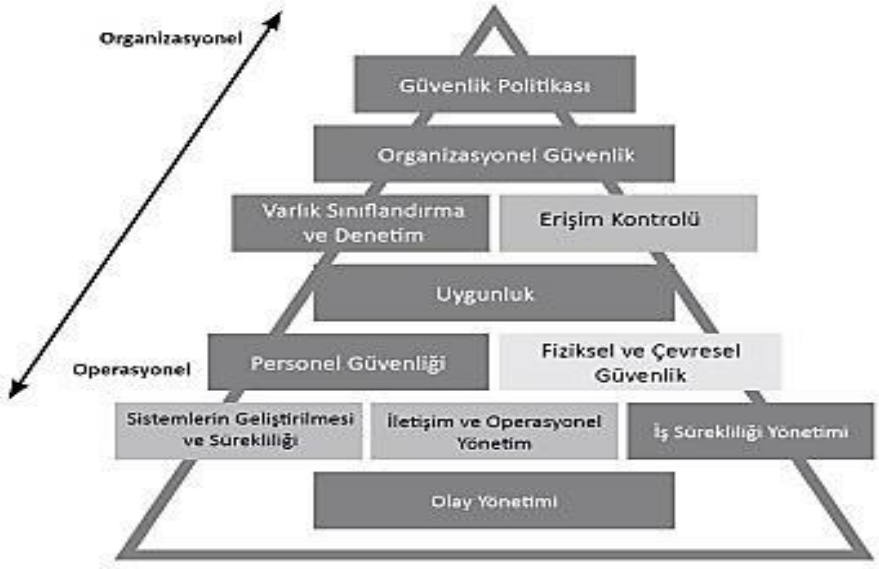
1. Sahip olunan bilgi varlıklarının gerekli kontroller ile korunması,
2. Mevcut bilgi varlıklarının farkına varılması,
3. Olası bir felaket halinde iş sürekliğinin sağlanması,
4. Kurum/kuruluş genelinde, bilgi varlıklarının korunması konusunda farkındalığın artması,
5. Güvenlik politikaları çerçevesinde, mevcut yapı ve kurumların – sistemlerin- kötü amaçlar için kullanımının veya suiistimal edilmesinin engellenmesi.

Standartlar kapsamında "BGYS'in kurulumu, işletilmesi, denetlenmesi-izlenmesi, gerektiğinde gözden geçirilmesi ve hizmetin sürdürülmesi için PUKÖ (Planla- Uygula- Kontrol et-Önlem al) modeli kullanılmaktadır"[28]. PUKÖ modeli özetle aşağıdaki şekilde gösterildiği gibi bir çalışma prensibine sahiptir.[29]

"BGYS'nin kontrol aşamalarının organizasyonel ve operasyonel boyutları, aşağıdaki gibi şematize edilebilir" (Marttin ve Pehlivan, 2010: 51):

[28]Detaylı bilgi için bkz. www.btyon.com.tr (2019).

[29] Detaylı bilgi için bkz. Hasan Yılmaz, "TS ISO/IEC 27001 Bilgi Güvenliği Yönetimi Standardı Kapsamında Bilgi Güvenliği Yönetim Sisteminin Kurulması ve Bilgi Güvenliği Risk Analizi", KİDDER İç Denetçiler Derneği, 2014-2015, s. 53.



3. Fiziksel ve Çevresel Güvenlik

İletişim sistemlerinin, giderek daha fazla ve daha çok kişi tarafından kullanımının artmasıyla birlikte bu sistemlerin güvenliğinin sağlanması gereksinimi de, her geçen gün daha fazla oranda kendini hissettirmiştir. "Sadece teknik önlemlerle (güvenlik duvarları, saldırı tespit sistemleri, antivirüs yazılımları, şifreleme, vb.) kurumsal bilgi güvenliğinin sağlanması yeterli olmamakta, teknik önlemlerin yanı sıra insanları, süreçleri ve bilgi sistemlerini içine alan ve üst yönetim tarafından desteklenen bir yönetim sisteminin gerekliliği de ortaya çıkmıştır" (www.tesladanismanlik.com, 2019). Diğer bir deyişle, bilgi güvenliğinin sağlanması amacıyla kart kontrollü giriş-çıkış, güçlü duvarlar, kameralarla izleme, insanlı güvenlik sistemi vb. gibi fiziksel sınır güvenliğinin de oluşturulması gerekmektedir. "Fiziksel sınır güvenliği, içindeki bilgi varlıklarının güvenlik ihtiyaçları ve risk değerlendirme sürecinin sonucuna göre oluşturulmalıdır. Kurum içerisinde belli yerlere sadece yetkili personelin girişine izin verecek şekilde kontrol mekanizmaları oluşturulmalı ve ziyaretçilerin giriş-çıkış zamanları ve ziyaret sebepleri kaydedilmelidir. Yangın, sel, deprem, patlama ve diğer tabii afetler veya toplumsal kargaşa sonucu oluşabilecek hasara karşı fiziksel koruma tedbirleri alınmış olmalı ve uygulanmalıdır" (www.ab.org.tr, 2019). Ayrıca bahsi geçen fiziksel güvenlik önlemlerine ilave olarak tespit edici güvenlik kameralarının kurulması, felaket kurtarma merkezlerinin farklı yerlerde olması, hat yedekliği, ışıklandırma ve alarm gibi caydırıcı ve tel örgü, kilit gibi geciktirici önlemler ile gerekli kontrollerin yapılması da gerekmektedir.

4. Son Kullanıcı Güvenliği

Kuruluşlar tarafından çoğunlukla ağ geçidi seviyesinde önlemler alınmış olmakla birlikte, bu güvenlik önlemlerinin yeterli olduğunu söyleyebilmek pek olanaklı değildir. Son kullanıcı bilgisayarlarındaki "antivirüs yazılımlarının yanı sıra, host firewall, host IPS, Host DLP gibi çözümlerin kullanımı da gerekmektedir. Host fireall ve host IPS ürünlerinin temel amacı; güvenlik cihazları üzerinden geçmeyen ağ cihazları aracılığıyla yerel ağdan gelebilecek tehditlere karşı savunma sağlamaktır. Host DLP çözümünün amacı ise, kullanıcı cihazına bir araç takılarak istenmeyen verilerin dışarı çıkmasını engellemektir" (www.egisbilisim.com.tr, 2019). Bunların yanı sıra özellikle son zamanlarda daha çok kullanılan mobil, BYOD (Bring Your Own Device – kendi cihazını getir), el terminalleri, dizüstü ve

masaüstü sistemler, misafir bilgisayarları vb. sistemleri önem arz etmektedir. Dolayısıyla riskleri en aza indirmek için sistem(ler) düzenli izlenmeli ve gereken takipler için ilgili çalışmaların yapılması gerekmektedir.

Son kullanıcı bilgisayarlarına ilişkin yaşanan en büyük zaafiyet, "kullanıcı bilgisayarlarının kaybolması ya da çalınması durumundaki içinde barındırdıkları önemli bilgilerin başkaları tarafından ele geçirilebilmesidir. Bu sebeple, özellikle kurum dışına çıkan kurum bilgisayarlarının disk şifreleme çözümleriyle disklerinin şifreleniyor olması büyük önem arz etmektedir" (www.egisbilisim.com.tr, 2019). Bu nedenle, bu tür önlemlerin ulusal düzeyde ve entegre bir sistem olarak oluşturulması büyük önem arz etmektedir.

5. E-posta Güvenliği

Bilindiği üzere e-postalar; günümüz iletişim ağı içerisinde çok önemli bir yer tutmaktadır. Her gün milyonlarca insan e-postalar üzerinde bilgi ve veri paylaşımı yapmakta, gereksinimlerini yerine getirebilmektedir. Aynı şekilde pek çok kişisel veya resmi iletişimler üzerinden işler yürütülmekte, ofisler, kurumlar, kişiler, şirketler hatta ülkeler arasında pek çok konu e-posta üzerinde tartışılmakta, değerlendirilmekte ve fikirler - çözümler paylaşılmaktadır. Bu nedenle, e-posta iletişim sisteminin, zararlı yazılım ve virüslerden korunması ve güvenliklerinin sağlanması gerekir. DDoS (Distributed Denial of Service – dağıtık hizmet engelleme) gibi saldırılar ile e-posta sunucuları çökertilmekte veya kullanılamaz hale getirilebilmektedir. E-postaların güvenliğini sağlayan teknolojiler özellikle şifreleme – sertifikalar, kum havuzu sistemi[30] vb. gibi e-postaların güvenliğini sağlamaya çalışan teknolojiler, sayesinde; e-posta saldırıları, spamlar, oltalamalar ve sahte e-postalar gibi tehlikelere karşı veri bütünlüğü ve güvenliği sağlanabilmektedir.

6. Ağ ve Bulut Teknolojileri Güvenliği

İletişim ve ağ sistemlerin giderek daha fazla büyümesi, karmaşık hale gelmesi, sistemi oluşturan bileşenlerin farklı ve değişik özelliklere sahip olması gibi durumlarda, her ayrı bileşenin güvenliğinin sağlanması kolay olmayacaktır. Ağ içinde hizmet veren sistemlerin ve ağlara erişimlerin kontrol altında olması gerekir. Çünkü ağlar, her an için bir saldırı ile karşı karşıya kalabilirler. Hele çok önemli bilgiler barındıran ağların veri ve hizmetlerinin korunması daha da büyük bir önem arz etmektedir. "Önemli verilerin sadece iç ağdaki kullanıcılar değil aynı zamanda dışarıdan girebilecek kişilere karşıda korunmuş olması gerekir" (www. fazliyildirim.com, 2019).

"Bulut teknolojisi ise bilgisayarlar ve diğer cihazlar için istendiği zaman kullanılabilen ve kullanıcılar arasında paylaşılan kaynakları sağlayan, internet tabanlı bilişim hizmetlerini" (www.garanticomputer.com) ifade etmektedir. Bu teknolojilerin, son zamanlarda, daha çok saklama ve altyapı işlemlerini içeren hizmetlere doğru kaydığını söylemek olanaklıdır. "Bu gidişin ilk öncü uygulamaları, internet sağlayıcıları tarafından, 'yedekleme' amacıyla sunulan bulutlardır. Örneğin, ülkemizde hizmet veren bir internet sağlayıcısı olan 'TTNET','TTNET Bulutu' adlı hizmetle Türkiye piyasasına girmiştir. Google gibi uluslararası bilişim şirketleri ise, 'Google Drive' gibi çevirim içi bilgi

[30]Detaylı bilgi için bkz. https://www.mertsarica.com/kum-havuzu-tespiti/"Kum havuzu sistemine yüklenen bir yazılım, dinamik analiz esnasında hedef bir sistem (c&c) ile haberleşmeye geçtiğinde kum havuzu sistemi tarafından izlenmekte ve kayıt altına alınmakta kısaca bu sistemler üzerinde internetteki bağlantısına izin verilmektedir" (www.mertsarica.com, 2019).

işleme özelliği sunan uygulamalar geliştirmiştir" (www. cansusonmez61142920.wordpress.com, 2019). Bununla birlikte, "Dropbox", "Microsoft" gibi kuruluşlar da bulut hizmeti vermektedir. Ancak bulut bilişim, sunmuş olduğu faydalarının yanı sıra tehlike ve tehditlere karşı kısmen savunmasızdır denebilir. Günümüzde bulut sistemleri kullanımı arttıkça, söz konusu tehditlerin de artacağı açıktır. Özellikle başka bulut sistemlerinin kullanılması veri ekonomisi açısından kayıplar yaratma potansiyeli de taşımaktadır. Dolayısıyla 'gizlilik' üzerine daha fazla risk çalışması yapılması ve tehditlerin azaltılması amacıyla, gerekli önlemlerin alınması büyük önem arz etmektedir.

7. Bilgi Güvenliği Önlemleri

Uluslararası Telekomünikasyon Birliği (International Telecommunication Union) tarafından 2017 yılında 164 ülkede; (i) Yasal Tedbirler, (ii) Teknik Tedbirler, (iii) Organizasyonel Tedbirler, (iv) Kapasite Geliştirme ve (v) İşbirliği kategorileri baz alınarak yapılan Küresel Güvenlik Endeks'inde Türkiye 43. sırada yer almıştır[31].

Türkiye'nin bu alanda daha güvenlikli ortam ve durumlara sahip olabilmesi için bilgi ve bilişim güvenliğine yönelik tehditlerin bertaraf edilebilmesi amacıyla gerekli tedbirlerin alınması önem teşkil etmekte olup kamu kurum ve kuruluşlarında şu tedbirlerin uygulanmasının çok önemli olabileceği düşünülmektedir:

a. Tüm kurum personeline belli periyotlarla şu eğitimlerin verilmesi:

- Bilgisayar açma ve güvenli şifre oluşturma,
- Donanım ve yazılım değişiklikleri yapabilme,
- Dosyaların erişim ve paylaşım işlemlerini yapabilme,
- Taşınabilir medya kullanımı,
- Zararlı yazılım ve virüslerden korunma,
- E-posta sistemlerinin güvenliği,
- Yedekleme,
- Güvenlikli kod geliştirme,
- Güvenlik testleri yapma,
- Düzenli izleme ve müdahale etme,
- Değişiklik yönetimi,
- Yerli ürün geliştirme ve kullanma,
- Siber kalkan geliştirme ve oluşturma,
- Sosyal mühendislik.

b. Kurumda risk analizi çalışmalarının yapılması:

Bu çerçevede ayrıca kritik altyapıların güvenliği de büyük önem arz etmektedir. Kritik altyapıların güvenliği, UAB tarafından hazırlanan "*Ulusal Siber Güvenlik Stratejisi ve 2016-2019 Eylem Planı*"nda; "işlediği bilginin gizliliği, bütünlüğü veya erişilebilirliği bozulduğunda can kaybına, büyük ölçekli ekonomik zarara, ulusal güvenlik açıklarına veya kamu düzeninin bozulmasına yol açabilecek bilişim sistemlerini barındıran altyapılar" (www.bolubeyi.net, 2019) şeklinde ifade edilmektedir.

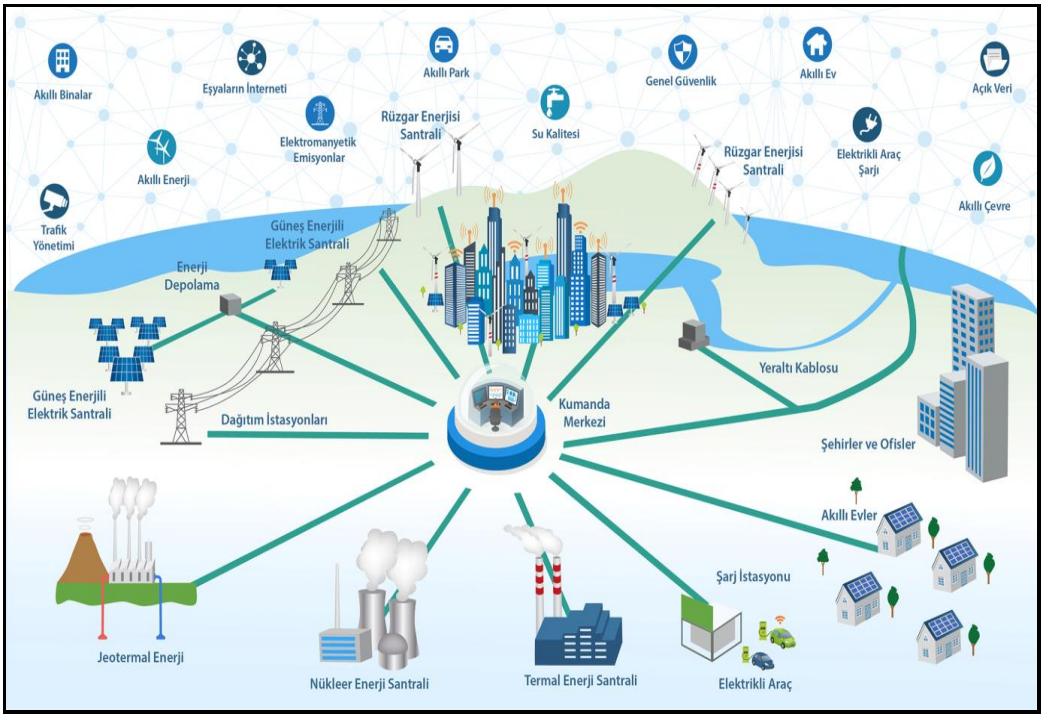
- "Kurumun bilgi varlıkları, bu varlıklara gelebilecek tehditler ve bu tehditlerin oluşturabileceği zararların tespit edilmesi,
- Kurumda veri sınıflandırılması çalışmaları yapılması,

[31]Detaylı bilgi için bkz. http://www.bilgitoplumu.gov.tr/wp-content/uploads/2017/07/global_cybersecurity_index_2017.pdf

- Kurumda çalışan kimliğinin tespiti sürecinin oluşturulması"[32],
- Kurumlarda periyodik olarak bilgi güvenliği testlerinin yapılması,
- Verilerin yedeklenmesi, bilgi varlıklarının korunması (son zamanlarda sıkça rastlanan fidye yazılımlar ile verilerin ve sistemlerin tahrip edilmesine yönelik),
- Antivirüs yazılımlarının tüm bilgisayarlara kurulması ve güncel olması,
- Kuruma ait önemli dokümanların çöpe atılmaması, kırpıcıdan geçirilmesi,
- Bilgisayarlarda şifre koruma uygulamalarının kullanılması.

Esasında sistemlerin ağ durumunu aşağıdaki şemada daha net görmek olanaklıdır. Zira tüm sistemler artık birbirlerine bağlı olduğu gibi, hepsini aynı merkezden kontrol etmek ve dışarıdan gelebilecek olası tehditlere karşı korumak durumundayız. Bu nedenle, entegre – bütünleşik bir yönetim ve bilişim güvenliğinin saplanması büyük önem arz etmektedir.

Şekil: Sistemlerin Ağ Durumu[33]



Aslında "modern kritik altyapılar, çeşitli ağ cihazları, kişisel bilgisayarlar, gözetim kameraları, RFID (Radio Frequency Identification - Radyo Frekanslı Tanımlama) gibi sistemleri kapsamaktadır. Güç tesisleri, su temin sistemleri, elektrik güç gridleri gibi modern kritik altyapı varlıkları; internet gibi büyük bilgi ve iletişim teknoloji altyapıları sistemlerinden farklıdır" (Genge, Kiss and Haller, 2015: 3-17). "Günümüzde 'kritik altyapı' dendiğinde her ne kadar güç tesisleri, elektrik iletim/dağıtım sistemleri, boru hatları gibi endüstriyel kontrol sistemleri aklımıza gelse de; finans, sağlık, telekomünikasyon gibi bilişim sistemlerinin de birer kritik altyapı olduğu unutulmamalıdır" (www.bolubeyi.net, 2019).

Bir bütün olarak bakıldığında "Endüstriyel Kontrol Sistemleri"nin, "SCADA sistemleri" olarak adlandırıldıkları görülmektedir. Fakat "Dağıtık Kontrol Sistemleri (DCS)", "Enerji Yönetim Sistemleri

[32]Detaylı bilgi için ayrıca bkz. www.bilgimikoruyorum.org.tr
[33] Bu şemanın çizimi sürecinde katkıda bulunan RNZ Medya'ya teşekkür ederiz.

(EMS)", "Süreç Kontrol Sistemleri (PCS)" gibi "Denetim Kontrolü ve Veri Toplama Sistemleri (SCADA)" de birer "Endüstriyel Kontrol Sistemleri" olarak kabul edilmektedir.[34] "İleri mühendislik teknikleri ve teknolojik yenilikler ile sahip olunan ve modern dünyanın neredeyse bütün kapılarını aralayan; internet, elektrik, ulaşım, sağlık, eğitim gibi tüm somut altyapılarda, soyut anlamdaki tamamlayıcı altyapı, güvenliktir. Tüm bu altyapı hizmetlerinin kesintisiz, karşılanabilir fiyatlarla ve çevreye duyarlı olarak sunulması için gerekli tedbirlerin alınması, 'güvenliğin sağlanması'" (www.tenva.org, 2019) olarak tanımlanabilmektedir.

Özellikle önemli enerji altyapılarında kullanılan "Endüstriyel Kontrol Sistemleri"nin (EKS) bilişim süreçlerinin sürekliliği ve izlenmesi ile siber tehditler açısından güvenliğinin sağlanması amacıyla 13.07.2017 tarihinde, "Enerji Piyasası Düzenleme Kurumu (EPDK)" tarafından "*Enerji Sektöründe Kullanılan Endüstriyel Kontrol Sistemlerinde Bilişim Güvenliği Yönetmeliği*" hazırlanmış ve "30123 sayılı Resmi Gazete"de yayımlanarak yürürlüğe girmiştir.[35] Söz konusu yönetmelikte yer alan sorumlu kuruluşların EKS'lere yönelik yaptıkları işlemlerin ve bilgi güvenliğine yönelik yaptıkları çalışmaların ve EKS'lerinde kullanılan bilişim sistemleri genel yapısının tanınmasına, bu sistemlerin güvenliğinin sağlanmasına ilişkin risklerin değerlendirilerek azaltılmasına veya ortadan kaldırılmasına yönelik EPDK tarafından;

- EKS Envanter Bildirimi,
- EKS Tanıma ve Risk Değerlendirme Bildirimi,
- Risk Azaltma Aktivite Takibi hazırlanmıştır.[36]

Bunun yanında Eylül 2014 ayında, "T.C. Başbakanlık Afet ve Acil Durum Yönetimi Başkanlığı (AFAD)" tarafından "*2014-2023 Kritik Altyapıların Korunması Yol Haritası Belgesi*" yayımlanmış olup "Kritik Altyapıların Korunması Yol Haritası Belgesi"nin amaçları arasında şunlar yer almıştır:[37]

a. "Afetin neden olduğu zararların en aza indirgenmesi amacıyla, doğal ve teknolojik afetlerde bütünleşik bir yaklaşımla sivil korunmadan sorumlu olanların hazırlığı ve afet durumunda müdahale konusunda ulusal, bölgesel ve yerel seviyedeki çalışmaları desteklemek,
b. Teknolojik afet konusunda sivil korunmayla ilgili AB mevzuatına göre uygulamalar yapabilecek şekilde hukuksal, kurumsal ve teknik çalışmalar yapmayı ve bu mevzuatın özellikle yetkili kurum ve kuruluşlar arasındaki iş birliğiyle ilgili olarak uygulanmasını koordine etmek,
c. Afet izleme ve bilgilendirmesi amacıyla, erken uyarı sistemlerindeki rolleri belirlemek,
d. Ülkemizde bulunan ulusal kritik altyapıları belirleyecek kurum ve kuruluşların koordinasyonunu yapmak" (www.afyonluoglu.org, 2019).

Söz konusu belgede, sektörlere göre sorumlu olan kurum/kuruluşlar aşağıdaki tabloda sunulmuştur:

[34] Detaylı bilgi için bkz. https://ics-cert.us-cert.gov/ (ICS-CERT); Ayrıca, (Cherdantseva Yulia. et all., 2015).

[35] Detaylı bilgi için bkz. "Enerji Sektöründe Kullanılan Endüstriyel Kontrol Sistemlerinde Bilişim Güvenliği Yönetmeliği", Resmi Gazete, 13 Temmuz 2017, http://resmigazete.gov.tr/

[36] http://epdk.org.tr/ (Enerji Piyasası Düzenleme Kurumu)

[37] Detaylı bilgi için bkz. "2014-2023 Kritik Altyapıların Korunması Yol Haritası Belgesi" https://www.afad.gov.tr/upload/Node/3910/xfiles/kritikaltyapi-son.pdf/ (AFAD).

Kritik Altyapı Sektörleri(KAS)	KAS Belirleme Sorumluluk	KAS Güvenlik Sorumluluk (Sektör Bazında)	KAS Güvenlik Sorumluluk (Tesis Bazında)	KAS Koordinasyon Sorumluluk
Enerji	EPDK, Enerji Bakanlığı, TAEK, AFAD	EPDK	İşletme Sahibi (Özel Sektör)	AFAD
Ulaştırma	UDHB, AFAD	UDHB,	İşletme Sahibi (Özel Sektör)	AFAD
Su Yönetimi/Barajlar	Orman ve Su işleri Bakanlığı, AFAD	Orman ve Su işleri Bakanlığı	İşletme Sahibi (Özel Sektör)	AFAD
Haberleşme	BTK, UDHB, AFAD	BTK, UDHB	İşletme Sahibi (Özel Sektör)	AFAD
Bankacılık ve Finans	BDDK,SPK, Hazine Müsteşarlığı, Maliye Bakanlığı, AFAD	BDDK,SPK, Hazine Müsteşarlığı, Maliye Bakanlığı	İşletme Sahibi (Özel Sektör)	AFAD
Kritik Kamu Hizmetleri	İçişleri Bakanlığı, AFAD	İçişleri Bakanlığı	İşletme Sahibi (Özel Sektör)	AFAD
Kritik Üretim/Ticari Tesisler	Bilim, Sanayi , ve Teknoloji Bakanlığı, Gümrük ve Ticaret Bakanlığı, AFAD TOBB	Bilim, Sanayi ve Teknoloji Bakanlığı, TOBB	İşletme Sahibi (Özel Sektör)	AFAD
Sağlık	Sağlık Bakanlığı, AFAD	Sağlık Bakanlığı	İşletme Sahibi (Özel Sektör)	AFAD
Tarım ve Gıda	GTHB, AFAD	GTHB	İşletme Sahibi (Özel Sektör)	AFAD
Kültür ve Turizm	Kültür ve Turizm Bakanlığı, AFAD	Kültür ve Turizm Bakanlığı	İşletme Sahibi (Özel Sektör)	AFAD

Kaynak:"2014-2023 Kritik Altyapıların Korunması Yol Haritası Belgesi" https://pdfslide.net/documents/2014-2023-kritik-altyapilarin-korunmasi-yol-haritasi-belgesi.html

"Elektrik Dağıtım Hizmetleri Derneği (ELDER)" ve "Bilgi Güvenliği Derneği (BGD)" tarafından 08.12.2015 tarihinde, "*Kritik Enerji Altyapılarının Korunması ve Siber Güvenlik Sempozyumu*" düzenlenmiştir. Söz konusu sempozyumun sonuç bildirgesi arasında şu açıklamalar yer almıştır[38]:

a. "Enerji sektöründe bilgi güvenliği farkındalığının arttırılması, eğitim altyapı ve içeriğinin oluşturulması, sektöre özgü siber güvenlik politika ve stratejilerinin belirlenmesi ve çözüm süreçleri geliştirilmesi gibi ana başlıklarda ortak çalışma gruplarının oluşturulması,

b. Siber güvenliğin sağlanmasında en kritik bileşenin insan olduğu" (www.kebak.org, 2019), bu nedenle enerji sektöründe çalışan personel için temel bilgi güvenliği eğitiminin verilmesi, personelin siber güvenlik farkındalığının dinamik tutulması,

c. "Enerji Sektörü Siber Güvenlik Koordinasyon Kurulu" oluşturularak, siber güvenlik çalışmalarının bu kurul tarafından koordine ve takip edilmesi,

d. "Enerji sektörüne yönelik "'Kritik Enerji Altyapılarının Korunmasına Yönelik Politika ve Strateji Belgesi ve Eylem Planı' hazırlanması, bu çalışmanın kritik altyapı olarak tespit edilen diğer sektörler için de yapılmasının gerektiği ile

e. Dağıtım şirketlerinin siber güvenlik durum tespitinin yapılması" (www.kebak.org, 2019),

[38] "Kritik Enerji Altyapılarının Korunması ve Siber Güvenlik Sempozyumu", Bkz. http://www.bilgiguvenligi.org.tr/kritik-enerji-altyapilarinin-korunmasi-ve-siber-guvenlik-sempozyumu-sonuc-bildirgesi

f. Yazılım ve donanım alanlarında, milli çözümler üretilmesi,
g. EKS kullanan kurumlar için EKS-SOME kurulması,
h. USOM'un yıllık faaliyet raporu yayımlaması.

8. Siber Güvenlik Ekosistemi

Ülkemizde siber güvenlik ekosistemi; kamu kurumları, özel şirketler ve üniversitelerden oluşmaktadır. Kamu kurum ve kuruluşlarından Savunma Sanayii Müsteşarlığı (SSM) ve TÜBİTAK Siber Güvenlik Enstitüsü (SGE), akademik çalıştaylar ve özel sektör çalıştayları düzenleyerek siber güvenlikte iş birliği ve bilgi paylaşımına katkıda bulunmaktadır. Bunların yanı sıra ODTÜ, İTÜ ve Bilkent gibi üniversitelerin teknokentlerinde ise birçok siber güvenlik firması faaliyet göstermektedir. Ayrıca; Bilkent, ODTÜ, TOBB ETÜ gibi üniversiteler siber güvenlik üzerine lisans ve yüksek lisans düzeyinde eğitim vermektedir.

Savunma sanayii firmalarından HAVELSAN tarafından, siber güvenlik alanında yatırım yapılmakta ve bahsi geçen üniversitelerdeki akademisyenler ile ortak çalışmalar gerçekleştirilmektedir. Ülkemizdeki siber güvenlik ekosistemini oluşturan kurum ve kuruluşlar aşağıdaki gibi sıralanabilir:

a. Kamu kurum ve kuruluşları: SSM, BTK, TUBİTAK.
b. Özel sektör kuruluşları: HAVELSAN, ASELSAN, ODTÜ Teknokent, Bilkent Cyberpark, İTÜ Arı Teknokent.
c. Üniversiteler: Bilkent İD Üniversitesi, ODTÜ, TOBB ETÜ, İTÜ.

Ayrıca Türk Silahlı Kuvvetleri bünyesinde, "günümüzün muharebe ortamının beşinci boyutu olarak da nitelendirilen bu yeni alanda tehditleri önleyerek, gelişmiş savunma ikaz ve tepki sistemlerine sahip güçlü bir siber savunma yeteneği kazanmak amacıyla 2012 yılında **TSK bünyesinde kurulan Siber Savunma Merkezi Başkanlığı,** 30 Ağustos 2013'te **TSK Siber Savunma Komutanlığı'na** dönüştürülmüştür" (www.webtekno.com, 2019)." *'TSK Siber Savunma Komutanlığı'*, aynı zamanda **NATO** ile de işbirliği içinde olup ulusal güvenlikte yeni bir '**kuvvet çarpanı**' anlayışıyla siber istihbarat, gerektiğinde aktif savunma yapabilme yeteneklerinin kazanılması ve siber caydırıcılığa yönelik milli teknoloji ile ürün geliştirme amaçlı Ar-Ge çalışmalarını da sürdürmektedir"[39]. Bu adımların atılmasının, ilgili kurumsal yapıların oluşturulmasının ülkemiz açısından çok önemli olduğu ve sürdürülmesi gerektiğini vurgulamakta fayda vardır.

SONUÇ

Bilgi, kamu kurum ve kuruluşlarının sahip olduğu en değerli kaynaklar arasında olup en iyi şekilde korunması gereken bir değerdir. Zira bilgi tek başına soyut bir niteliğe sahip olma ya da entelektüel sermaye olmanın da ötesinde günümüzde kamusal açıdan da hizmete dönüşmüş olma noktasında somut bir çıktı haline dönüşmüş durumdadır. Devletin vatandaşlarına sunduğu hizmet bağlamındaki işlevi, bunun aksamasında ya da art niyetli oluşumların eline geçmesinde yaşanacak zararlar ve prestij kaybı, konuya verilen önemin arttırılmasını gerektirmiştir.

Bilgi güvenliği, kurum/kuruluştaki işlerin sürekliliğinin sağlanması, meydana gelebilecek aksaklıkların azaltılması amacıyla bilginin tehditlerden korunmasını sağlamaktadır. Bilgi/bilişim sistemlerine yönelik gerçekleştirilen saldırılar ile sistemlerin tahrip edilmesi, silinmesi, bütünlüğünün veya gizliliğin zarar görmesi mümkün olabilmektedir. "Tek bir güvenlik stratejisi, siber uzay açıklarını ve bununla ilgili tehditleri yok etmeyecektir" (Yılmaz, 2017: 723). Ülkeler, olası risk durumlarını

[39]Detaylı bilgi için bkz. https://www.webtekno.com/internet/tsk-siber-savunma-komutanligi-h17616.html

yönetmek için gerekli tüm önlemleri almalı ve oluşabilecek zararları yok etmek veya en aza indirebilmek için tüm olanak ve kabiliyetlerini hazır ve işlevsel halde bulundurmak zorundadırlar. Zira artık ülkeler arası rekabet ve savaşlar giderek sanal dünyaya kaymaya başlamış durumdadır. Bu bağlamda, kamu kurum ve kuruluşlarında bilgi güvenliğinin sağlanmasına yönelik; asgari kriterlerin uygulanması, yasal mevzuat çalışmalarının tamamlanması, uzman personel eksikliğinin giderilmesi[40] amacıyla üniversitelerde ilgili bölümlerde lisans ve lisansüstü eğitimlerin verilmesi, siber güvenlik akademilerinin kurulması ve ekosisteminin geliştirilmesi, yönetici ve personel seviyesinde farkındalık ve hizmet içi eğitimlerinin düzenlenmesi, yerli ve milli siber güvenlik ürünlerinin geliştirilmesinin önem arz ettiği değerlendirilmektedir. Ülkemizde son yıllarda, 'Türkiye Siber Güvenlik Kümelenmesi' organizasyonu[41] ile bu konuda 'Siber Güvenlik Fikir Yarışması' düzenlenmiş olup çeşitli alanlarda yerli ve milli ürünler üretilmesi konusunda önemli adımların atılmakta olduğu görülmektedir. Kısacası üretim, eğitim, bilinçlendirme, denetim, karşı koyma ve mücadele, sorumluluk ile fırsatları yakalama konularının bilgi ve bilişim güvenliği sürecinde bütüncül bir yaklaşım ile ele alınması gerekmektedir. Bu konuların temel bir devlet politikası yaklaşımı ile desteklenmesi hem ülkemizin güvenliği ve hem de uluslararası siber kaynaklı saldırı ve tehditlere karşı korunabilmek açısından büyük önem arz etmektedir.

Bir süreç tarihi olan insanlık tarihi belli dönemlerden geçerek bilgi toplumu seviyesine ulaşmıştır. Bu geçiş aşamasında ise fiziksel güç ve paraya dayalı sermaye yerini beyin gücü ve bilgiye dayalı sermayeye bırakırken, hiyerarşiye dayalı yönetim yapısı da yönetişim temelinde oluşmaya başlamıştır (Kutlu ve Taban, 2007: 15-21). Gelinen nokta olan bilgi toplumu seviyesi ise bilginin en önemli güç unsuru haline geldiği bir toplum düzeni olarak karşımıza çıkmaktadır (Aktan ve Vural, 2016: 3). Bu noktada bilginin üretilmesi, kullanılması, işlenmesi gibi olguların geçerlilik düzeyini koruması ve günden güne gelişimini arttırması, bir ülkenin küresel ölçekteki rakipleriyle rekabet edebilir hale gelmesine olanak sağlamıştır (Aktel, 2003: 239).

Ancak çalışma içerisindeki ilgili literatüre dayanarak varılan sonuç, Türkiye'nin bilgi toplumu seviyesine henüz erişemediği yönündedir. Türkiye' de bilgisayar ve internet kullanımı oldukça fazla olmasına rağmen Ar-Ge harcamaları için ayrılan bütçe çok düşük bir düzeydedir (TÜİK, 2020a). Sadece bilgisayar ve internet kullanımının bilgi toplumu kavramı ile eş değer olmadığı *"Bilgi toplumunu yakalamış olmak tek başına bilgisayar kullanımının belli bir düzeye gelmiş olması ve ağ teknolojilerinin günlük hayatta yaygın bir biçimde yer almasıyla sınırlı değildir"* (Saran, 2015) sözü ile geçerliliğini korumuştur. Eğitimin, nitelikli insan faktörünün oldukça önem kazandığı toplum düzeninde (Kocacık, 2003: 9), Türkiye' de bilim ve teknoloji alanında nitelik kazanmış insan oranı nüfusa oranla düşük bir seyir izlemektedir (Eurostat, 2020). Bu düzeye erişebilmek adına yeni politikalar geliştirmeli (Bozkurt, 2000: 214), alanın temel taşı niteliğinde olan teknoloji alanına, Ar-Ge faaliyetlerine ve insan faktörüne yatırım yapması gerekmektedir (Aktaş, 2007: 191).

Bilgi kavramı ve beraberinde getirdiği toplum düzeni bu kadar önemli bir çizgide ilerlerken, bilgi güvenliği de üzerinde hassasiyetle çalışılması gereken bir konu haline dönüşmüştür (Koçak ve Memiş, 2018: 1). Gelişen teknoloji ve yaygınlaşan internet kullanımı sonucunda karşımıza çıkan kavram ise siber güvenlik olmuştur (Choucri, 2012: 5; Aktaran: Tarhan, 2017: 5). "*Yakın gelecekte çıkabilecek büyük bir savaşta ilk mermi internette atılacaktır"* sözü ile bilgi güvenliği ve siber güvenlik kavramlarının önemi ve değeri gözler önüne serilmiştir (Nato Güvenlik Danışmanı- Rex Hughes). Yaşanan/yaşanması muhtemel siber saldırılarla bilgi çalınabilir, kötüye kullanılabilir, yetkisiz kişileri eline geçebilir, değiştirilebilir bir unsura dönüşmüştür (Rittinghouse ve Hancock, 2003: 334). Bu

[40]Mesleki Yeterlilik Kurumu (MYT), 'siber güvenlik elemanı – seviye 5' personel tanımı yapmış olup bu sayede kamuda istihdam kolaylaştırılmıştır.
[41] Detaylı bilgi için bkz. http://www.hurriyet.com.tr/teknoloji/yeni-yerli-siber-guvenlik-urunleri-geliyor-41171131

doğrultuda hükümetler ilgili tedbirlerin alınması yönünde adımlar atmış ve faaliyetlerde bulunmuşlardır (Önen ve Kurnaz, 2017: 733).

Türkiye kapsamında bilgi güvenliği ve siber güvenlik alanı ile ilgili gerekli maddi, beşerî ve sosyal sermayeye sahip olunmadığı görülmektedir (Yılmaz vd., 2015: 145). Her ne kadar eylem planları geliştirilse, önemli yapılanmalar oluşturulsa da alanda uzman ve yeterli teknik donanıma sahip insan kaynağının olmadığı yapılan siber güvenlik tatbikatında ortaya çıkmıştır (Bıçakçı, 2013: 45-46). Bu doğrultuda, yerli yazılımların ve bilişim sistemlerinin üretilmesi ve kullanılması, yönetişim esaslı uygulama ve kararlar oluşturulması, geçmiş saldırılardan ders alınarak daha güçlü sistemler oluşturulması, zararın sadece dış kaynaklardan değil iç kaynaklardan da gelebileceğinin bilincinde olarak kurum içi personele ilgili güvenlik eğitimlerin verilmesi aracılığı ile siber güvenlik olgusunun gereklilikleri tam anlamıyla yerine getirilmelidir (Yalçın, 2019: 96-97).

KAYNAKÇA

Akbulut, Bilal (2015) *Güvenlik***,** Ankara: Barış Kitap.

Akyıldız, M. Alparslan (2017) *Uygulamalarla Siber Güvenliğe Giriş,* Ankara: Gazi Kitabevi.

Atıcı, Bünyamin (2005) "Cyber Terror: New Trends and Opportunities", *İstanbul Conference on Democracy and Global Security,* İstanbul, s.791.

Bayazıt, Hüseyin, (2005) "Teknolojik Küreselleşmenin Güvenlik ve Strateji Alanındaki Gelişmelere, Uluslararası Güvenlik ve Strateji Kurumlarının İşlevine ve Yapılanmasına Etkisi", *Gelişen Bilgi Teknolojisi ile Güvenlik Politikası ve Stratejiler Arsındaki Etkileşim ve Yönlendirme Sempozyumu,* 10-11 Mart 2005, İstanbul, Harp Akademileri Basım Evi, s.19-31.

Cherdantseva Yulia, Burnap Pete, Blyth Andrew, Eden, Peter, Jones, Kevin, Soulsby, Hugh ve Stoddart, Kristan (2015) "A review of cyber security risk assessment methods for SCADA systems", *Computers & Security* 56, pp. I-27, September 2015.

Genge, Bela, Kiss Istvan and Haller, Piroska (2015) "A system Dynamics approach for assessing the impact of cyber attacks on critical infrastructures", *International Journal of Critical Infrastructure Protection* IO. pp. 3-17.

Marttin, Vedat ve Pehlivan, İhsan (2010) *"ISO 27001:2005 Bilgi Güvenliği Yönetimi Standardı ve Türkiye'deki Bazı Kamu Kuruluşu Uygulamaları Üzerine Bir inceleme*", *Mühendislik Bilimleri ve Tasarım Dergisi***,** Cilt:1 Sayı:1, s. 51.

Miller, Benjamin (2001), "The Concept of Security: Should it be Redefined", *Journal of Strategic Studies,* Cilt: 24, No. 2, s.16.

O'Brien, Kevin A. (2004) "Information Age Terrorism and Warfare", *Globalisation and the New Terror-The Asia Pacific Dimension-***,** David Martin Jones (Ed.) England, Edward Elgar, s.132.

Sabah Gazetesi (05.06.2016). https://www.sabah.com.tr/gundem/2016/06/05/tsknin-siber-savunma-kuvveti-24-saat-gorevde/

Stolfo, Salvatore (2008)*Insider Attack and Cyber Security-Beyond the Hacker Advances in Information Security,* New York: Spinger, s.63-72.

UDHB (2019) www.udhb.gow.tr http://ulk.ist/destekleyen-kuruluslar/tc-ulastirma-denizcilik-ve-haberlesme-bakanligi/ Erişim tarihi: 03.06.2020Yılmaz, Hasan (2005) "TS ISO/IEC 27001 Bilgi Güvenliği Yönetimi Standardı Kapsamında Bilgi Güvenliği Yönetim Sisteminin Kurulması ve Bilgi Güvenliği Risk Analizi" İç Denetçi, İstanbul Üniversitesi.

Yılmaz, Hasan (2015) "TS ISO/IEC 27001 Bilgi Güvenliği Yönetimi Standardı Kapsamında Bilgi Güvenliği Yönetim Sisteminin Kurulması ve Bilgi Güvenliği Risk Analizi", *KİDDER* İç Denetçiler Derneği, 2014-2015, s. 53.

Yılmaz, Sait (2017)*Uluslararası Güvenlik,* Ankara: Kaynak Yayınları.

Yılmaz, Sait ve Salcan Olay (2008)*Siber Güvenlik ve Türkiye*, İstanbul: Milenyum Yayınları.

İnternet Kaynakları

6698 sayılı Kişisel Verilerin Korunması Kanunu, 24 Mart 2016, https://www.mevzuat.gov.tr/MevzuatMetin/1.5.6698.pdf Erişim tarihi: 11/12/2019.

28447 Sayılı Bakanlar Kurulu Kararı "Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Karar" Resmi Gazete, 20 Ekim 2012, www.resmigazete.gov.tr/eskiler/2012/10/20121020-18.htmErişim tarihi: 01/12/2018.

28683 Sayılı Bakanlar Kurulu Kararı, Resmi Gazete, 20 Haziran 2013, www.resmigazete.gov.tr/eskiler/2013/06/20130620-1.htmErişim tarihi: 05/12/2018.

"2014-2023 Kritik Altyapıların Korunması Yol Haritası Belgesi" https://pdfslide.net/documents/2014-2023-kritik-altyapilarin-korunmasi-yol-haritasi-belgesi.html Erişim Tarihi: 11/12/2019.

"Enerji Sektöründe Kullanılan Endüstriyel Kontrol Sistemlerinde Bilişim Güvenliği Yönetmeliği", Resmi Gazete, 13 Temmuz 2017, http://resmigazete.gov.tr/Erişim tarihi: 13/12/2018.

"Kamu Kurumlarının Uyması Gereken Asgari Bilgi Güvenliği Kriterleri (UDHB)", http://www.udhb.gov.tr/doc/siberg/ASBK.pdf Erişim tarihi: 13/12/2018.

"Kamu Kurum ve Kuruluşlarının KamuNET'e Dâhil Edilmesi ile İlgili 2016/28 Sayılı Başbakanlık Genelgesi", https://www.tbb.gov.tr/www.tbb.gov.tr/basin-ve-yayin/mevzuat-duyurulari/20161205-kamu-kurum-ve-kuruluslarinin-kamunete-dahil-edilmesi-ile-ilgili-201628-sayili-basbakanlik-genelgesi Erişim Tarihi: 13/12/2019.

"Kritik Enerji Altyapılarının Korunması ve Siber Güvenlik Sempozyumu", http://www.bilgiguvenligi.org.tr/kritik-enerji-altyapilarinin-korunmasi-ve-siber-guvenlik-sempozyumu-sonuc-bildirgesi, Erişim tarihi: 13/12/2018.

The White House (2003), "The National Strategy to Secure Cyberspace", The White House, Şubat 2003, s.viii, https://www.us-cert.gov/sites/default/files/publications /cyberspace_strategy.pdf Erişim tarihi: 12/12/2018.

"Türkiye'de E-Devlet: Genel Görünüm" https://www.dijitalakademi.gov.tr/wp-content/uploads/2016/12/TUBITAK-BILGEM-YTE-TurkiyedeEDevletGenelGorunumRaporu2017.pdf Erişim Tarihi: 10/12/2019.

Munger, Jason (2019, https://www.behance.net/gallery/2722993/BRIDGEWAY-ACADEMY Erişim Tarihi: 13/12/2019.

https://www.aa.com.tr/tr/bilim-teknoloji/siber-tatbikat-icin-turkiyeye-gelecekler/1660435, Erişim Tarihi: 11/12/2019.

https://www.aa.com.tr/tr/politika/siber-guvenlik-kanun-taslagi-calismasini-tamamladik/984785 Erişim Tarihi: 10/12/2019.

https://www.btk.gov.tr/tr-TR/Sayfalar/SG-SIBER-GUVENLIK KURULU/ (Bilgi Teknolojileri ve İletişim Kurumu), Erişim tarihi: 02/12/2018.

https://www.btk.gov.tr/siber-guvenlik-tatbikatlari Erişim Tarihi: 10/12/2019.

https://www.btk.gov.tr/tr-TR/Sayfalar/SG-Siber-Guvenlik-Tatbikatlari/ Erişim tarihi: 01/12/2018.

https://www.btk.gov.tr/tr-TR/Kurumdan-Haberler/Siber-Guvenlik-Kurulu-Toplandi/ (Bilgi Teknolojileri ve İletişim Kurumu), Erişim tarihi: 02/12/2018.

https://www.hgm.gov.tr/tr/haber/86/ Erişim tarihi: 12/12/2018.

https://www.hgm.ubak.gov.tr/sayfa/16/ (UDHB Haberleşme Genel Müdürlüğü), Erişim tarihi: 10/12/2018.

https://ics-cert.us-cert.gov/ (ICS-CERT), Erişim tarihi: 11/12/2018.

https://www.sabah.com.tr/gundem/2016/06/05/tsknin-siber-savunma-kuvveti-24-saat-gorevde/ Erişim tarihi: 01/11/2018.

https://www.sge.bilgem.tubitak.gov.tr/tr/kurumsal/sge-tarihcesi/ , Erişim tarihi: 13/12/2018.

http://www.tenva.org (Türkiye Enerji Vakfı), Erişim tarihi: 10/12/2018.

Ulusal Siber Güvenlik Stratejisi ve 2016-2019 Eylem Planı, www.udhb.gov.tr/doc/siberg/2016-2019guvenlik.pdf
http://hgm.udhb.gov.tr/en/sayfa/47 , Erişim Tarihi: 11/12/2019.
https://www.mertsarica.com/kum-havuzu-tespiti/ Erişim tarihi: 27.01.2020.
https://cbddo.gov.tr/dijital-donusum/ Erişim Tarihi: 27.01.2020.
http://www.bilgitoplumu.gov.tr/wp-content/uploads/2017/07/global_cybersecurity_index_2017.pdf Erişim tarihi: 27.01.2020.
http://www.hurriyet.com.tr/teknoloji/yeni-yerli-siber-guvenlik-urunleri-geliyor-41171131 Erişim tarihi: 27.01.2020.
https://www.webtekno.com/internet/tsk-siber-savunma-komutanligi-h17616.html Erişim tarihi: 28.01.2020.
http://csirt.ulakbim.gov.tr/dokumanlar/Ceviri_OWASP_ilk10_2007.pdf ve https://www.cloudflare.com/learning/security/threats/owasp-top-10/ Erişim tarihi: 09.02.2020.
https://www.memurlar.net/haber/761188/tum-mustesar-kadrolari-kaldirildi-mustesarin-gorevini-bakan-yardimcisi-yurutecek.html
www.cybermagonline.com (2019) Erişim 20.12.2019.
www.lostar.com.tr (2019) Erişim 11.12.2019.
www.memurlar.net (2019) Erişim 11.12.2019.
www.diamondvision.com.tr (2019) Erişim 11.12.2019.
www.btyon.com.tr (2019) Erişim 11.12.2019.
www.tesladanismanlik.com (2019) Erişim 11.12.2019.
www.ab.org.tr (2019) Erişim 15.12.2019.
www.fazliyildirim.com (2019) Erişim 15.12.2019.
www.garanticomputer.com (2019) Erişim 15.12.2019.
www.bilgimikoruyorum.org.tr Erişim 17.12.2019.
www.tenva.org Erişim 17.12.2019.
www.kebak.orgErişim 17.12.2019.
www.webtekno.com Erişim 17.12.2019.
www.mertsarica.com Erişim, 17.12.2019