International
SMART Journal
International SOCIAL MENTALITY AND RESEARCHER THINKERS Journal
e-ISSN: 2630-631X

REVIEW ARTICLE
COMPUTER AND TECHNOLOGY

Türkiye'de Siber Güvenlik Ve Bilgi Güvenliği Çalışmaları

Cyber Securıty And Informatıon Securıty Studıes In Turkey

Burçak Akseki [1]
Serdar Meydaneri [2]
Coşkun Taşdemir [3]

ÖZET

Bu çalışmada, siber güvenlik ve bilgi güvenliğinin ne olduğu ve Türkiye'kapsamında yapılan çalışmalar ele alınmıştır. Siber güvenlik ve bilgi güvenliğinin önemli bir konu olduğu ve üzerinde durulması gereken bir alan olduğu anlaşılmıştır. Siber güvenlik ve bilgi güvenliğinin ne olduğu ayrı ayrı açıklanarak tanımlanmıştır. Siber güvenlik, programları, sosyal ağları, sistemleri ve verileri siber saldırıdan korumak amacıyla tehlikelerin önceden analiz edilerek önlem alınmasıdır. Bilgi güvenliği ise verilerin ve bilgilerin yetkisiz kişiler tarafından ele geçirilmesinin önlenmesidir. Siber güvenlik ve bilgi güvenliği kurumların devamlılığının sağlanması, tehlikelerin bertaraf edilmesi adına önemli bir alandır. Bilgi güvenliği kurumlarda sürekliliğin sağlanması konusunda önemli bir değerdir. Kurumlar ve bilgiler var olduğu sürece sürekli gelişim göstermekte ve değişime adapte olması kritik bir noktadır. Tehlike öncesi önlem alma, tehlike anına hazırlıklı olmaktır. Siber güvenlik ve bilgi güvenliği günümüzde sıklıkla üzerinde durulan bir konu olmuştur. Türkiye'de siber güvenlik ve bilgi güvenliği çalışmaları mevzuat ve kurumsal yapılar bağlamında ele alınmıştır. Bu bağlamda bu alanda atılan çalışmalar ve hukuki boyutları değerlendirilmiş, sorumlu kurumlar incelenmiştir. Hukuki mevzuatların ve kurumların gelişiminden bahsedilmiştir. Yasal ve kurumsal altyapı üzerinden yapılacak çıkarımlarla beraber öneriler sunulmuştur. Bu makalenin amacı, siber güvenlik ve bilgi güvenliği perspektifinde Türkiye'de yapılan hukuki düzenlemeler ve sorumlu kurumların tespit edilmesidir.

Anahtar Kelimeler: Siber Güvenlik, Bilgi Güvenliği, Siber Tehlike

ABSTRACT

In this study, what cyber security and information security are and the studies carried out in Turkey are discussed. It has been understood that cyber security and information security is an important issue and an area that needs to be emphasized. Cyber security and information security are defined by explaining separately. Cyber security is the pre-analysis of hazards and taking precautions to protect programs, social networks, systems and data from cyber attacks. Information security, on the other hand, is the prevention of data and information from being captured by unauthorized persons. Cyber security and information security is an important area for ensuring the continuity of institutions and eliminating dangers. Information security is an important value in ensuring continuity in institutions. As long as institutions and information exist, they are constantly evolving and adapting to change is a critical point. Taking precautionary measures is to be prepared for the moment of danger. Cyber security and information security have been a frequently discussed topic today. Cyber security and information security studies in Turkey are discussed in the context of legislation and institutional structures. In this context, the studies in this field and their legal dimensions have been evaluated and the responsible institutions have been examined. The development of legal regulations and institutions has been mentioned. Suggestions are presented along with the inferences to be made on the legal and institutional infrastructure. The purpose of this article is to determine the legal regulations and responsible institutions in Turkey in the perspective of cyber security and information security.

Keywords: Cyber Security, İnformation Security, Cyber Danger

How to Cite This Article
Akseki, B., Meydaneri, S. & Taşdemir, C. (2023). "Türkiye'de Siber Güvenlik Ve Bilgi Güvenliği Çalışmaları", International Social Mentality and Researcher Thinkers Journal, (Issn:2630-631X) 9(73): 3902-3909. DOI: http://dx.doi.org/10.29228/smryj.70755

Arrival: 21 April 2023
Published: 31 July 2023

GİRİŞ

Siber tehditlerin hedefinde bireylerden devletlere kadar tüm gerçek ve tüzel kişilerin olması siber güvenlik ve bilgi güvenliği bireylerin olduğu kadar kurumlarında gereksinimi olmuştur. Siber güvenlik, programları, ağları, sistemleri cihaz ve verileri siber saldırılardan korumak amacıyla üretilmiş, teknoloji, süreç ve kontrollerin uygulanmasıdır. Siber saldırı riskini azaltmak, sistemlerin, ağların ve tekonolojilerin yetkisiz kullanımını önlemek ve korumak istenmiştir (Garantibbva, 2022). Bilgi güvenliği ise bilginin tehdit veya tehlikelerden korunması amacıyla doğru teknolojinin, doğru bir şekilde kullanılarak bilginin varlığının her türlü ortam üzerinde istenmeyen kişiler tarafınca elde edilmesinin önlenmesi olarak tanımlanabilir. Bir başka ifadeyle bilgi güvenliği, tehdit ve tehlikelerden korunmak için gerekli analizin sonucunda gerekli önlemlerin tehdit öncesi alınmasıdır (Beyaz, 2017). Siber güvenlik ve bilgi güvenliği değişen düzen ve teknolojinin sürekli gelişim göstermesiyle üzerinde sıklıkla durulmuş ve geniş bir perspektifte yer almıştır. Tehditlerin

[1-2-3] Öğretmen, MEB, İzmir, Türkiye

önceden analiz edilerek önlemler alınması siber güvenlik ve bilgi güvenliğinin sağlanması konusunda hayati önem taşımaktadır. Bu durum siber güvenlik ve bilgi güvenliğinin ulusal ve uluslararası alanda önemini arttırmıştır. Türkiye'de 1990'lardan bu yana bu çerçevede programlar, eylem planları ve politikalar uygulanmaktadır. Bu doğrultuda önemli çalışmalar gerçekleştirilmiştir. Bu çalışma çerçevesinde siber güvenlik ve bilgi güvenliği alanında atılan adımlar ve Türkiye'deki durum mevzuat odaklı olarak incelenmiştir. Bu çerçevede siber güvenlik ve bilgi güvenliği incelenmiş, akabinde hukuki mevzuat düzenlemeleri ve kurumsal yapılar ele alınmıştır.

SİBER GÜVENLİK

Güvenlik, tarihsel süreç içerisinde üzerinde sıklıkla durulmuş hem dar hem de geniş anlamda tanımlanan çok boyutlu bir kavramdır. ''İnsanlık tarihiyle birlikte alındıklarında, insanın doğa ile mücadelesi içerisinde ekonomik, siyasal, psikolojik, sosyal vb. şekilde yaşamın her boyutunda insanın davranışlarını etkileyen bir kavram''olarak yaşamın her alanını kapsadığı göz ardı edilmemelidir (Dedeoğlu, 2003, s. 279). Tehditlerden, korkulardan ve tehlikelerden uzak olma, korunma anlamına gelmektedir. Siber kavramı ise sibernetik kelime kökünden türetilmiştir. İlk kez 1985 yılında canlılar ve makineler arasındaki etkileşimi inceleyen sibernetiğin babası olarak bilinen Louis Couffignal tarafından kullanılmıştır (SesliSözlük, 2017). Kavramdan sanal alan ve bu alana ilişkin olduğu anlaşılmaktadır. Bu bağlamda Siber güvenlik, programları, ağları, sistemleri cihaz ve verileri siber saldırılardan korumak amacıyla üretilmiş, teknoloji, süreç ve kontrollerin uygulanmasıdır. Siber saldırı riskini azaltmak, sistemlerin, ağların ve tekonolojilerin yetkisiz kullanımını önlemek ve korumak istenmiştir (Garantibbva, 2022). Kavramsal olarak, siber kelimesi bilgisayar ağlarına veya internete ait anlamına gelir. Bu bağlamda ''siber güvenlik''denecek olursa bilgi ve bilgisayar güvenliğinden dijital ortamın bilgi güvenliğine kadar geniş bir yelpazede bahsedilebilir. Siber güvenliğin konusu, ''bilgi silahları'' ve ''bilgi savaşı veya siber savaş'' gibi yeni kavramların güvenlik literatüründe yer bulmasına olanak sağladı (Atıcı, 2005, s. 791). Siber güvenlik, bilgi teknolojisi güvenliği veya elektronik bilgi güvenliği olarak da bilinir. Bir diğer deyişle siber güvenlik, ''farklı kitleler için farklı şeyler ifade etse de, güvende hissetmek, kişisel verileri ve mahremiyeti korumak anlamına gelir'' (Yılmaz, 2017, s. 718).

Siber güvenlik konusunda ilgili kurumlar açısından bakıldığında temel hedef, verilen görevle ilgili olan çok önemli bilgi ve verilerin kullanabilirliğini, korunmasını sağlamakken, ''devletler açısından ise vatandaşların, kurumların, kritik öneme sahip altyapıların ve devlete ait bilgisayar sistemlerinin çökertilmesi ve ele geçirilmesi amacıyla yapılan saldırılara karşı önlemler alınarak verilerin çalınmasını koruma olduğu ifade edilebilir (Yılmaz, 2017, s. 718). Siber ortamlardaki bilişim sistemleri saldırı ve tehditlerden korunmak, korunmak istenen bilginin güvenliğini sağlamak, tehdit ve saldırıların ana kaynağını belirlemek, bu saldırılara karşı hamle ve tedbirler geliştirmek amacıyla oluşturulmuş olup ulusal, uluslararası hukuk ve insan haklarına uygun bütün önlem ve sistemleri siber güvenlik olarak tanımlamak mümkündür (Kara, 2013, s. 5-6). Siber güvenlik önceden öngörülen tehdit ve saldırılara karşı önlem almaktır. Bir diğer anlamıyla siber uzayda kullanıcı, kurum ve kuruluşların güvenliğini sağlamak için kullanılan yöntemler, güvenlik politikaları, eğitimler, uygulamalar ve her türlü teknolojik altyapıdır (BTK, 2008, s. 1-13). Bu bilgiler bağlamında siber uzay siber olana yönelik olarak en geniş kavram olarak karşımıza çıkar. Siber uzay bilgisayar ağlarıyla ve bu ağlarla beraber ulaşılabilen her türlü veri kaynağını kapsayan alan olarak tanımlanmaktadır. Telefon, radyo gibi kumanda edilen elektronik cihazlar, kayıt edilebilen ses ve görüntüler, e-ticaret, e-devlet üzerinden yapılan işlemler siber uzay tanımlamasına uygundur. Siber uzay konusunda başka bir deyişle tanım ABD Savunma Bakanlığı tarafından üretilmiştir. Bu bağlamda siber uzay, ''internet iletişim ağları, işlemci ve kontrol birimlerini içeren bilgi teknolojileri altyapılarının meydana getirdiği, birbirine bağlı ağların oluşturduğu bilgi alanında küresel bir alanı ifade etmektedir'' (Ceylan, 2014). Bu doğrultuda siber güvenlik sayesinde siber tehditler yok edilmekte veya etkisi azaltılarak en aza indirilebilmektedir. Bu adımları atabilmek hayati bir önem taşır. Siber saldırılar, bir ülkedeki tüm yaşamı durdurabilecek ve felaketlere yol açabilecek bir yapıya sahiptir. Tehditlerin artmasıyla güvenliğin daha çok tehlikeye düşmesi sonucu birçok ülke, siber güvenlik konusuna güvenlik politikalarında yer vermiştir (Yıldız, 2014, s. 58). Siber güvenlik, sistem, ağ ve programları dijital saldırılara karşı korumaktır. Bu siber saldırılar, hassas bilgilere ulaşmak, değiştirmek, kullanıcılardan para çekmeyi ve iş sürecini kesintiye uğratmayı amaçlar. Günümüzde her anlamda ve her alanda siber savunma programlarından yararlanıldığı görülür. Bireysel alanda bakıldığında bir siber güvenlik saldırısı, kimlik bilgilerinin çalınmasından, zorla sistemlerimize girme denemelerine ayrıca önemli verilerin kaybolmasına kadar her şekilde sonuçlanabilir. Tüm bu neticeler bağlamında altyapının korunması ve kuruluşların güvence altına alınması toplumumuzu çalışır durumda tutmak için esastır.

Siber güvenliğin temel olarak yedi ilkeden oluştuğu söylenebilir. Siber güvenliğin en üst aşamada sağlanması için uygulanan ilkeler aşşağıdaki gibi tanımlanabilir (Uzun & Çakır, 2021, s. 358).

Gizlilik : Amaç, sanal dünyada oluşturulan bilgilerin yetkili kişiler veya ilgili sistemler tarafından erişilebilir olmasını sağlamaktır.

Bütünlük : Bilginin, dış etkenlerle temas etmeden kaynaktan çıktığı anda alıcıya ulaşmasıdır.

Erişebilirlik : bilginin izin verilen yetkili kişi ve sistemlerin gerektiğinde verilere ulaşabilmesidir.

İzlenebilirlik : Sistemde meydana gelen her bir olayın analizi ve kaydıdır.

Kimlik Doğrulama : Üretilen bilgilerin kaynağı olan alıcının, gönderenin ifade ettiği kişi olduğu şüphesiz bilinmelidir.

Güvenilirlik : Sistemin amacına uygun olarak çalışması, dış etkenlerle temas etmemesi ve elde edilen sonuçların beklentileri karşılamasıdır.

İnkar Edememe : Mesajın gönderen tarafından alıcıya gönderildiği kanıtlanabilir.

TÜRKİYE'DE SİBER GÜVENLİK

Ulusal siber güvenlik yol haritası çizebilmek adına mevzuatlar üzerinde yapılan düzenlemeler siber güvenlik alanında Türkiye'de atılan ilk adımlardan biridir. Siber güvenliğin sağlanması konusunda hukuksal altyapı olarak 5237 Sayılı Türk Ceza Kanunu'na bazı hükümler eklendi. Elektronik ağlar aracılığıyla işlenen suçlar davada ağırlaştırıcı sebep olarak kabul edilmiş ve elektronik ağlarla ilgili suçlar kanunun onuncu bölümünde ''Kanundaki Suçlar'' başlığı altında yer almıştır. 2004 yılında 5070 Sayılı Elektronik İmza Kanunu ile de güvenlik anlamında ilk adım atılmıştır (Tamyapar, 2019, s. 10). Türkiye'de 1990 ların sonlarına doğru Milli Savunma Bakanlığı'nın koordinatörlüğünde bilgi güvenliği organizasyonu ve görevleri ile ilgili bir çalışma yapılmıştır. Bu kanunla, devletin bilgi güvenliğinin sağlanmasına yönelik olarak hükümetin himayesinde ve Bilgi Güvenliği Başkanlığında bir üst komutanlık oluşturulması planlanmış ancak uygulanması konusunda mutabakata varılamamıştır. Derleme aşamasında durdurulmuştur. Bir diğeri ise 5070 Sayılı Elektronik İmza Kanunu'nun yürürlülüğe girmesidir. Bu kanunun birinci maddesinde ''elektronik imzanın esasları ile kullanımının hukuki ve teknik yönlerini düzenlemek'' ibaresi yer almaktadır. Ayrıca 5237 Sayılı Yeni Türk Ceza Kanunu'nun Yürürlülüğe girmesinden de bahsedilebilir. Siber alandaki özgürlükleri de ihmal etmemiştir. 3713 Sayılı Terörle Mücadele Kanunu'nda yapılan değişiklikle beraber bilişim suçları ''terör amacıyla işlenen suçlar''kapsamına alınmıştır. Böylece Türkiye'de siber güvenlik konusunun ilk kez terörizmin faaliyet sahası olabileceği kanun tarafından kabul edilmiştir. Yasal düzenler bağlamında yapılan diğer çalışmalar ise 2007 yılında 5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun'un yürürlülüğe girmesi, 2008 yılında 5809 Sayılı Elektronik Haberleşme Kanunu, 2009 E-Devlet ve Bilgi Toplumu Kanunu Tasarı şeklinde ifade edilebilir (Karasoy & Babaoğlu, 2021, s. 135-137). Türkiye Siber Güvenlik Kurulu ilk toplantısını 21 Aralık 2012 tarihinde UDHB Bakanı başkanlığında gerçekleştirdi. Bu kapsamda ''Siber Güvenlik Kurulu görev, faaliyet, usul ve esasları ile yönergesi'' ile ''2013-2014 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı''onaylandı. İkinci toplantı 20 Haziran 2013 tarihinde gerçekleşti. Bu toplantı 15 Mayıs 2013 tarihinde faaliyete geçen ''Ulusal Siber Olay Müdahale Merkezi''nin oluşturulması ile sonuçlandı. Üçüncü toplantı ise 2016 yılında gerçekleştirildi. Ayrıca 2013 yılında Türk Silahlı Kuvvetleri bünyesinde Siber Savunma Komutanlığı kurulmuştur (Erdoğan, 2023, s. 15).

Türkiye'de siber güvenlik konusunda yapılan çalışmalara baktığımız zaman Bilgisay Olaylarına Müdahale Ekibi (TR BOME), Bilgi Toplumu Stratejisi ve Bilgisayar Acil Müdahale Merkezi kurulması faaliyete geçirilmiştir (Hekim & Başıbüyük, 2013, s. 140). Siber güvenlikle ilgili bir diğer çalışmada ulusal düzeyde siber güvenliğe yönelik politikaların, stratejilerin ve eylem planlarının oluşturulması ve SGK sekreterlik hizmetlerinin ''Amerika Birleşik Devletleri tarafından tanımlandığı şekliyle'' UAB'ye sağlanmasıdır. 28447 Sayılı Bakanlar Kurulu gereğince. Ayrıca siber güvenlik konularında strateji ve eylem planları oluşturmak, kamu kurum ve kuruluşlarının altyapısını oluşturmak, bu yapıların doğruluğunu test etmek ve farkındalıkla ilgili eğitim araştırmaları yapmakla görevlendirildiler. Bu kapsamda UDHB koordinasyonunda ilgili kurum ve STK'ların katkılarıyla ''Ulusal Siber Güvenlik Stratejisi ve Eylem Planı 2013-2014'' hazırlanmış ve bu plan SGK tarafından onaylanmıştır (Erdoğan, 2023). 2015-2018 Bilgi Toplumu Stratejisi ve Eylem Planı ile sürece devam edilmiştir. Bilişim teknolojilerinin her alanında Türkiye'nin kalkınması hedeflenerek kamu politikası çalışması geleneğine devam edilmiştir. 2016 – 2019 ve 2020 – 2023 yılları ulusal siber güvenlik stratejisi ve eylem planları oluşturulmuştur. Siber güvenliğe ilişkin ilk stratejik belgenin Ulusal Siber Güvenlik Stratejisi ve Eylem Planı 2013-2014 olduğu ve bu belgenin bir öncü olduğu söylenebilir. Ulaştırma ve Altyapı Bakanlığı,2020 – 2023 ulusal siber güvenlik stratejisi ve eylem planını hazırladı ve Cumhurbaşkanlığı genelgesi ile birlikte yayınlandı. Siber güvenliğin ulusal güvenliğin ayrılmaz bir parçası olduğu belirtilmiştir. Bu eylem planının kamuoyu ile paylaşılan stratejik amaçları şu şekilde sıralamak mümkündür : (UAB, 2021).

1. Kritik altyapıların korunarak mukavemetin arttırılması
2. Ulusal kapasitenin geliştirilmesi
3. Organik siber güvenlik ağı
4. Yeni nesil teknolojilerin güvenliği
5. Siber suçlarla mücadele
6. Yerli ve milli teknolojilerin geliştirilerek desteklenmesi
7. Siber güvenliğin milli güvenliğe entegrasyonu
8. Uluslararası iş birliğinin geliştirilmesi

Tüm bunların yanı sıra Türkiye'de siber güvenlik alanında yer alan kurum ve kuruluşların varlığı söz konusudur. Bu kuruluşlara bakıldığında TÜBİTAK'tan bahsetmek mümkündür. Tübitak bünyesindeki kuruluşlarla beraber Türkiye'de 2012 yılı öncesi siber güvenlik alanında bu görevi üstlenmiştir. Tübitak bünyesinde bulunan UEKAE, Türkiye'nin ilk kurumların taşıdığı risk analizlerin yapmıştır. Marmara Araştırma Merkezi bu bünyede yer alan bir diğer önemli kuruluştur. Bu kuruluşlar 2010 yılında tek çatı altında birleşerek BİLGEM adını almıştır.bu bağlamda Tübitak'ın Ulaştırma ve Altyapı Bakanlığı ile birlikte uyumlu bir şekilde çalıştığı BİLGEM vasıtasıyla siber güvenlik alanında görevler üstlenmeye devam ettiği söylenebilir. Türkiye'deki siber güvenlik alanındaki kuruluşlardan bir başka kuruluş olan Bilgi Teknolojileri ve İletişim Kurumundan bahsetmek mümkündür. 2000 yılında 4502 sayılı kanunla Telekomünikasyon kurumu adıyla kurulmuştur. 2014 yılında siber güvenlik ve alan adları konularında verilen görevleri yerine getirme görevi verilmiştir. Bir diğer kuruluş Cumhurbaşkanlığı Dijital Dönüşüm Ofisidir. Bu kuruluşa asıl görevlerinin yanı sıra bilgi güvenliği ve siber güvenliği arttırıcı görevlerde verilmiştir. Bu bağlamda bu ofiste Siber Güvenlik Daire Başkanlığı birimi de bulunmaktadır. Aynı zamanda Ulaştırma ve Altyapı Bakanlığı'da bu alanda çalışmaları olan bir kuruluştur. 2012 yılında Tübitak'tan ''Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Karar''la görevleri devraldığını söylemek mümkündür. Bu kuruluşların yanı sıra Türkiye'de siber güvenlik alanında çalışmalar yürüten Afad gibi kuruluşların varlığı da söz konusu olmuştur (Karasoy & Babaoğlu, 2021, s. 146-149). Ayrıca kamu sanal ağ projesi çerçevesinde kamu güvenlik ağı ''kamu sektörü kurum ve kuruluşlarının içerik güvenliği ile kurumlar arası kapalı daha güvenli bir sanal ağ üzerinden sağladığı bilgi iletişimini, riskleri en aza indiren ortak merkezleri kapsayacak şekilde uygulama altyapısı oluşturulmuş ve ortak bilgilendirme planlanmıştır. Bir diğer husus olarak da Kamu Entegre Veri Merkezinin varlığından bahsedilebilir. Bir diğer husus olarak da Kamu Entegre Veri merkezinin varlığından bahsedilebilir. KEVM, kamuya açık bilgi kaynaklarının ve bilgilerin izlenmesi, düzenlenmesi, bilgilerin tek bir merkezden saklanması ve sunulması amacıyla oluşturulmuştur.

BİLGİ GÜVENLİĞİ

Bilgi, iş sürekliliğini sağlamak için kuruluşun en önemli varlıklarından biridir. ''Özellikle internetin hayatın her alanına yaygınlaşmasıyla bağlantılı olarak, küreselleşen iş dünyası ciddi bir rekabet aracı haline gelmiştir.'' Bilgi güvenliğinin, iş sürekliliği, felaket durumlarında kaybı en aza indirmek, firmaların yapı taşlarını oluşturan kaynakların gizliliği, kullanabilirliği ve bütünlüğünün korunması amaçlarını taşıdığı söylenebilir (Lostar, 2019). Bilgi güvenliği, bilgileri tehdit veya tehditlerden korumak için doğru teknolojiyi kullanarak istenmeyen kişilerin herhangi bir yolla bilgiye erişmesini engellemek olarak tanımlanabilir. Bir başka ifadeyle bilgi güvenliği, tehdit ve tehlikelerden korunmak için gerekli analizin sonucunda gerekli önlemlerin tehdit öncesi alınmasıdır (Beyaz, 2017). Aynı zamanda bilginin izinsiz bir şekilde erişilmesi,kullanılması, değiştirilmesi, açıklanması, ortadan kaldırılmaya çalışılması, el değiştirilmesi ve zarar görmesinin sağlanması gibi tehditleri önlemektir. Gizlilik, bütünlük ve erişebilirlik unsurlarının korunmasıdır (TKDK, 2018). Bilgi, kurumun içinde önem taşıyan diğer varlıklar gibi korunması gereken bir varlıktır. Bu bağlamda bilgi güvenliği, kurumdaki işlerin istikrarının sağlanması, aksaklıkların önlenmesi ve yatırımların sağlayacağı faydanın artması hususunda bilginin geniş çaplı tehditlerden korunması oldukça önemlidir. Gerek elektronik ortamlarda, gerek sözlü olarak, gerek kağıt üzerinde yazılı bir şekilde vb. yöntemlerle bilgi bir yerden bir yere iletilebilir. Bu bağlamda hangi yöntemle olursa olsun uygun bir şekilde korunmalıdır. Bilgi güvenliği, bütünlüğü, gizliliği ve kullanabilirliliği hedefler (İk, 2019, s. 1). Sağlanan servis ve sistem verilerinin korunmasını sağlar. Bilgi çok çeşitli alanda olabilmektedir. Bu bağlamda bilgi güvenliği, mobil bilişim, siber adli tıp, sosyal medya vb. gibi pek çok alanı kapsamaktadır. Bilgi güvenliği bilgiye karşı olan tehditlerle ilgilenir. Bilgi güvenliğinin yedi tane unsuru bulunmaktadır. Bunlar sırasıyla şu şekildedir. Bu unsurların başında güvenilirlik gelmektedir. Güvenilirlik unsuru, sistemlerin kurulmasından sonra sistemlerden beklenen davranış ve sonuç arasındaki tutarlılıktır. Kurulan sistemin istenilen gibi çalışıp

çalışılmadığının gözlemi sistemin güvenilirlik unsurunu ortaya çıkarmaktadır. Bir diğer unsur bütünlük unsurudur. Bütünlük unsuru, bilginin yetkisi olmayan kişilerce değiştirilmemesini ifade etmektedir. İki tür bütünlük vardır. Veri bütünlüğü ve sistem bütünlüğüdür. Veri bütünlüğü, bilgileri yetkisiz değişikliklere karşı korumayı, sistem bütünlüğü ise sistemin yetkisiz değişikliklerden korunmasını amaçlar. Bilgi güvenliğinde yer alan bir diğer unsur kimlik tespitidir. Bilgiye erişmek isteyen kullanıcının kimliğinin doğrulanarak tespit edilip sistemde kayıtlı olup olmadığının kontrol edilmesidir. Bir diğer unsur inkar edememe unsurudur. Bilginin gönderilmesi durumunda bilgiyi gönderen ve alan kişinin bilginin paylaşılmadığını inkar edememesidir. Gizlilik unsuru ise bilginin yetkisiz kişilerin eline geçmesinin engellenmesidir. Bu hususta önemli olan bir diğer unsur ise Log (kayıt) tutmadır. Bir sistemdeki olayların, saat, kullanıcı adı ve eylem türünden otomatik olarak kaydedilmesidir. Sonuncu unsur ise erişebilirliktir. Bu bağlamda bilginin yalnızca yetkisi olan kişiler tarafından erişilebilir olmasını ifade eder (CyberMag, 2022).

Bilgi güvenliği, başlanıp bitirilecek bir iş değildir. Kurumlar ve bilgi var olduğu sürece sürekli yönetilmesi ve gözden geçirilmesi gereken bir yaşam döngüsüdür (Eminağaoğlu & Gökşen, 2009, s. 9). Bilgi güvenliğini sağlamak kurumlara pek çok faydayı beraberinde getirir. Bu faydaları şu şekilde açıklayabiliriz :

Bilgi güvenliği ihlallerini önleme, rekabet üstünlüğü, yasal yönden sorun yaşanmasını engelleme, üçüncü taraflara güven verme, bilgisayarların verimli kullanılmasını sağlama, siber saldırı risklerinden korunma vb. gibi birçok şekilde sıralanabilir (Çubukçu, 2018, s. 4). Bilgi güvenliği, kişisel bilgisayarlardan tüm kurumsal ve ulusal bilgi sistemlerine ve kritik altyapılara kadar çok çeşitli alanlarda bilgi sistemlerini kapsayan bir güvenlik yönetimi yaklaşımıdır. bu bağlamda genel olarak bilgi güvenliği, ciddi bir konu olarak ele alınmaktadır. Bilgi güvenliği, siber güvenlik gibi önlem mekanizmasının oluşması için son derece önemli bir yer edinmiştir. Tehdit öncesi güvenlik tedbirlerinin alınarak tehdit anında savunma mekanizmasının harekete geçirilebilirliğidir.

TÜRKİYE'DE BİLGİ GÜVENLİĞİ ÇALIŞMALARI

Türkiye'de bilgi güvenliği bağlamında yasal mevzuat çalışmaları, Anayasa ile kanunlarda geçen kişisel hak ve özgürlüklere dair konuların yanı sıra bilişim güvenliği ve suçlarına ilişkin hükümler etrafında değerlendirilebilir. Bu bağlamda Türkiye'de yürürlülükte olan hukuki çalışmalar şöyle sıralanabilir.

Türkiye'de bu hukuki düzenlemelerin başında 1982 Anayasası gelmektedir. Bu anayasaya göre madde 19 kişi hürriyeti ve güvenliğini tanımlamakta, madde 20 özel hayatın gizliliğini tanımlarken haberleşme hürriyetinin tanımlandığı madde 22 ise bilişim güvenliği ve suçları kapsamında ele alınan konular bağlamında önem taşır. Bu anayasaya göre kişisel veriler, kanunda öngörülen haller ve kişinin açık rızasına göre işlenebilmektedir. Herkesin kendisiyle ilgili kişisel verilerin korunmasını isteme hakkı olduğu açıktır. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenmektedir. bu bağlamda işletme ve kurumlar, muhafaza ettikleri kişisel verilerden son derece sorumludur. Bilgi güvenliği kapsamında yapılan bir diğer hukuki düzenleme ise 5237 Sayılı Türk Ceza Kanunu'dur. Bu kanun kapsamında bilgi güvenliği geniş bir perspektif içerisinde çizilmiştir. Böylece bilişim sistemine giriş, sistemi engelleme, bozma veya yok etme, haberleşmenin engellenmesi, hakaret, haberleşmenin gizliliği, kişiler arasındaki konuşmanın kayıt altına alınması ve dinlenmesi, özel hayatın gizliliğinin ihlal edilmesi, kişisel verilerin kaydedilmesi, kişisel verileri yok etmeme, dolandırıcılık, banka ve kredi kartlarını kötüye kullanma gibi konular yer almış ve bütün bunlar bilişim suçları olarak nitelendirilmiştir. Bir diğer çalışma ise 5809 Sayılı Elektronik Haberleşme Kanunudur. Bu kanunla beraber bilgi güvenliği temel ilkeler arasında yer alır. Bilgi güvenliği ve haberleşme gizliliğinin korunması kanun kapsamında hüküm altına alınmıştır. Ayrıca işletme ve kurumlara haberleşmede gizliliğin sağlanması gibi görevler verilmiştir. Türkiye'de bu alanda yer alan bir diğer hukuki çalışma olarak 5070 Sayılı Elektronik İmza Kanunu'ndan bahsedilebilir. Bu kanun bilgi güvenliğini ilgilendiren bir takım bilişim suçlarını kapsamı içerisine alır. Elektronik imza oluşturma verilerinin izinsiz kullanımı ve elektronik sertifikalarda sahtekarlık suçları, bu kanun kapsamında öne çıkar. 5651 Sayılı İnternet iletimlerinin düzenlenmesi ve bu iletimler yoluyla işlenen suçların önlenmesine dair kanun, içeriki, yer ve paylaşım sağlayıcıların sorumluluk ve yükümlülüklerini belirlemektedir. Ayrıca bilgi güvenliği kapsamında 5846 Sayılı Fikri ve Sanat Eserleri Kanunu'yla herhangi bir eserin çoğaltılması, yayılması veya temsil hakkı eser sahibine verilmiştir. 6698 Sayılı Kişisel Verilerin Korunması Kanunu'na göre kişisel veri, belirli veya belirlenebilir bir kişiye dair olan her türlü bilgiyi ifade etmektedir. Kişisel veri, bu kişiye ait olmalıdır ve bu kişinin belirlenebilir nitelikte olması gerekir. Bu kanunla kişisel verilerin işlenmesinde özel hayatın gizliliği, temel hak ve özgürlükleri korumak böylece kişisel verileri işleyen gerçek ve tüzel kişilerin uyması gerekenlerin usul ve esaslarının düzenlenmesi amaçlanmıştır. Bu bağlamda 6279 Sayılı Çoğaltılmış Fikir ve Sanat Eserlerini Derleme Kanunu, İnternet Alan Adları Yönetmeliği gibi öne çıkan yasal mevzuatlar ile bilginin farklı yönleriyle korunduğunu görmek mümkündür (BilgiGüvende, 2021).

Türkiye'de bilgi güvenliğinin korunması kapsamında bilgi sistemleri denetimi alanında çalışma yapan kurumların varlığındanda bahsedilebilir. Bu kurumlara bakıldığında Bankacılık Düzenleme ve Denetleme Kurumundan (BDDK) bahsetmek mümkündür. Türkiye'de bankacılık sektöründe düzenleme ve denetleme yetkisi BDDK' ya aittir. Bankalarda bilgi sistemleri denetimi 5411 Sayılı Bankacılık Kanunu kapsamında temelleri atılmıştır. Bu bağlamda bankalarda kullanılan verilerin korunması ve bilgi güvenliğinin sağlanması bağlamında çalışmalar yapılmıştır. Bir diğer kurum olarak Sermaye Piyasası Kurulu söylenebilir. Türkiye'de sermaye piyasaları konusunda düzenleme ve denetleme yetkisi SPK'dedir. Kurul, Sermaye Piyasası Kanunu'na göre bağlı bulunan kuruluşların bilgi sistemlerinin denetlenmesi, bilgi güvenliğinin sağlanması, bağımsız ve güvenli bir şekilde yürütülmesi vb. amaçlar doğrultusunda gözetim ve denetim yapar. Bilgi güvenliği konusundaki kuruluşlardan bir diğeri ise T.C. Maliye Bakanlığı İç Denetim Koordinasyon Kurulu (İDKK) dur. Bu konuda Sayıştay, Hazine Müsteşarlığı ve Bilgi Teknolojileri ve İletişim kurumu gibi kurumların varlığı ile de Türkiye'de bilgi güvenliğinin sağlanmaya çalışıldığı gözlemlenebilir (Meral, 2016, s. 29-50). Aynı zamanda Türkiye'de bu mevzuatlar ve kurumların yanı sıra birçok çalışmanın varlığı söz konusudur.

SONUÇ

Bu çalışmada siber güvenliğin tanımı ve önemi ele alınmış aynı zamanda Türkiye'de siber güvenlik çalışmaları tespit edilmiştir. Ayrıca bilgi güvenliği ve Türkiye'deki bilgi güvenliği çalışmaları değerlendirilmiştir. Siber güvenliğin önemli bir konu olduğu ve Türkiye'de bu konu kapsamında hukuki düzenlemelerin varlığı ve siber güvenliğin sağlanması hususunda kurumların sıklıkla çalışmalar yaptığı görülmüştür. Siber güvenliğin tehlike boyutunun büyük olduğu ve neticesinde büyük olumsuzluklar getirdiği, kurum itibarının sarsılmasına neden olabileceği gibi dezavantajlarının olduğunu söylemek mümkündür. Siber güvenliğin sağlanması, kurumların itibarının zedelenmemesi ve tehidtlerin önceden analiz edilerek önlenmesi konusunda bir dayanak olmuştur. Siber güvenliğin sağlanmasında programların, sanal ağların, cihazların, bilgilerin vb. dayanakların korunması istenmiş ve bu doğrultuda gerekli önlemlerin alınarak etkin kurumların varlığının sağlanması ve hukuki mevzuatların düzenlenmesi ve bu mevzuatlara uyulması beklenmiştir. Türkiye'de siber güvenlik kapsamı çerçevesinde yapılan hukuki düzenlemelerin tarihsel süreç içerisinde varlığını hissettirdiğini söylemek ve her yapılan düzenlemenin bir önceki düzenlemenin devamı niteliğinde olduğundan bahsetmek mümkündür. Bu bağlamda yapılan hukuki mevzuat çalışmaları ve eylem planlarının genişletilmesinin ve alınan önlemlerin sürekli gelişen ve değişen teknolojik çerçeveye uyum sağlamasının varlığının gerektiğini söylemek mümkündür. Siber güvenlik, tehlikelerden korunmadır. Tehlikelerle baş edebilmek bağlamında Türkiye'de çeşitli kurumların kurulduğu ve bunların yetersiz olduğu söylenebilir. Yapılan çalışmaların daha aktif ve somut bir perspektifte yapılmasının sağlanması gerekir. Yapılan çalışma neticesinde siber güvenlik olgusunun günümüzün değişen ve gelişen dünyasında önemli bir yere sahip olduğu görülmüştür. Türkiye'de siber güvenlik çalışmaları, çalışmanın yeteri kadar gelişme göstermediğini tam anlamıyla hayata geçirilmediğini göstermiştir. Siber güvenlik, bireylerden devlete kadar tüm gerçek ve tüzel kişilerin güvenliklerinde göz ardı edilemeyecek kadar önemli bir yere sahiptir. Siber saldırılar neticesinde devletlerin hizmet mekanizmaları sarsılabilmekte, gerçek ve tüzel kişilerin varlıklıkları olumsuz etkilenebilmektedir. Bu sebeblerden ötürü siber saldırıların ve siber güvenliğin tehlikeye düşmesi bir savaş meydanını ortaya çıkardığını söylemek yanlış olmayacaktır. Türkiye siber güvenlik konusunda bir hayli yol kat etmiş önemli çalışmalarla devlet mekanizması ve toplumun siber güvenliğini sağlamayı amaçlamıştır. Yapılan siber güvenlik çalışmaları, teknik ve işlevsel tedbirlerin alınması, kurumsal yapılanmanın oluşturulması, işbirliğinin sağlanmasıyla beraber eksik kalan sorunlar zaman içerisinde çözüme kavuşturulacaktır. Bu kapsamda siber sektörün güvenliğini sağlamak için hassas alanların farklı değerlendirilmesi gerekmektedir. Aynı zamanda bilgi güvenliği, kağıt üzerinde bir zorunluluk ya da sertifika almak değildir. Güvenlik sadece teknolojik problem olarak değil, insan ve yöntem problemi olarak de ele alınmalıdır. Bilgi güvenliği, bilgilerin yetkisiz kişiler tarafından ele geçirilmesinin, işgal edilmesinin veya değiştirilmesinin önlenmesidir. Kritik bir öneme sahiptir. Bu netice itibari ile Türkiye'de bilgi güvenliği alanında yasal mevzuat çalışmaları ve bu güvenliğin sağlanması konusunda çeşitli işletme ve kurumların olduğunu söylemek mümkündür. Ancak elde edilen veriler neticesinde Türkiye'de bilgi güvenliği kapsamındaki çalışmaların yetersiz olduğunu söylemek yanlış olmayacaktır. Bu kapsamda yapılan hukuki düzenlemelerin arttırılması ve mevcut mevzuatların bilgi güvenliği konusunda gözden geçirilmesi ve eksikliklerin tespit edilmesi gerekmektedir. Ayrıca bilgi güvenliğinin sağlanması konusunda var olan kurumların daha somut çalışmalar yürütmesi gerekmektedir.

Sonuç olarak siber güvenlik ve bilgi güvenliği kritik bir öneme sahip olan iki ayrı konudur. Bu iki konu üzerinde gerekli önemin verilmesi ve Türkiye'nin bu konuları güvenlik açısından odak noktada görmesi ve ele alması gerekir. Tüm bu durumlar neticesinde yapılan çalışmaların gelişen ve değişen dünya düzeni ve teknolojik değişimliği yakalayacak şekilde sürekli güncellenmesi ve yeni adımların atılması ve çalışmaların

sürdürülmesi Türkiye'nin siber güvenlik ve bilgi güvenliği alanında başarılı olmasına doğrudan katkı sağlayacaktır.

KAYNAKÇA

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

Beyaz. (2017). *Bilgi Güvenliği*. Retrieved 05 30, 2023, from beyaz.net web sitesi: https://www.beyaz.net/tr/guvenlik/makaleler/bilgi_guvenligi.html

BilgiGüvende. (2021, 12 14). *Türkiye'de Bilgi Güvenliği Odağındaki Yasal Mevzuatlar*. Retrieved 03 31, 2023, from bilgigüvende.com web sitesi: https://bilgiguvende.com/turkiyede-bilgi-guvenligi-odagindaki-yasal-mevzuatlar/

BTK. (2008). *Bilgi Teknolojileri ve İletişim Kurumu*. Retrieved 03 23, 2023, from Siber Güvenlik Ulusal ve Ulaslararası Boyutları web sitesi: https://www.btk.gov.tr/File/?path=ROOT%2F1%2FDocuments%252%20FSayfalar%2FSiberGuvenlik%2FUlusalVeUluslararasiBoyutlariileSG.pdf

Ceylan, H. (2014, 11 10). *Siber alan-siber uzay nedir*. Retrieved 03 23, 2023, from Halukceylan.wordpress web sitesi: https://halukceylan.wordpress.com/2014/11/13/siber-alan-siber-uzay-nedir/

CyberMag. (2022, 09 27). *Bilgi güvenliği nedir*. Retrieved 05 30, 23, from cybermagonline.com web sitesi: https://www.cybermagonline.com/bilgi-guvenligi-nedir-bilgi-guvenligi-nasil-saglanir

Çubukçu, F. (2018). *Bilgi Güvenliği Yönetim Sistemi Uygulama Kılavuzu* . İstanbul: Pusula Yayıncılık.

Dedeoğlu, B. (2003). *Uluslararası Güvenlik ve Strateji.* İstanbul: Derin Yayınları.

Eminağaoğlu, M., & Gökşen, Y. (2009). Bilgi Güvenliği Nedir, Ne Değildir, Türkiye'de Bilgi Güvenliği ve Çözüm Önerileri. *Dokuz Eylül Üniversitesi Sosyal Bilimler Enstitüsü Dergisi* , 1-15.

Erdoğan, S. (2023). Türk Kamu Sektöründe Bilgi ve Bilişim Güvenliği. *Bitirme Projesi* . Kütahya: Kütahya Dumlupınar Üniversitesi.

Garantibbva. (2022, 12 01). *garantibbva*. Retrieved 03 23, 2023, from siber güvenlik nedir web sitesi: https://www.garantibbva.com.tr/blog/siber-guvenlik-nedir

Hekim, H., & Başıbüyük, O. (2013). Siber Suçlar ve Türkiye'nin Siber Güvenlik Politikaları. *Uluslararası Güvenlik ve Terörizm Dergisi* , 135-158.

İk, K. (2019, 09 12). *Bilgi Güvenliği Politikası*. Retrieved 03 30, 2023, from Kolayik.com web sitesi: https://kolayik.com/wp-content/uploads/2020/02/bilgi-guvenligi-politikasi.pdf

Kara, M. (2013). Sibel Saldırılar-Sibel Savaşlar ve Etkileri. *Yüksek Lisans Tezi* . İstanbul: İstanbul Bilgi Üniversitesi Sosyal Bilimler Enstitüsü.

Karasoy, A., & Babaoğlu, P. (2021). Türkiye'de Siber Güvenlik : Yasal ve Kurumsal Altyapı . *Yasama Dergisi* , 125-155.

Lostar. (2019). *Bilgi Güvenliği Nedir*. Retrieved 03 30, 2023, from lostar.com.tr web sitesi: https://lostar.com.tr/2023/01/cbddo-bilgi-ve-iletisim-guvenligi-rehberi-uyum-surecinin-yonetilmesi.html

Meral, E. (2016). Türkiye'de Bilgi Sistemleri Denetimi ve Kamu Gözetimi Kurumu'nun Bilgi Sistemleri Denetiminde Üstlendiği Misyon. *Uzmanlık Tezi* . Ankara: T.C. Kamu Gözetimi Muhasebe ve Denetim Standartları Kurumu Bilgi Sistemleri Yönetimi Daire Başkanlığı.

SesliSözlük. (2017, 11 30). *Sesli Sözlük*. Retrieved 03 23, 2023, from cyber-nedir-ne-demek web sitesi: https://www.seslisozluk.net/cyber-nedir-ne-demek/

Tamyapar, B. (2019). Siber Güvenlik ve Türkiye'de Yürütülen Siber Güvenlik Çalışmaları. 1-16.

TKDK. (2018). *Bilgi Güvenliği Yönetim Sistemi*. Retrieved 03 30, 2023, from tkdk.gov.tr web sitesi: https://www.tkdk.gov.tr/Kurumsal/BGYS

UAB. (2021, 01 30). *Ulusal Siber Güvenlik Stratejisi ve Eylem Planı 2020-2023*. Retrieved 03 26, 2023, from hgm.uab.gov.tr.siber güvenlik stratejisi web sitesi: https://hgm.uab.gov.tr//

Uzun, S. A., & Çakır, H. (2021). Türkiye'nin Siber Güvenlik Eylem Planlarının Değerlendirmesi. *Ekonomi İşletme Siyaset ve Uluslararası İlişkiler Dergisi* , 353-379.

Yıldız, M. (2014). Siber Suçlar ve Kurum Güvenliği. *Uzmanlık Tezi* . Ankara: Ulaştırma Denizcilik ve Haberleşme Bakanlığı.

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