Necmettin Erbakan Üniversitesi Siyasal Bilgiler Fakültesi Dergisi
(NEUSBF Dergisi)
Journal of the Faculty of Political Science (NEUSBF)
DOI: 10.51124/jneusbf.2023.56

Cilt: 5 Sayı: Özel Sayı Yıl: 2023 | Araştırma Makalesi / Research Article | E-ISSN: 2687-5063

Bilgi Güvenliği ve Elektronik Harp*

Erdal Bayrakcı[1] **Mehmet Ali Koçman**[2]

[1] Doç. Dr., Necmettin Erbakan Üniversitesi, Konya, Türkiye, ebayrakci@erbakan.edu.tr

[2] Siyaset Bilimi ve Kamu Yönetimi Uzmanı, Türkiye, malikocman@yandex.com, *(Sorumlu Yazar / Corresponding Author)*

Makale Bilgileri

Makale Geçmişi

Geliş: 30/10/2023
Kabul: 04/12/2023
Yayın: 17/12/2023

Anahtar Kelimeler: Elektronik Harp, Bilgi Güvenliği, İstihbarat, Kişisel Verilerin Korunması, Kamu Yönetimi

Jel Kodları: D8, Z18, O3, L9, K1, F5

ÖZ

Bilgi, günümüzde bireylerin ve kurumların kendilerine özgü, birey ve kurum hakkında insanlara kimlik kazandıran her türlü veriden meydana gelmektedir. Günümüzde bilginin oluşumun da bireylerin zihinlerinde oluşan veriler neticesinde, insanları harekete geçiren ve verilerin bir bütün olarak anlamlı hale gelmesiyle oluşmaktadır. Çalışma da bilgi güvenliği ve kişisel verilerin korunmasına yönelik incelemeler ve günlük hayatta kullanımı değerlendirilmektedir. Bilginin yönetim sürecinde bilgi sınıflandırılması ve bilginin hangi sınıflarda ne tür verileri işlendiğine dair konular incelenmektedir. Bilgi, yüzeysel bilgi, derin bilgi, teknik ve uygulanabilir bilgi, yoruma dayalı bilgi, açık ve örtülü bilginin ne ifade ettiği ele alınmıştır. Bilgi yönetim sisteminde, bilginin sınıflandırılması ve verilerin işlenişi detaylı olarak ele alınmıştır. Çalışma da bilgi kavramı, bilgi yönetimi, dijital bilgi ve bilgi güvenliği, risk yönetimi ve risk analiz raporlarının hazırlanmasına ilişkin konularda bilginin etkin ve aktif olarak nasıl kullanılacağına dair durum değerlendirilmesi yapılmakta ve elektronik harp' in tanımı ve unsurlarına yer verilmektedir.

Information Security and Electronic Warfare

Article Info

Article History

Received: 30/10/2023
Accepted: 04/12/2023
Published: 17/12/2023

Keywords: Electronic Warfare, Information Security, Intelligence, Personal Data Protection, Public Administration

Jel Codes: D8, Z18, O3, L9, K1, F5

ABSTRACT

Today, information consists of all kinds of data that are unique to individuals and institutions and that give people an identity about the individual and the institution. Nowadays, the formation of knowledge occurs as a result of the data formed in the minds of individuals, which mobilizes people and the data becomes meaningful as a whole. In the study, investigations regarding information security and protection of personal data and its use in daily life are evaluated. In the information management process, the classification of information and the subjects of which types of data are processed in which classes are examined. It is explained about knowledge, superficial knowledge, deep knowledge, technical and applicable knowledge, interpretive knowledge, explicit and implicit knowledge. In the information management system, the classification of information and the processing of data are discussed in detail. In the study, a situation assessment is made on how to use information effectively and actively on the issues related to the concept of information, information management, digital information and information security, risk management and the preparation of risk analysis reports, and the definition and elements of electronic warfare are included.

Atıf/Citation: Bayrakcı, E. & Koçman, M. A. (2023**).** Bilgi Güvenliği Ve Elektronik Harp, *Necmettin Erbakan Üniversitesi Siyasal Bilgiler Fakültesi Dergisi*, *5*(Özel Sayı), 184-206.

* Bu çalışma Necmettin Erbakan Üniversitesi Sosyal Bilimler Enstitüsü'nde savunularak kabul edilen "Bilgi Güvenliği Bağlaminda Kişisel Verilerin Korunmasi ve Elektronik Harp" başlıklı yüksek lisans tezinden faydalanılarak hazırlanmıştır.

GİRİŞ

Bilginin özgürce aktığı ve teknolojinin hayatımızın her alanına nüfuz ettiği günümüzde, bilgi güvenliği ihtiyacı son derece önemli hale gelmiştir. Hükümetler, kuruluşlar ve bireyler benzer şekilde, siber suçluların ve kötü niyetli aktörlerin sürekli olarak güvenlik açıklarından yararlanmaya ve hassas verilere yetkisiz erişim sağlamaya çalıştığı, sürekli büyüyen bir tehdit ortamıyla karşı karşıyadır. Bilgi güvenliği, değerli bilgi varlıklarını korumak için sürekli ihtiyat, yenilik ve aktif önlemler gerektiren en önemli endişe konusu haline gelmektedir. Bu çalışma, bilgi güvenliği alanını derinlemesine inceleyerek önemini, zorluklarını ve kapsamlı koruma stratejilerini ortaya koymaya çalışmaktadır. Dijital teknolojinin ortaya çıkışı çeşitli alanlarda devrim yaratmıştır. Dijital çağ, insan davranışını, siyasi dinamikleri ve bilginin yayılmasını anlamada yeni fırsatlar ve zorluklar ortaya çıkarmaktadır. Sosyal medya platformlarından büyük veri analitiğine kadar dijital araçlar, araştırmacılara, politika yapıcılara ve iletişimcilere çok büyük miktarda veriye eşi benzeri görülmemiş erişim ve izleyicilerle etkileşim kurmanın yeni yollarını sağlamaktadır.

Dijital teknolojilerin ve birbirine bağlı sistemlerin hızla büyümesiyle birlikte, siber istihbarat, siber risklerin belirlenmesinde ve azaltılmasında çok önemli bir rol oynamaktadır. Siber istihbarat, büyük miktarda veriyi analiz ederek ve dijital faaliyetleri izleyerek, ortaya çıkan tehditleri tespit edebilir, saldırıları belirli aktörlere atfedebilir ve kritik varlıkları korumak için proaktif stratejiler geliştirebilir. Çalışmanın amacı, bilginin güvenli bir şekilde saklanması, iletimi ve kişisel verilerin korunmasına ilişkin literatürdeki bileşenlerinin temel olarak günümüzde elektronik harp kapsamına girdiği, elektronik harbin sadece askeri alanda değil kamu yönetimlerinde, sosyal yaşamda beşerî ilişkiler ile bir bütün olduğunu açıklamaktır.

1. BİLGİ GÜVENLİĞİ KAVRAMI ve ELEKTRONİK HARP

Bilginin değerli bir para birimi olarak hizmet ettiği ve veri ihlallerinin geniş kapsamlı sonuçları olabileceği modern dijital çağda, bilgi güvenliği alanı her zamankinden daha önemli hale gelmektedir. Birbirine bağlı teknolojilere olan güvenimiz arttıkça, elektronik harbin dijital varlıkları bozma, manipüle etme ve tehlikeye atma potansiyelinin de arttığı bilinmektedir. Geleneksel olarak askeri operasyonlarla ilişkilendirilen elektronik harp, etkinliğini bilgi güvenliği alanınada genişletmiştir (Çalışkan, 2023).

Teknolojik savunmaları proaktif stratejiler, uluslararası iş birliği ve politika çerçeveleriyle birleştirmek, elektronik harpten kaynaklanan riskleri azaltmak ve dijital dünyamızın güvenliğini ve bütünlüğünü sağlamak için çok önemli olacaktır. Giderek birbirine bağlanan bir dünyada bilgi, ekonomileri, toplumları ve hatta siyasi olayları şekillendiren en değerli varlıklardan biri haline gelmektedir. Ancak dijitalleşmedeki artışla birlikte bu değerli kaynağın kırılganlığı da artmakta ve bilgi güvenliği alanında elektronik harbin ortaya çıkışı, sürekli gelişen siber tehditler ve savunmalar manzarasına yeni bir boyut kazandırmaktadır (Çalışkan, 2023). Devlet destekli aktörler ve siber suç örgütleri, ağlara sızmak, hassas verileri çalmak ve rekabet veya stratejik avantaj elde etmek için elektronik harp taktiklerini kullanarak siber casusluk faaliyetlerinde bulunmaktadır. Özel bilgilerin, ticari sırların ve sınıflandırılmış verilerin dışarı sızması, ulusal güvenlik ve kurumsal çıkarlar için önemli riskler oluşturmaktadır. Sosyal medya ve çevrimiçi platformlar aracılığıyla yanlış veya yanıltıcı bilgilerin yayılması, modern bilgi savaşı cephaneliğinde güçlü bir silah olarak nitelendirilmektedir. Elektronik harp, genellikle siyasi sistemleri istikrarsızlaştırma veya kurumlara olan güveni baltalama niyetiyle yanlış bilgileri çoğaltmak, anlaşmazlık çıkarmak ve kamuoyunu manipüle etmek için kullanılmaktadır (Özdemir ve Uluyol, 2021).

1.1. Bilgi Güvenliği ve Bilgi Yönetim Sistemleri: Dijital Dünyada Verilerin Korunması

Günümüzün veri odaklı dünyasında bilgi, bir işletmenin veya kuruluşun sahip olduğu en değerli varlıklardan biridir. Bu bilgilerin etkili yönetimi ve korunması, gizliliğinin, bütünlüğünün ve kullanılabilirliğinin sağlanması açısından çok önemlidir. Bilgi güvenliği ve bilgi yönetimi sistemleri, hassas verilerin korunmasında, uyumluluğun sürdürülmesinde ve verimli operasyonların desteklenmesinde hayati bir rol oynamaktadır (Yılmaz vd., 1989).

1.2. Bilgi Yönetim Sistemi

Bilgi Yönetim Sistemi, bir kuruluş içinde bilgilerin toplanması, düzenlenmesi, saklanması ve dağıtılmasına yönelik yapılandırılmış bir yaklaşımdır. Verileri ve bilgiyi etkili bir şekilde yönetmek için teknolojinin, süreçlerin ve politikaların kullanımını içermektedir (Alagöz ve Allahverdi, 2011). İyi tasarlanmış bir bilgi yönetim sistemi, bilgi akışını kolaylaştırır, karar almayı geliştirir ve genel iş operasyonlarını desteklemektedir. Bir bilgi yönetim sisteminin bileşenleri, veri yönetimi, veri toplama, depolama ve alma süreçlerini içermektedir. Doküman Yönetimi ise dokümanları, kayıtları ve dosyaları verimli bir şekilde yönetmeyi ve bir organizasyon içerisinde bilginin organize edilmesi, saklanması ve paylaşılmasını kapsamaktadır (Yılmaz vd., 1989). İş akışı yönetiminde verimliliği artırmak için iş süreçlerini otomatikleştirmek ve optimize etmek ve son olarak kayıt yönetimi, veri saklama ve imha konusunda yasal ve düzenleyici gerekliliklere uygunluğun sağlanmasını içermektedir. Bilgi Güvenliği, gizliliğin, bütünlüğün ve kullanılabilirliğin korunması olarak, bilgiyi yetkisiz erişime, ifşa edilmeye, değiştirilmeye veya yok edilmeye karşı koruma uygulamasıdır (Alagöz ve Allahverdi, 2011). Temel amaç, verilerin gizliliğini, bütünlüğünü ve kullanılabilirliğini sağlamaktır.

1.3. Bilgi Güvenliğinin Temel İlkeleri

Bilgi güvenliğinin, gizlilik, bütünlük, kullanılabilirlik, kimlik doğrulama, yetkilendirme, şifreleme ve güvenlik politikaları olmak üzere yedi temel ilkesi vardır. Bu ilkeler kısaca aşağıdaki şekilde ifade edilebilir (Yılmaz, 2014):

Gizlilik: Hassas bilgilere yalnızca yetkili kişilerin erişiminin sağlanması,

Bütünlük: Verilerin doğru, güvenilir ve yetkisiz değişikliklerden arınmış olduğunun garanti edilmesi,

Kullanılabilirlik: Veri ve sistemlerin ihtiyaç duyulduğunda kullanılabilir ve erişilebilir olmasını sağlamak,

Kimlik Doğrulama: Kullanıcıların ve varlıkların kimliğinin doğrulanması,

Yetkilendirme: Kullanıcı rolleri ve ayrıcalıklarına göre bilgiye erişimin kontrol edilmesi,

Şifreleme: Verileri güvenli, okunamaz bir formata dönüştürerek korumak,

Güvenlik Politikaları: Bilgi güvenliği uygulamalarına yönelik kuralların ve yönergelerin tanımlanmasıdır.

Bilgi güvenliğini bilgi yönetim sistemi ile birleştirmek güçlü bir sinerji yaratır. Entegre bir yaklaşım, verilerin yalnızca iyi yönetilmesini değil aynı zamanda iyi korunmasını da sağlamaktadır. Güvenlik kontrolleri, erişim kısıtlamaları ve şifreleme, verilerin, belgelerin ve bilginin yönetimine sorunsuz bir şekilde entegre edilebilir. Bilgi güvenliği genellikle düzenleme ve uyumluluk gereksinimleriyle iç içe geçmiş durumdadır. Bir bilgi güvenliği yönetim sistemi, kuruluşların sektöre özel yasa ve standartlarla uyumluluğunu sürdürmesine yardımcı olabilir ve aynı zamanda düzenleme amacıyla denetim ve raporlamayı kolaylaştırabilir (Atılgan, 2009). Bilgi güvenliği ve bilgi yönetimi sistemleri, bir kuruluş içindeki verilerin etkili ve güvenli bir şekilde işlenmesini destekleyen iki önemli unsurdur. İşletmeler ve kurumlar, sağlam bilgi güvenliği, yönetim sistemi ve kapsamlı bilgi güvenliği önlemlerini uygulayarak, düzenlemelere uyarken ve riskleri en aza indirirken verilerin gizli, doğru ve erişilebilir kalmasını sağlayabilir (Martinn ve Pehlivan, 2010). Verilerin değerli bir varlık olduğu ve tehditlerin hedefi olduğu bir çağda, bu uygulamalar dijital dünyada bilgilerin korunması için hayati öneme sahip olmaktadır. Sürekli genişleyen ve birbirine bağlanan dijital ortamda, bilgi güvenliği ve siber güvenlik alanları birbirinden ayrılamaz hale gelmekte olup, bunlar, hassas verileri ve dijital altyapıyı giderek artan tehditlere karşı korumak için birlikte çalışan aynı madalyonun iki yüzü olarak bu iki alan arasındaki ilişkiyi anlamak, dijital dünyamızı korumak açısından kritik öneme sahiptir (Martinn ve Pehlivan, 2010).

1.4. Bilgi Güvenliği ve Siber Güvenlik

Bilgi güvenliği, şekli ne olursa olsun, verilerin yetkisiz erişime, ifşa edilmeye, değiştirilmeye veya yok edilmeye karşı korunmasına odaklanmaktadır. Bu sadece dijital verileri değil aynı zamanda fiziksel belge ve kayıtları da kapsamaktadır. Bilgi güvenliğinin temel amacı veri gizliliğini, bütünlüğünü ve

kullanılabilirliğini korumaktır (Yılmaz, 2014). Siber güvenlik ise özellikle dijital sistemlerin, ağların ve verilerin siber tehditlerden korunmasıyla ilgilenir ve kötü amaçlı yazılım, bilgisayar korsanlığı, kimlik avı ve hizmet reddi saldırıları gibi daha geniş bir risk yelpazesini içermektedir. Siber güvenlik, dijital ortamı bu dış tehditlere karşı korumayı amaçlamaktadır. Hem bilgi güvenliğinin hem de siber güvenliğin merkezinde verilerin korunması yer alırken bilgi güvenliği daha kapsamlı olup her türlü veriyi içerirken, siber güvenlik ise özellikle dijital verilerin korunmasını ele almaktadır. İkisi birbirine bağlıdır çünkü hassas belgelere yetkisiz erişim gibi bilgi güvenliği ihlalleri, veri hırsızlığı veya fidye yazılımı saldırıları gibi siber tehditlere yol açabilir (Atılgan, 2009). Bilgi güvenliği çalışmaları, verilerin gizli kalmasını sağlar ancak siber güvenlik, bu gizliliği ihlal etmeyi amaçlayan saldırılara karşı savunmadan sorumludur. Şifreleme ve erişim kontrolü önlemleri, verileri yetkisiz erişime karşı koruyarak siber güvenliği doğrudan etkileyen bilgi güvenliği uygulamalarına örnektir.

Günümüzün dijital çağında, bilgi güvenliği ve siber güvenlik birbirinden ayrı kavramlar değil, verileri ve dijital altyapıyı korumaya yönelik birleşik bir çabanın derinden iç içe geçmiş yönleridir. Siber dünyada gelişen bir dizi tehdidi engellemek için kolektif olarak çalışarak birbirlerini tamamlamaktadır. Teknoloji ilerledikçe ve siber tehditler daha karmaşık hale geldikçe, bilgi güvenliği ile siber güvenlik arasındaki ilişkinin önemi daha da artacaktır. Kuruluşlar ve bireyler, bu birbirine bağlı yapının farkına varmalı ve dijital varlıklarını korumak için kapsamlı güvenlik stratejileri uygulamalıdır. Sonuçta herhangi bir kuruluşun siber güvenlik çabalarının başarısı, bilgi güvenliği uygulamalarının gücüne bağlıdır (Çelik, 2018). Kuruluşlar, bu iki alan arasındaki etkileşimi tanımalı ve sürekli gelişen siber ortamda ortaya çıkan tehditlere karşı dirençli kalabilmek için veri korumayı ve daha geniş dijital ortamı kapsayan bütünsel bir güvenlik stratejisine yatırım yapmalıdır.

Genellikle "siber savaş" veya "siber çatışma" olarak adlandırılan ancak aslında elektronik harp bileşeni olan siber dünyada bilgi savaşı, dijital alanda stratejik hedeflere ulaşmak için bilgi ve iletişim teknolojilerinin kullanılmasını içeren bir savaş biçimidir (Çelik, 2018). Geleneksel savaşın aksine, bilgi savaşı öncelikle düşmanın bilgi sistemlerini, verilerini ve iletişim ağlarını hedef alır ve çeşitli şekillerde avantaj elde etmeyi, bozmayı, manipüle etmeyi veya avantaj elde etmeyi amaçlamaktadır. Bilgi savaşı ulus devletler, hacktivist gruplar ve diğer kuruluşlar tarafından belirli hedefler doğrultusunda yürütülür ve çeşitli biçimlerde olabilir. Bilgi savaşı çeşitli şekillerde karşımıza çıkmaktadır. Bunlardan ilki, siber saldırılardır. Siber saldırılar, bir hedefin ağını veya web sitesini aşırı miktarda trafikle boğarak erişilemez hale getirmek şeklinde Hizmet Reddi (DoS) ve Dağıtılmış Hizmet Reddi (DDoS) Saldırıları olarak karşımıza çıkmaktadır.(Çelik, 2018). İkinci olarak, Kötü Amaçlı Yazılımla sistemlere sızmak, verileri çalmak veya işlemleri aksatmak için virüsler, solucanlar veya Truva atları gibi kötü amaçlı yazılımlar tarafından bilgi dezenformasyonu gerçekleşmektir. Üçüncüsü bir hedefin verilerini şifreleyin ve şifre çözme anahtarları için fidye talep ederek verileri etkili bir şekilde rehin tutmak şeklinde karşımıza çıkan Fidye Yazılımıdır. Dördündücüsü ise casusluk, veri hırsızlığı veya sabotaj amacıyla bir hedefin ağına sızmayı ve erişimi sürdürmeyi içeren ve gizli, uzun vadeli stratejik hamleler ile gerçekleşen gelişmiş kalıcı tehditlerdir (Çelik, 2018). Beşincisi, dezenformasyon ve propagandadır. Kamuoyunu manipüle etmek, anlaşmazlık yaratmak veya rakipleri itibarsızlaştırmak için çeşitli çevrimiçi kanallar aracılığıyla yanlış veya yanıltıcı bilgiler ortaya atarak ve sosyal medya platformları ve haber siteleri sıklıkla propaganda ve dezenformasyon yaymak için kullanılmaktadır (Eldem, 2021). Altıncısı, kimlik avı saldırıları, kişileri veya kuruluşları, oturum açma kimlik bilgileri veya finansal ayrıntılar gibi hassas bilgileri ifşa etmeleri için kandırmak amacıyla yanıltıcı e-postalar, web siteleri veya mesajlar hazırlanarak gerçekleşen saldırıları içermekte, hedef odaklı kimlik avı özellikle yüksek değere sahip bireyleri veya kuruluşları hedef almaktadır. Yedincisi, hassas bilgileri, fikri mülkiyeti veya devlet sırlarını çalmak için bilgisayar ağlarına ve sistemlerine sızarakşeklinde karşımıza çıkan bilgisayar korsanlığı ve casusluktur ve genellikle istihbarat faaliyetleri devlet destekli bilgisayar korsanları veya siber casusluk grupları tarafından yürütülmektedir (Eldem, 2021). Sekizincisi, psikolojik operasyonlardır, hem savaş alanında hem de kamusal alanda rakipleri etkilemek veya morallerini bozmak için psikolojik taktikler kullanılarak, korku, belirsizlik ve şüphenin yayılmasını veya moral artırıcı mesajların desteklenmesini kapsamaktadır. Sonuncusu ise, karşı istihbarattır. Bu yöntem casusluğu veya gizli bilgilere yetkisiz erişimi tespit etmek ve önlemek için faaliyetler yürütmek, içeriden gelen tehditlerin izlenmesini ve güvenlik denetimlerinin yürütülmesi kapsamaktadır(Eldem, 2021).

Geleneksel elektronik harp karıştırma tekniklerine benzer şekilde, işletim sistemi saldırıları internet ağları, web sitelerini veya aşırı internet trafiğine sahip hizmetleri kullanılamaz hale getirmek için sıklıkla kullanılmaktadır. Elektronik harp karıştırma tekniği, kamu yönetimi operasyonları kesintiye uğratır, finansal kayıplara neden olur ve daha çok veri kaybına uğratmak maksadıyla siber saldırılar için bir sis perdesi görevi de görebilmektedir (Özdemir ve Uluyol, 2021). Kamu yönetiminde kullanılan bilgi ve iletişim teknolojilerinde yer alan kritik verilerin değiştirilmesi veya silinmesi, özellikle sağlık, finans ve kamu hizmetleri gibi sektörlerde feci sonuçlara yol açabilir ve bu tür bir manipülasyon, sağlık hizmetlerini, finansal istikrarı ve hatta kamu güvenliğinin tehlikeye girmesine neden olabilir (Çalışkan, 2023). Bir siber saldırının kaynağını belirlemek, genellikle devlet destekli aktörleri veya gelişmiş bilgisayar korsanlığı gruplarını içeren karmaşık bir zorluktur ve bu kamu yöneticilerince gerçekleştirilebilecek misillemeyi veya karşı önlemleri zorlaştırır ve gerilimleri tırmandırabilir. Siber saldırılar, istenmeyen sonuçlara yol açabilir ve hizmet sağlayıcılar veya aynı ağdaki kullanıcılar gibi masum tarafları ve vatandaşları doğrudan etkileyebilir (Sertçelik, 2015).

Teknoloji ilerledikçe, bilgi güvenliğinde elektronik harp alanı gelişmeye devam edecek ve yapay zekâ, kuantum hesaplama ve nesnelerin interneti cihazlarının çoğalması hem saldırganlar hem de savunucular için yeni fırsatlar ve zorluklar getirecektir (Çam vd., 2019). Bilgi güvenliği önlemleri, hassas verileri ve dijital sistemleri yetkisiz erişim, ifşa, kesinti, değişiklik veya imhadan korumak için tasarlanmış bir dizi strateji, teknoloji ve uygulamayı kapsamaktadır (Özdemir ve Uluyol, 2021). Bu önlemler, kuruluşların dijital çağdaki savunma mekanizmalarının kritik bir bileşenidir. Geleneksel fiziksel bölgelerin aksine, siber uzay coğrafi sınırlarla sınırlı değildir. Bir ülkeden kötü niyetli faaliyetlerde bulunan bir varlık, herhangi bir fiziksel sınırı geçmeden başka bir ülkedeki kurbanları hedefleyebildiğinden, bu özellik yasaların uygulanmasını zorlaştırır (Güngör ve Güney, 2017). Bu sınırsız doğa, geleneksel yargı kavramlarına meydan okumaktadır. Siber saldırıları belirli bireylere, gruplara ve hatta uluslara atfetmek oldukça zor olabilir. Saldırganlar genellikle kimliklerini gizlemek için teknikler kullanır ve bu da suçluluk tespitini zorlaştırır. Bu açık atıf eksikliği, faillerin mevcut yasal çerçeveler kapsamında sorumlu tutulması sürecini karmaşıklaştırmaktadır (Önok, 2013).

Teknolojik ilerlemenin hızı genellikle ilgili düzenleyici ve yasal çerçevelerin gelişimini geride bırakmaktadır. Yeni dijital araçlar ve yöntemler ortaya çıktıkça, düzenleyiciler ve yasa koyucular bu değişikliklere ayak uydurmak için mücadele ederek boşluklara ve belirsizliklere yol açabilmektedir. Bir siber olay birden fazla yargı bölgesini etkilediğinde, hangi ülkenin yasalarının geçerli olması gerektiği konusunda anlaşmazlıklar ortaya çıkabilir (Güngör ve Güney, 2017). Bu, özellikle etkilenen ülkeler farklı yasal standartlara sahip olduğunda, elektronik harp tehditlerine verilen yanıtları koordine etmede yasal belirsizliklere ve zorluklara neden olabilir. Siber uzayın toplumları ve ekonomileri birbirine bağladığı bir çağda, siber diplomasi oluşturmak uluslararası iş birliği ve istikrara yönelik önemli bir adımdır.(Yılmaz, 2016).

Elektronik harp, bilgi güvenliği ve kamu yönetiminde, kuruluşları sürekli gelişen siber tehdit ortamından korumak için etkili güvenlik politikaları oluşturma temel görevini üstlenmektedir. (Özdemir ve Uluyol, 2021). Kuruluşlar, politika oluşturmanın nüanslarını anlayarak dijital varlıklarını koruyan ve bir siber güvenlik kültürü geliştiren elektronik harp ile sağlam savunmalar oluşturabilir.

Elektronik harp, geleneksel askeri anlamında, savaşta avantaj elde etmek için elektromanyetik enerjinin kullanılmasını ve düşman iletişimini bozmak, sinyalleri yakalamak ve hatta komuta ve kontrol sistemlerini bozmak için siber saldırılar başlatmak gibi çeşitli taktikleri kapsamaktadır (Sertçelik, 2015). Teknoloji ilerledikçe, bu taktikler bilgi güvenliği alanındaki kötü amaçlı kullanıcılar tarafından uyarlanarak kullanılmaktadır. Elektronik harp ve bilgi güvenliğinin birbiri ile doğrudan ilişkilendirilmesi, coğrafi sınırları aşan, genellikle gizlice yürütülen ve yıkıcı sonuçları olan yeni bir savaş biçiminin ortaya çıkmasına neden olmaktadır (Güngör ve Güney, 2017). Bilgisayar korsanları ve siber suçlular artık sistemleri ihlal etmek, verileri manipüle etmek ve kritik altyapıyı tehlikeye atmak için gelişmiş tekniklerden yararlanarak sanal bir ortamda geleneksel elektronik harbin hedeflerini yansıtmaktadır (Korucu, 2021). Bu geleceğin manzarasını yönlendirmek için, teknolojik ilerlemeler, uluslararası anlaşmalar ve bilgi güvenliğinde elektronik savaşı yönetebilecek vasıflı bir iş gücünün yetiştirilmesini içeren kapsamlı bir yaklaşıma ihtiyaç vardır (Vural ve Sağıroğlu, 2008).

Elektronik harp, dijital alanda yeni bir sınır bularak bilgi güvenliği manzarasını yeniden şekillendirmektedir. Siber tehditlerin ortaya çıkardığı zorluklar karmaşıktır ve sürekli olarak gelişmekte olup, kuruluşların ve hükümetlerin, hassas bilgileri ve kritik altyapıyı korumak için stratejilerini ve teknolojilerini uyarlamasını gerektirir (Sertçelik, 2015). Teknoloji ilerlemeye devam ettikçe, elektronik harp dünyasında saldırı ve savunma arasındaki denge hassas olmaya devam edecek ve bilgi güvenliği alanında sürekli uyanık olma ve yenilik ihtiyacı doğacaktır (Korucu, 2021). Modern çatışmalar, konvansiyonel askeri operasyonların siber ve enformasyon savaşıyla bütünleşmesiyle giderek daha fazla karakterize edilmekte ve bu hibrit savaş yaklaşımını ortaya çıkartarak elektronik harbin önemine vurgu yapmaktadır. Elektronik harp, bir rakibin dijital faaliyetleri hakkında izleme ve istihbarat toplamayı içermektedir. Elektronik harp faaliyetleri ile iletişimleri yakalamayı, bilginin değerli bir meta olduğu dijital çağda verileri toplamayı ve hedefin ağ altyapısının haritasını çıkarmayı kapsamakta olup, bilgi güvenliği bağlamında, bu strateji, bir hedefin savunmasındaki güvenlik açıklarını belirlemek için kullanılabilmekte ve zayıf noktaların kullanılmasına olanak tanıyabilmektedir (Özdemir ve Uluyol, 2021). Elektronik harp stratejileri daha sofistike hale geldikçe, bilgi güvenliği önlemleri de buna ayak uydurması gerekmektedir. Elektronik harp dinamikleri, saldırganların savunmaları aşmak için yeni yollar bulması ve savunucuların bu saldırıları engellemek için yorulmadan çalışmasıyla sürekli bir yenilik ve karşı yenilik döngüsü yaratılmasını sağlamaktadır. Siber uzayın doğasında var olan anonimlik, siber saldırıların atfedilmesini karmaşıklaştırmaktadır. Gelişmiş kalıcı tehditler genellikle kökenlerini gizleyerek sorumlu tarafın doğru bir şekilde belirlenmesini zorlaştırarak, bu ilişkilendirme zorluğu, etkili bir şekilde yanıt verme çabalarını engelleyebilir ve dijital alandaki uluslararası ilişkiler için sonuçlar doğurabilmektedir (Efendioğlu ve Sezgin, 2007).

Bilginin hem bir varlık hem de bir güvenlik açığı olduğu sürekli genişleyen dijital ortamda, bilgi güvenliği önlemlerinin rolü çok önemli hale gelmektedir. Bu önlemler, yalnızca hassas verilerin korunmasında değil, aynı zamanda elektronik harp dinamiklerinin şekillenmesinde de çok önemli bir rol oynamaktadır. İçinde yaşadığımız birbirine bağlı dünya, sınırları aşan dijital teknolojilerle şekilleniyor. Ancak bu teknolojik bağlantılılık, siber güvenlik ve siber çatışmalarla ilgili olanlar da dahil olmak üzere yeni zorlukları da beraberinde getirmektedir. Bu bağlamda elektronik harp diplomasisi kavramı, siber uzay alanında iş birliğini teşvik etmek, normlar oluşturmak ve uluslararası anlaşmalar geliştirmek için hayati bir strateji olarak ortaya çıkmaktadır (Korucu, 2021). Bilgi güvenliği ise ister dijital ister analog olsun, her türlü bilginin yetkisiz erişime, ifşaya, değiştirilmeye veya imhaya karşı korunmasını kapsar, daha geniş bir kavram olarak, dijital sistemlerin ötesinde bir varlık yelpazesini ve fiziksel belgeleri, iletişim kanallarını ve fikri mülkiyeti kapsamaktadır (Efendioğlu ve Sezgin, 2007).

Bilgi güvenliğinin sağlanabilmesi ve elektronik harp saldırılarına karşı düzenli yazılım güncellemeleri, güçlü parola yönetimi ve kullanıcı eğitimi gibi en iyi uygulamaları teşvik etmek, elektronik harbin temel bileşenleri arasında yer almaktadır (Özbilen ve Çağlar, 2020). Elektronik harp, dijital sistemlerin elektronik verilerin korunması için gerekli olan siber tehditlere karşı korunmasını sağlayarak bilgi güvenliğini tamamlanmasına ve fiziksel ve dijital entegrasyon ile bilgi güvenliği, basılı belgeler ve çıkarılabilir medya gibi hassas bilgiler içeren fiziksel varlıkların hırsızlığa ve yetkisiz erişime karşı korunmasını sağlamaktadır (Aydın, 2022).

Elektronik harp izinsiz giriş tespit sistemleri ve izinsiz giriş önleme sistemleri ile ağ trafiğini olağandışı veya kötü amaçlı etkinlikler için izler ve olası tehditleri azaltmak için önleyici eylemde bulunarak, yetkisiz erişimi veya veri ihlallerini önlemekte, kamu yönetimlerinde ve kuruluşlarda, kullanıcı davranışını ve ağ etkinliğini izleyerek anormallikleri ve potansiyel tehditleri belirleyebilir ve ihlalleri önlemek için zamanında yanıt verilmesini sağlamaktadır (Özbilen ve Çağlar, 2020). Düşman ateşine karşı koymak için askeri önlemlere benzer şekilde, elektronik koruma, elektronik saldırılara karşı savunma için güvenlik önlemlerinin uygulanmasını ve güvenlik duvarları, saldırı tespit sistemleri ve şifreleme protokolleri elektronik harp kapsamı dahilinde yer almaktadır (Çalışkan, 2023).

Bilgi güvenliği ve elektronik harbin kesişimi, modern toplumun gidişatını şekillendirmeye devam eden dinamik ve karmaşık bir alan olarak, dijital dünya geliştikçe, onu hem korumak hem de karşı atak yapmak için kullanılan stratejiler ve araçlar da gelişmektedir (Özbilen ve Çağlar, 2020). Bu alanlar arasındaki çok yönlü ilişkiyi anlamak, sürekli gelişen siber tehditler ve savunmalar ortamında gezinmek isteyen kuruluşlar, hükümetler ve bireyler için zorunlu hale gelmekte, bilgi güvenliği ve elektronik harp

arasındaki karmaşık etkileşimi kabul ederek, daha güvenli bir dijital gelecek planlamaları gerçekleştirilebilir(Aydın, 2022). Tıpkı askerlerin savaş alanında kendilerini korumak için zırh giymesi gibi, elektronik koruma da bilgi sistemlerini korumak için savunma önlemlerinin uygulanmasını içermektedir. Güvenlik duvarları, izinsiz giriş tespit sistemleri, şifreleme protokolleri ve erişim kontrolleri bu stratejinin bir parçası olarak, kamu yönetimleri ve sivil kuruluşlar, bilgi altyapısını güvence altına alarak elektronik saldırı riskini azaltabilir ve riski ortadan kaldırabilir (Canbek ve Sağıroğlu, 2006).

Bilginin güvenli bir şekilde korunabilmesi için, kamu yönetimi ve sosyal hayatta kriptografi, düz metni şifrelenmiş verilere dönüştürerek dijital iletişimi güvence altına almak için matematiksel tekniklerin kullanılmasını içermektedir (Marşap vd., 2010). Bu önlem, orijinal bilgilere yalnızca yetkili tarafların erişebilmesini sağlamaktadır. Elektronik harp bağlamında kriptografi, hassas verileri iletim sırasında müdahale ve manipülasyondan korumak için temel bir araç olarak hizmet etmektedir (Özbilen ve Çağlar, 2020). İzinsiz giriş tespit ve önleme sistemleri, bir ağ veya sistem içindeki yetkisiz erişimi veya kötü amaçlı etkinlikleri algılamak ve bunlara yanıt vermek için tasarlanmış teknolojiler olan bu sistemler, bir siber saldırıya işaret edebilecek anormallikleri belirlemek için, ağ trafik kalıplarını ve davranışlarını izlemekte, elektronik harp senaryolarında, izinsiz giriş tespit ve önleme sistemleri, tehditleri hasara yol açmadan önce tespit edip etkisiz hale getirmede çok önemli bir rol oynamaktadır (Aydın, 2022).

Elektronik harp güvenlik operasyon merkezleri, güvenlik olaylarını izlemek, tespit etmek ve bunlara yanıt vermek için merkezi bir unsur görevi görmektedir. Güvenlik operasyon merkezlerindeki yüksek eğitimli profesyoneller, gelen verileri analiz eder, potansiyel tehditleri belirler ve zamanında müdahaleleri düzenler. Siber saldırılara karşı savunma ve karşı koyma çabalarını koordine ettikleri için elektronik harp bağlamında rolleri kritiktir. Hiçbir güvenlik önlemi %100 korumayı garanti edemez, bu nedenle, olay müdahalesi ve kurtarma planları bilgi güvenliğinin temel bileşenleridir (Aydın, 2022). Bu planlar, bir ihlal veya siber saldırı durumunda atılacak adımları özetlemektedir. Kuruluşlar, bir saldırının etkilerini hızla kontrol altına alıp hafifleterek hasarı en aza indirebilir ve normal operasyonlarına daha hızlı bir şekilde devam edebilmelerine olanak tanımaktadırlar (Korucu, 2021).

Bilgi güvenliği önlemleri, siber saldırıların atfedilmesine katkıda bulunur. Güçlü güvenlik önlemleriyle desteklenen gelişmiş adli tıp teknikleri, bir saldırının kaynağının ve yöntemlerinin izlenmesine yardımcı olarak, düşmanın taktik ve amaçlarının daha iyi anlaşılmasını sağlamaktadır (Güngör ve Güney, 2017). Güçlü bilgi güvenliği önlemleri, bir kuruluşun caydırıcılık yeteneklerini destekleyerek, sağlam bir savunma duruşu sergilenmesine, potansiyel saldırganları bir kuruluşun sistemlerini ihlal etmeye çalışmaktan caydırılabilir ve bu önlemler, başarılı atfedilebilecek saldırıların etkisini en aza indirerek bir kuruluşun dayanıklılığını arttırarak bilgi güvenliğinin üst seviyelerde olmasını sağlayabilmektedir (Marşap vd., 2010).

Bilgi güvenliği ve elektronik harp, elektronik ortamlardaki davranışa ilişkin uluslararası anlaşmalar ve normlar oluşturma çabaları esas olup, bu anlaşmalar, kabul edilebilir davranışların ana hatlarını çizebilir, bilgi paylaşımı için mekanizmalar kurabilir ve siber olaylara karşı koordineli müdahaleler kolaylaştırılabilir.(Efendioğlu ve Sezgin, 2007). Kamu yönetimleri ülkelerin ulusal hükümetler ve özel sektör kuruluşları arasındaki iş birliğinin desteklenmesinde, düzenleyici ve yasal zorlukların ele alınmasında çok önemlidir. Özel şirketler genellikle siber güvenlik çabalarına ve düzenleyici geliştirmeye yardımcı olabilecek değerli öngörülere ve kaynaklara sahip olmasından dolayı kamu özel ortaklıklarının kurulması elzem hale gelmektedir.

2. KAMU YÖNETİMİNDE ELEKTRONİK HARP

Elektronik harp diplomasisi için bir çerçeve geliştirmek, ülkelerin düzenleyici ve yasal belirsizlikleri ele almak için yapıcı diyaloglar kurulmasına yardımcı olabilir. Bu yaklaşım karşılıklı anlayışı kolaylaştırabilir, güven inşa edebilir ve iş birliğini teşvik edebilir. Bu normlar, elektronik harp ile diğer ülkelerin ağlarına müdahale etmeme ve kritik altyapının korunması gibi alanları kapsayabilir. Anlaşmalar, belirli siber faaliyetlerden kaçınma veya tehdit istihbaratını paylaşma taahhütlerini içerebilir. Ulusal düzeyde elektronik harp güvenlik kapasitesi oluşturmak, hukukçuları elektronik harp ile ilgili yasalar konusunda eğitmek ve vatandaşlar arasında elektronik harp tehditleri hakkında

farkındalığı artırmak, bilgi açığını kapatmaya ve genel hazırlığı geliştirmeye yardımcı olacaktır. (Ülker vd., 2017).

Elektronik harp kapsamındaki düzenleyici ve yasal belirsizlikler, hükümetler, işletmeler ve benzer şekilde bireyler için önemli zorluklar oluşturmaktadır. Teknoloji gelişmeye devam ettikçe, kapsamlı ve uyarlanabilir yasal çerçevelere duyulan ihtiyaç giderek daha belirgin hale gelmektedir. Bu belirsizliklerin üstesinden gelmek, iş birliğine dayalı, uluslararası ve ileriye dönük bir yaklaşım gerektirir. Güvenlik, mahremiyet ve yenilikçiliğin zorunluluklarını dengeleyen bir yaklaşımın paydaşların, dijital çağın karmaşıklıklarını doğrudan ele alarak herkes için daha güvenli, düzenlenmiş ve dayanıklı bir elektronik ortam içerisinde çalışabilmesine imkân vereceği düşünülmektedir (Dayıoğlu, 2010).

Bilgi güvenliği yeteneklerinin geliştirilmesi için elektronik harp diplomasinin mihenk taşı olarak gelişmekte olan ülkeler, genellikle siber savunmalarını oluşturmak, elektronik harp uzmanları eğitmek ve etkili olay müdahale mekanizmaları kurmak için yardıma ihtiyaç duymaktadır (Üstün, 2023). Kapasite geliştirme girişimlerinin, bilgi güvenliği bağlamında elektronik harbin istikrarı ve esnekliği teşvik edebileceği değerlendirilmektedir. Elektronik harp diplomasisi yoluyla ülkeler, siber güvenlik uygulamaları için uluslararası kabul görmüş standartlar geliştirmek üzere birlikte çalışabilir ve bu standartların, sınırlar ötesindeki politikalara, düzenlemelere ve uygulamalara rehberlik edebileceği öngörülmektedir (Baran ve Şener, 2020).

Bilgi savaşının giderek yaygınlaştığı bir ortamda, kişisel verilerin korunması hem bir kalkan hem de bir silah görevi gibi görülmektedir. Kötü niyetli aktörler, bilgi harbi kampanyalarının etkilerini artırmak için kişisel verilerin korunmasındaki güvenlik açıklarından yararlanmaktadırlar (Karaoğlan Yılmaz vd., 2014). Tersine, sağlam kişisel veri koruma mekanizmaları, yani elektronik harp uygulamaları bu tür kampanyaların etkisini azaltmak için bireyler, kuruluşlar ve hükümetler için çok önemlidir. Dijital okuryazarlık kültürünü teşvik ederek, etkili mahremiyet düzenlemelerini yürürlüğe koyarak ve uluslararası iş birliğini teşvik ederek, tehlikeye atılmış kişisel veriler ve bilgi savaşından oluşan ikili tehdide karşı güçlendirilmiş bir savunma oluşturabilmesi mümkün hale gelmektedir (Ülker vd., 2017). Dijital ara bağlantılar ile tanımlanan bir çağda, kişisel verilerin korunması ile bilgi savaşı dayanıklılığı arasındaki sinerji, güvenli ve bilinçli bir gelecek için çok önemli hale gelmektedir.

Devlet operasyonlarını yönetme sanatı ve bilimi olan kamu yönetimi, modern yönetişimin önemli bir disiplini olarak nitelendirilmektedir. Dünya, ileri teknolojilere büyük ölçüde bağımlı bir döneme girerken, kamu yönetimini önemli ölçüde etkileyen alanlardan biri de elektronik harptir. Elektromanyetik spektrumun düşman kuvvetlerini bozmak veya onlara karşı savunma yapmak için kullanılması olan elektronik harp, geleneksel idari uygulamaları hızla yeniden şekillendirmektedir. Elektronik harp, 20. yüzyılda modern savunma stratejilerinin çok önemli bir yönü olarak ortaya çıkmıştır. Düşman radarlarını bozmak veya aldatmak için elektronik karşı önlemler, sinyal yakalama yoluyla istihbarat toplamak için elektronik destek önlemleri ve düşman iletişim sistemlerini hedef alıp devre dışı bırakmak için elektronik saldırı dahil olmak üzere bir dizi faaliyeti kapsamaktadır (Aydın, 2022). Teknoloji geliştikçe, elektronik harbin yetenekleri ve karmaşıklığı da gelişerek ve kamu yönetiminin bu zorluklara nasıl yanıt verdiği konusunda bir paradigma değişikliğini zorunlu kılmaktadır.

Elektronik harbin yayılmasının kamu altyapısı üzerinde derin bir etkisi olup, ulaşım, iletişim, enerji ve sağlık gibi kritik sektörler giderek daha fazla dijitalleşmekte ve birbirine bağlı hale gelmektedir (Üstün, 2023). Bu karşılıklı bağlantı, verimliliği ve hizmet sunumunu geliştirirken, aynı zamanda bu sistemleri potansiyel elektronik tehditlere maruz bırakmaktadır. Kamu yöneticileri artık bu altyapıları siber saldırılara ve elektronik izinsiz girişlere karşı koruma gibi göz korkutucu bir görevle karşı karşıya kalabilmekte ve bu da gelişmiş elektronik harp güvenlik önlemlerinin idari çevrelere entegrasyonunun gerekliliğini ortaya çıkarmaktadır (Ülker vd., 2017).

Kamu yönetimi ve elektronik harbin kesişimi, veri gizliliği ve ulusal güvenlik hakkında ilgili soruları gündeme getirerek, hükümetler, vatandaşların ihtiyaçlarını daha iyi anlamak ve kamu hizmetlerini geliştirmek için rutin olarak büyük miktarda veri toplamakta ve depolamaktadır (Güldoğan ve Işıklı, 2022). Bununla birlikte, elektronik harbin ortaya çıkmasıyla birlikte, bu hassas bilgileri

potansiyel düşmanlardan korumak çok önemli hale gelmektedir. Kamu yöneticileri, ulusal güvenlik çıkarlarını yabancı elektronik casusluk faaliyetlerinden korurken, veriye dayalı yönetişim ile vatandaşların mahremiyet haklarının güvence altına alınması arasında hassas bir denge kurması gerekmektedir (Güldoğan ve Işıklı, 2022).

Elektronik harp teknolojilerinin hızlı evrimi, kamu yönetiminde karar verme sürecinde yeni zorluklar ortaya çıkararak, yöneticilerin zamanında ve bilinçli kararlar alarak elektronik tehditlerin dinamik ve öngörülemez doğasına uyum sağlaması zorunlu hale gelmektedir. Geleneksel hiyerarşik yaklaşımlar, potansiyel siber veya elektronik saldırılara hızlı bir şekilde yanıt vermek için çevik ve iş birliğine dayalı karar alma modellerinin benimsenmesini gerektirerek, ortaya çıkan bu zorlukları ele almada yetersiz kalınmaması için elektronik harp stratejileri kamu yönetiminde yer alması gerekmektedir. Elektronik harbin kamu yönetimine entegrasyonu, gelişmiş teknolojiler konusunda kapsamlı bir anlayışa sahip yetenekli bir iş gücü gerektirmektedir. Elektronik tehditlerle etkili bir şekilde mücadele etmek için kamu görevlilerini gerekli uzmanlık alaları ile donatmak için eğitim ve beceriyle yükseltme zorunlu hale gelmekte, hükümetler, elektronik harbin karmaşıklıklarını ele alabilecek bir iş gücü geliştirmek için sürekli öğrenme programlarına ve teknoloji uzmanlarıyla iş birliğine yatırım yapmalıdır.

Elektronik harp ulusal sınırları aşarak ve elektronik tehditlere etkin bir şekilde karşı koymada uluslararası iş birliğini hayati hale getirmektedir. Kamu yöneticileri, elektronik harp teknolojilerinin sorumlu kullanımını yöneten uluslararası normların ve anlaşmaların formüle edilmesinde kritik bir rol oynamaktadır. Hükümetler ve uluslararası kuruluşlar arasındaki iş birliği, elektronik harbin kötüye kullanılmasını önlemek ve daha güvenli bir küresel dijital ortam sağlamak için yasalar oluşturulması gerekmektedir. Kamu yönetiminde elektronik harp hem zorluklar hem de fırsatlar sunmaktadır. Elektronik harp yetenekleri gelişmeye devam ettikçe, kamu yöneticileri stratejilerini ve uygulamalarını ulusal çıkarları, kritik altyapıları ve vatandaşların mahremiyetini korumak için proaktif olarak uyarlamalıdır (İleri, 2016). Devlet kurumları, özel sektör paydaşları ve uluslararası ortaklar arasındaki iş birliği, elektronik tehditleri azaltmak, etkili politikalar ve stratejiler geliştirmek için çok önemlidir. Teknolojik gelişmeleri benimsemek ve vasıflı bir iş gücünü teşvik etmek, bir bütün olarak toplumun yararına güvenlik, mahremiyet ve iyi yönetişim sağlarken, kamu yönetiminin elektronik harp çağında gelişmesini sağlayacaktır (Edegbeme-Belaz ve Kerti, 2022). Dijital devrimle birlikte, elektronik harp teknikleri iletişim ağları, ulaşım sistemleri ve devlet hizmetleri gibi alanları etkileyerek sivil alana taşınmıştır. Devlet operasyonlarını yönetmekten ve vatandaşlara temel hizmetleri sunmaktan sorumlu olan kamu yönetimi, elektronik harbin kendi etki alanlarına entegrasyonunun önemini kavraması gerekmektedir (İleri, 2016).

Dijital altyapıya artan güven, kamu yönetimini bilgisayar korsanlığı girişimlerinden veri ihlallerine kadar değişen siber tehditlere karşı duyarlı hale getiriyor (Güldoğan ve Işıklı, 2022). Kamu yöneticileri, hassas bilgileri ve kritik sistemleri elektronik harp saldırılarından korumak için yine elektronik harp güvenlik önlemleri uygulamalıdır. Elektronik harp savunma mekanizmalarını kamu yönetimi sistemlerine entegre etmek, teknoloji, eğitim ve altyapıya önemli yatırımlar gerektirmektedir. Bütçe kısıtlamaları ile güvenli bir dijital ortam ihtiyacı arasında bir denge bulmak önemli bir zorluk teşkil etmekte ve kamu yönetimi, her biri elektronik harp sistemleri ve güvenlik açıkları olan birden fazla kurum ve departmanı içermesi, elektronik harp tehditlerine karşı koyma çabalarını koordine etmek, düzenli iletişim ve iş birliğini zorunlu kılmaktadır (Edegbeme-Belaz ve Kerti, 2022).

Elektronik harp teknolojilerinden yararlanarak, kamu yöneticileri acil durumlara ve felaketlere hızlı bir şekilde müdahale etme yeteneklerini geliştirebilirler. Gerçek zamanlı veri alışverişi ve iletişim, kriz durumlarında hayat kurtarabilir ve hasarı en aza indirebilir. Kamu yöneticileri, potansiyel saldırılara karşı kritik altyapıyı güçlendirmek için elektronik harp stratejilerinden yararlanabilir ve sağlam siber güvenlik önlemlerinin uygulanması, iletişim ağlarının, elektrik şebekelerinin ve ulaşım sistemlerinin dayanıklılığını artırabilir (İleri, 2016). Kamu yönetimleri, çok sayıda hassas vatandaş verisi ile ilgilenir. Elektronik harp çözümleri, veri güvenliğini artırabilir ve vatandaşların mahremiyetini koruyarak devlet hizmetlerine güven ve itimat sağlanmasına olanak tanımaktadır.

Elektronik harp, dijital ortamda giderek daha yaygın hale geldikçe, kamu yöneticileri bunun önemini ve kendi alanları üzerindeki etkilerini kabul etmelidir. Teşkilatlar arasında uyanık, uyumlu ve işbirlikçi kalarak kamu yönetimi, hizmet ettikleri vatandaşlara karşı temel sorumluluklarını yerine getirirken elektronik harp ortamında yol katedebilir (Uysal, 2020). Devlet kurumlarını hedef alan siber saldırılardaki artış, hassas verilerin güvenliğini ve gizliliğini sağlamak için acil ve kapsamlı çözümler gerektirmektedir. Kamu yöneticilerinin elektronik harp ve bilgi güvenliği önlemlerini güçlendirmek için uygulayabilecekleri, vatandaşlar ve devlet operasyonları için daha güvenli ve daha esnek bir ortam geliştirebilecekleri etkili stratejilere yer verilmesi gerekmektedir (Uysal, 2020). Devlet çalışanları için en iyi elektronik harp uygulamaları hakkında sürekli eğitim oturumları düzenlemek ve kimlik avı girişimlerini belirlemek, güvenlik ihlallerine yol açan insan hatası riskini önemli ölçüde azaltabilir.

Kamu yönetimlerinde elektronik harp saldırılarına karşın yine bir takım elektronik harp önlemleri ile bilgi güvenliğinin sağlanması mümkün hale gelmektedir. Bunlar (Szczepaniuk vd., 2020);

Risk Değerlendirmesi, kamu kuruluşlarının dijital altyapısındaki güvenlik açıklarını ve potansiyel saldırı vektörlerini belirlemek için düzenli risk değerlendirmeleri yapmak,

Politikalar ve Protokoller, çalışan davranışını, veri işlemeyi ve sistem erişimini yönetmek için katı siber güvenlik politikaları ve protokolleri geliştirmek ve uygulamak,

Eğitim, çalışanları en iyi elektronik harp uygulamaları hakkında eğitmek ve kimlik avı, fidye yazılımı ve sosyal mühendislik gibi ve son olarak siber tehditler hakkında farkındalık yaratmak,

Sürekli izleme, ağ etkinliklerini sürekli olarak izlemek ve şüpheli davranışları gerçek zamanlı olarak belirlemek için gelişmiş tehdit algılama sistemlerini devreye almak,

Çok faktörlü kimlik doğrulama uygulanması, kullanıcıların parolalar, biyometri veya donanım belirteçleri gibi birden çok kimlik biçimi sağlamasını zorunlu kılarak, güvenliği ihlal edilmiş bir parola durumunda bile yetkisiz erişim riskini önemli ölçüde azaltacaktır,

Güçlü şifreleme yöntemlerinin uygulanması, verilerin ele geçirilse bile yetkisiz kişiler tarafından okunamaz ve kullanılamaz durumda kalmasını sağlanması gibi önlemler ile gerçekleştirilebilmektedir.

Kamu yönetiminde bir elektronik harp farkındalığı kültürünün teşvik edilmesi çok önemlidir. Çalışanları şüpheli faaliyetleri bildirmeye teşvik etmek, iyi güvenlik uygulamalarını ödüllendirmek ve iletişim için açık kanalları sürdürmek, daha dayanıklı bir güvenlik duruşuna katkıda bulunacaktır. Kamu yönetiminin dijitalleşmesi, hizmet sunumunda, idari verimlilikte ve vatandaş katılımında önemli gelişmeler sağlamakta olup, e-devlet platformları, açık veri girişimleri ve dijital iletişim kanalları gibi önemli teknolojik gelişmeler, devlet kurumları ve vatandaşlar arasındaki etkileşimlerdeki yenilikler, kamu yönetimini potansiyel tehditlere karşı korunmak için sağlam önlemler gerektiren çok çeşitli güvenlik risklerine de maruz bırakmaktadır (Szczepaniuk vd., 2020). Vatandaş verilerinin toplanması ve saklanması, mahremiyet ve veri koruma ile ilgili endişeleri artırmaktadır. Kamu yönetimi, verimli hizmetler sunmak ile vatandaşların mahremiyet haklarını korumak arasında hassas bir denge kurmak zorundadır. Güvenlik zorluklarını etkili bir şekilde ele almak için kamu yönetimi, elektronik harp ve bilgi güvenliğinin çeşitli yönlerini içeren kapsamlı bir güvenlik çerçevesi oluşturmalıdır.

Kamu idareleri, temel hizmetleri ve vatandaşların refahını sağlayarak yönetişimin bel kemiği olarak hizmet ederken, günümüzün teknoloji odaklı dünyasında, kamu idareleri siber tehditlerden fiziksel güvenlik açıklarına kadar bir dizi güvenlik sorunuyla karşı karşıya kalmaktadır.(Önen ve Kurnaz). Kamu yönetimi, potansiyel tehditleri gerçek zamanlı olarak tespit etmek için sürekli izleme sistemleri kurmalıdır. Bu, güvenlik olaylarına anında yanıt vermelidir.(Çakır ve Uzun, 2021).

Kamu yönetiminde elektronik harp risk analizi, bilgi sistemlerinin güvenliğini ve bütünlüğünü tehlikeye atabilecek potansiyel tehditleri belirlemek, değerlendirmek ve öncelik sırasına koymak için aktif bir yaklaşım olarak hizmet eder (Önen ve Kurnaz, 2017). Siber olayların olasılığını ve etkisini anlayan kamu yöneticileri, kaynakları etkili bir şekilde tahsis edebilir, özel güvenlik önlemleri geliştirebilir ve kritik varlıkları ve vatandaş verilerini koruyabilir.

Kamu yönetiminde dijital dönüşüm, verimliliği, şeffaflığı ve iyileştirilmiş vatandaş deneyimlerini destekleyen yenilikçi araçlar ve teknolojilerle kamu idarelerini güçlendirmektedir. Kamu yönetiminde dijital dönüşümün temel unsurları şunları içerir (Karasoy ve Babaoğlu, 2021):

E-Devlet hizmetleri, dijital platformlar, vatandaşların çevrimiçi olarak bilgilere erişmesine ve işlemleri tamamlamasına izin vererek, devlet hizmetlerinin sorunsuz bir şekilde sunulmasını kolaylaştırmakta,

Açık veri girişimleri, kamu idareleri, şeffaflığı ve hesap verebilirliği teşvik ederek, devlet verilerini vatandaşlar, işletmeler ve araştırmacılar için erişilebilir kılmak için açık veri girişimlerinden yararlanmakta,

Yapay zekâ ve otomasyon, idari süreçleri kolaylaştırarak evrak işlerini azaltır ve karar verme yeteneklerini geliştirmekte,

Mobil uygulamalar, vatandaşların kamu idareleri ile rahat bir şekilde etkileşim kurmasını sağlayarak daha fazla vatandaş katılımına yol açmakta, ancak bu temel unsurların bilgi güvenliği ve fiziksel güvenlik endişelerine mahal vermeden gerçekleştirilmesi gerekmekte olup, bu güvenlik endişelerinin elektronik harp stratejileri ve uygulamaları ile sağlıklı bir kamu yönetişimi gerçekleştirmek mümkün hale gelmektedir.

Kamu yönetiminde dijital sistemlere ve veri toplamaya artan güven, kişisel verilerin korunmasına ilişkin endişeleri artırmaktadır. Vatandaşlar, tıbbi kayıtlar, finansal veriler ve diğer kişisel olarak tanımlanabilir bilgiler dahil olmak üzere hassas bilgileri kamu idarelerine emanet etmekte, bu tür verilere yanlış kullanım veya yetkisiz erişim, kimlik hırsızlığı, gizlilik ihlalleri ve kamu güveninin kaybı gibi ciddi sonuçlara yol açmasına neden olacaktır (Çahmutoğlu, 2020). Kamu idareleri, kişisel verileri korumak için veri koruma düzenlemelerine uymalıdır. Avrupa Birliği'ndeki Genel Veri Koruma Yönetmeliği gibi düzenlemeler ve dünya çapındaki benzer veri gizliliği yasaları, veri işleme, onay ve ihlal bildirimi konusunda katı gereksinimler getirir. Bu düzenlemelere uymak, yalnızca yasal sonuçlardan kaçınmak için değil, aynı zamanda vatandaşların haklarını ve mahremiyetini koruma taahhüdünü göstermek için de gereklidir. Kişisel verilerin korunması, bireysel mahremiyetin korunması ve temel hakların korunması için çok önemlidir. Hükümetler, kuruluşlar ve bireyler, hizmet sunumundan hedefli reklamcılığa kadar çeşitli amaçlar için çok büyük miktarlarda kişisel veri toplamakta ve işlemektedir (Aslay, 2017). Kişisel verilerin korunması sadece yasal bir zorunluluk değil, aynı zamanda bireylerin dijital ekosisteme güvenini sağlamak için ahlaki bir zorunluluktur.

Elektronik harp, genellikle ulusal güvenlik ve savunma stratejilerinde kritik bir rol oynamaktadır. Hükümetlerin vatandaşlarını, kritik altyapılarını ve gizli bilgileri yabancı düşmanlardan ve siber tehditlerden koruması gerekir. Bu arayışta, ulusal güvenliğin zorunlulukları ile bireysel mahremiyetin korunması arasında gerilim olabilmekte, bu çıkarlar arasında doğru dengeyi kurmak, politika yapıcılar ve kamu yöneticilerini direkt olarak ilgilendirmektedir (Orak, 2021).

3. ELEKTRONIK HARP ve ETIK ANLAYIŞI

Kamu yönetimlerinde bilgi güvenliği ve elektronik harp, özellikle siber operasyonlarda kullanılması etik kaygıları gündeme getirmektedir. Siber saldırıların ve veri dinlemenin gelişigüzel veya yetkisiz kullanımı ikincil hasara ve mahremiyet ihlallerine yol açabilir (Kayacı, 2019). Hükümetler ve kuruluşlar, bireysel haklara ve mahremiyete saygı gösterilmesini sağlamak için elektronik harp operasyonlarında yer alırken etik çerçevelere ve yönergelere uymak zorundadır. Vatandaşlar arasında elektronik harbin riskleri ve kişisel verilerin korunmasının önemi hakkında farkındalık yaratmak çok önemlidir. Bireyleri elektronik harp uygulamaları, veri gizliliği hakları ve karşılaştıkları potansiyel tehditler hakkında eğitmek, onların bilgilerini korumak için aktif önlemler almalarını sağlayabilmektedir (Demirtaş ve Karaca, 2018).

Elektronik harp, kamu idareleri tarafından kullanılanlar da dahil olmak üzere, modern harp ve savunma stratejilerinde giderek daha önemli bir rol oynamaktadır. Teknoloji geliştikçe, saldırı, savunma ve keşif amaçları için elektronik ve elektromanyetik araçların kullanımı daha karmaşık hale gelmekte, ancak, elektronik harbin potansiyel yararlarının yanı sıra, kamu idarelerinde uygulanmasına ilişkin etik kaygılar ortaya çıkmaktadır (Şenol, 2017).

Gizlilik ve veri koruma, elektronik harp özellikle siber operasyonlar bağlamında, kişisel verilerin mahremiyeti ve korunmasına ilişkin endişelere yol açabilir. Vatandaşların verileri, siber saldırılarda yanlışlıkla tali hasara dönüşerek mahremiyet ihlallerine ve veri koruma yasalarının ihlal edilmesine yol açabilir. İkincil hasar, herhangi bir askeri operasyon gibi elektronik harpte istenmeyen sonuçlara ve tali hasara neden olabilir. Yöneticiler, elektronik harp eylemlerinin sivil nüfus ve muharip olmayan varlıklar üzerindeki potansiyel etkisini dikkatle tartmalıdır. Siber silahların yayılmasında kamu idareleri, siber silahların geliştirilmesinde ve kullanılmasında etik ikilemlerle karşı karşıya kalabilmekte ve bu tür silahların saldırı operasyonlarında kullanılması potansiyel olarak daha geniş bir silahlanma yarışına ve siber çatışmaların tırmanmasına yol açabilir (Tunca, 2019). İlişkilendirme ve hesap verebilirlik, elektronik harp saldırılarının gerçek kaynağını belirlemek ve sorumluluğu doğru bir şekilde ilişkilendirmek zor olabilir. Kamu idareleri, masum taraflara karşı misilleme niteliğindeki eylemlerden kaçınmak için dikkatli davranmak zorundadır.

Elektronik harp için etik çerçeveler, adil savaş teorisi, savaşa gitme hakkı ve savaş sırasındaki davranış dahil olmak üzere adil savaş teorisinin ilkeleri, elektronik savaşın etik olarak gerekçelendirile bilirliğini değerlendirmek için bir çerçeve sunmaktadır (Kayacı, 2019). Orantılılık, ayrımcılık ve gereklilik, adil savaş teorisinin etik karar vermeye rehberlik edebilecek temel bileşenleridir. Orantılılık ilkesi ile kamu yöneticileri, beklenen faydaların potansiyel zarar ve tali zarardan daha ağır basmamasını sağlamak için elektronik harp operasyonlarının potansiyel faydalarını ve risklerini dikkatli bir şekilde değerlendirmelidir (Nurata, 2021).

Muharip olmayan dokunulmazlık karar vericiler, elektronik harp operasyonlarında sivilleri veya sivil altyapıyı hedef almaktan kaçınarak, muharip ve muharip olmayanlar arasında ayrım yapma ilkesine bağlı kalmalıdır (Tunca, 2019). Kamu idareleri tarafından yürütülen elektronik harpte şeffaflık esastır. Yöneticiler, elektronik harp faaliyetlerinin amaçları, yöntemleri ve sonuçları konusunda açık olmalıdır. Ek olarak, etik ilkelere bağlılığı sağlamak ve elektronik harp yeteneklerinin kötüye kullanılmasını önlemek için hesap verebilirlik mekanizmaları yürürlükte olmalıdır. Kamu yöneticileri, elektronik harp konusunda etik olarak bilinçli kararlar verecek şekilde donatılmalıdır. Bu tür elektronik harp operasyonlarının yasal ve ahlaki sonuçlarının kapsamlı bir şekilde anlaşılmasını gerektirir. Etik eğitimi ve uzmanlarla istişare, yöneticilere karmaşık etik ikilemlerde yön bulmada yardımcı olabilir. Elektronik harpteki etik zorlukları ele almak için kamu idareleri, elektronik harp normları ve çerçeveleri oluşturmak için uluslararası iş birliğine girmelidir. Diğer hükümetler ve uluslararası kuruluşlarla iş birliği yapmak, ortak etik standartların ve en iyi uygulamaların geliştirilmesine yol açacaktır.

Kamu idarelerinde elektronik harp ve etik arasındaki ilişki karmaşık ve çok yönlüdür. Teknoloji ilerlemeye devam ettikçe, politika yapıcılar ve yöneticiler ulusal güvenlik kurulları arasında bir denge kurma zorluğuyla karşı karşıya kalması söz konusu olabileceği ön görülmektedir (Güntay, 2018). Siber casusluk, siber araçlarla istihbarat toplanmasını içeren elektronik harbin önemli bir yönüdür. Kamu idareleri potansiyel tehditler, yabancı hükümetler veya terör örgütleri hakkında bilgi toplamak için siber casusluk faaliyetleri yürütebilir (Önen ve Kurnaz, 2017). Bununla birlikte, siber casusluk, özellikle diğer ülkelerin veya özel kuruluşların bilgisayar sistemlerini ele geçirmeyi içerdiğinde etik kaygılara yol açabilir. Yönetimler, potansiyel egemenlik ve bireysel mahremiyet hakları ihlalleri de dahil olmak üzere siber casusluğun etik sonuçlarını dikkatle değerlendirmesi gerekmektedir (Kayacı, 2019).

Kamu idarelerinin, kritik altyapıyı, kamu hizmetlerini ve vatandaşların verilerini korumak için elektronik harbe öncelik verme konusunda etik bir yükümlülüğü bulunmaktadır. Elektronik harbin ihmal edilmesi, veri ihlalleri, ekonomik krizler ve ulusal güvenliğin tehlikeye atılması gibi ciddi sonuçlara yol açabilir. Güçlü elektronik harp güvenlik önlemlerine yatırım yapmak, yalnızca pratik bir gereklilik değil, aynı zamanda kamu çıkarlarını korumak için etik bir sorumluluktur. Kamu idarelerinde etik liderlik, elektronik harpte sorumlu karar almayı sağlamak için çok önemlidir. Yöneticiler, bilgi güvenliği ve elektronik harp operasyonlarında etiğin önemini vurgulayarak önemini önceden belirlemelidir. Siber faaliyetler için net sorumluluk hatları oluşturmak, elektronik harp yeteneklerinin kötüye kullanılmasını önleyebilir ve etik ilkelere bağlılığı sağlayabilir (Güntay, 2018). Elektronik harp ve bunun etik sonuçları hakkındaki tartışmalarda halkla ve paydaşlarla etkileşim kurmak çok önemli olduğu düşünülmektedir. Kamu idareleri elektronik harp uygulamaları konusunda şeffaf olmalı ve vatandaşları elektronik harp ile

ilgili etik hususlar hakkında bilgilendirmelidir. Geri bildirim istemek ve halkın endişelerini ele almak, sorumlu politikaların şekillendirilmesine ve halkın güveninin oluşturulmasına yardımcı olacaktır.

4. ELEKTRONİK HARP ve HUKUK İLİŞKİSİ

Avrupa Birliği, giderek dijitalleşen dünyamızda siber güvenliğin kritik öneminin farkına varmış ve siber saldırıların oluşturduğu artan tehditleri ele almak için bölgenin dijital altyapısını, hassas verilerini ve vatandaşlarının mahremiyetini korumayı amaçlayan sağlam bir yasal çerçeve uygulamaya koymaktadır (Önok, 2013). Siber güvenlik tehditlerinin ölçeği ve karmaşıklığı son yıllarda artmakta olup, kritik altyapılara yönelik saldırılar, veri ihlalleri ve devlet destekli aktörlerin dahil olduğu olaylar, kapsamlı siber güvenlik mevzuatına olan ihtiyacın ortaya çıkmasına neden olmaktadır. Kritik altyapı, enerji, ulaşım ve sağlık hizmeti sağlayıcıları gibi kritik altyapıyı işleten kuruluşların yükümlülüklerini, bu kuruluşların yeterli siber güvenlik önlemlerini uygulaması ve ciddi olayları ulusal yetkililerin gerekli önlemleri alması için çevrimiçi platformlar, bulut bilişim hizmetleri ve arama motorları olarak kategorize edilmektedir (Önok).

Siber Güvenlik Yasası, AB'nin siber güvenlik kurumu Avrupa Birliği Siber Güvenlik Ajansı rolünü güçlendirerek kalıcı bir yetki verilerek ve AB çapında siber güvenlik sertifikasyon programlarının geliştirilmesi de dahil olmak üzere daha büyük sorumluluklar bu ajans tarafından gerçekleştirilmektedir (Karaca ve Gül, 2021). Aralık 2020'de Avrupa Komisyonu, AB'nin siber güvenliğe hazırlıklılığını güçlendirmeye yönelik kapsamlı ve ileriye dönük bir yaklaşım olan AB Siber Güvenlik Stratejisini tanıtmıştır.

Stratejide birkaç temel amaç ve girişim özetleniyor: Dayanıklılık, AB, kritik altyapının korunmasına, tehdit istihbaratı paylaşımının arttırılmasına ve güvenlik duruşunun iyileştirilmesine odaklanarak genel siber güvenlik direncini artırmayı amaçlamaktadır. Teknolojik özerklik, AB yabancı teknoloji sağlayıcılara bağımlılığı azaltmak için bulut bilişim, 5G ve yapay zekâ gibi kritik alanlarda kendi yeteneklerini geliştirmeyi amaçlamaktadır (Aliusta ve Benzer, 2018). Dijital Tek Pazar Stratejisi ile tüm AB üye ülkelerinde yüksek düzeyde siber güvenlik sağlayarak dijital tek pazarın oluşturulmasını teşvik ederek, uluslararası iş birliği siber tehditlerin küresel doğasının bilincinde olan AB, önemli müttefikler ve uluslararası kuruluşlarla siber güvenlik diyalogları da dahil olmak üzere uluslararası ortaklıklarını güçlendirmeyi planlamaktadır (Aliusta ve Benzer, 2018). Strateji, mevcut siber güvenlik mevzuatını güçlendirmeyi ve genişletmeyi, sertifikasyon programlarını daha da geliştirmeyi ve yüksek riskli teknolojiler için düzenleyici önlemleri dikkate almayı ve eğitim ve sertifikasyon programları ile elektronik harp dünyasında farkındalığı arttırmaktadır.

AB'nin siber güvenlik yasalarının çeşitli sonuçları ve zorlukları vardır. Yasaların, kritik altyapıyı, hassas verileri ve gizliliği koruyacak gelişmiş siber güvenlik standartlarına ve uygulamalarına yol açması bekleniyor. İş uyumluluğu, AB'de faaliyet gösteren kuruluşlar, siber güvenlik önlemleri ve sertifikasyonla ilgili olarak potansiyel artan maliyetlere yol açacak şekilde bu yasalara uyumu sağlamalı ve AB'nin siber güvenliğe yaklaşımının küresel etkileri olması muhtemeldir ve dünya çapındaki işletmelerin siber güvenlik endişelerini nasıl ele aldığını etkileyeceğini değerlendirmektedir (Renda, 2022). Düzenleme ile yenilik arasında doğru dengeyi kurmak zorlu bir iş olarak görünebilir ancak aşırı külfetli düzenlemeler teknolojik ilerlemeyi engelleyebilir. AB üye ülkeleri arasında etkili sınır ötesi iş birliği ve bilgi paylaşımı başarı için çok önemli hale gelmektedir. Siber güvenlik tehditleri bireyleri, kuruluşları ve ulusları benzer şekilde etkileyen küresel bir soruna dönüşmüş olup, bu tehditlerle etkili bir şekilde mücadele etmek için çeşitli yargı bölgelerinde siber güvenlik tehditlerine karşı yasal bir temel sağlayacak yasal çerçeveler oluşturulmuştur (Aliusta ve Benzer, 2018).

4.1. Uluslararası Anlaşmalar ve Sözleşmeler

Budapeşte Sözleşmesi: Budapeşte Sözleşmesi olarak da bilinen Avrupa Konseyi Siber Suçlar Sözleşmesi, siber suçları ele alan öncü bir uluslararası anlaşmadır. Ülkelerin hukuk sistemlerini uyumlu hale getirmeleri, soruşturma tekniklerini geliştirmeleri ve siber suçluların kovuşturulmasında uluslararası iş birliğini kolaylaştırmaları için bir çerçeve sağlamaktadır. Birleşmiş Milletler (BM) Anlaşmaları, siber güvenliğin ve siber suçların önlenmesinin önemini kabul etmiş ve Hükümet Uzmanları Grubu raporları gibi çeşitli kararlar ve anlaşmalar, siber uzayda sorumlu devlet davranışına ilişkin ilkeleri ve yönergeleri özetlemektedir (Renda, 2022). Suçluların iadesi anlaşmaları, ülkelerin bir

yargı bölgesinde siber suçlar işleyip diğerine kaçan kişilerin iadesini talep etmelerine olanak tanımakta, bu anlaşmalar siber suçluların sınır ötesinde kovuşturulmasını kolaylaştırmaktadır. Karşılıklı Adli Yardım Anlaşmaları, ülkelerin siber suçları soruşturma ve kovuşturmada birbirlerinden hukuki yardım talep etmelerine olanak tanıyarak, verilerin korunması ve toplanmasından kanıtların paylaşılmasına kadar çok çeşitli konuları kapsamaktadır (Aliusta ve Benzer, 2018).

Siber güvenlik tehditlerine karşı yasal dayanak, siber suçlarla mücadele ve dijital altyapıyı ve verileri korumaya yönelik küresel çabanın önemli bir bileşenidir. Uluslararası anlaşmalar ve sözleşmeler, ulusal yasa ve düzenlemeler, uluslararası hukuki iş birliği mekanizmaları bu çerçeveye katkıda bulunmaktadır. Zorluklar devam etse de siber güvenlik tehditlerine karşı yasal temel, ortaya çıkan tehditleri ele almak ve siber suçlarla mücadelede uluslararası iş birliğini kolaylaştırmak için sürekli olarak gelişmektedir.

AB-ABD Gizlilik Kalkanı sözleşmesi, standart sözleşme maddeleri ve bağlayıcı kurumsal kurallar, yasal veri aktarımlarını sağlamaya yönelik mekanizmalardır. AB, veri koruma standartlarını iyileştirmek için üçüncü ülkelerle anlaşmalar müzakere etmeye devam etmektedir. Bazı AB üye devletleri, verilerin kendi sınırları içinde saklanmasını gerektiren veri yerelleştirme tedbirlerini dikkate almaktadır. Bu, sınır ötesi veri akışını engelleyebilir ve işletmelerin maliyetlerini artırabilir (Dolma, 2023). Sağlam veri koruma önlemlerini alırken AB içinde serbest veri akışını teşvik ederek, üye devletleri yerelleştirme yerine tek tip veri koruma standartlarını benimsemeye teşvik etmektedir.Yapay zeka çağında veri gizliliği, yapay zekanın ve makine öğreniminin büyümesi, kişisel verilerin özellikle otomatik karar verme süreçlerinde potansiyel olarak kötüye kullanılmasına ilişkin endişeleri artırmaktadır (Can, 2023). Yapay zekanın etik kullanımına ilişkin net yönergeler geliştirilmesi ve uygulanması, yapay zekâ algoritmalarında şeffaflık ve hesap verebilirliğe yönelik mekanizmalar uygulanması gerekmektedir. Nesnelerin interneti ve 5G ağları gibi yeni teknolojiler yaygınlaştıkça, bu bağlamlarda kişisel verilerin korunması daha da zorlaşmaktadır (Can, 2023). Gelişmekte olan teknolojilerde veri korumasına yönelik özel düzenlemeler ve standartlar oluşturulması ve gizliliğin bunların tasarım ve uygulamasının ayrılmaz bir parçası olmasını sağlayarak bilgi güvenliğine katkıda bulunulacağı düşünülmektedir. Küçük ve orta ölçekli işletmeler, sınırlı kaynak ve bilgi nedeniyle kişisel verilerin korunmasına ilişkin yasalara uyumluluğu konusunda zorluk yaşayabilir ve uyumsuzluk para cezalarına ve yasal sonuçlara yol açabileceği değerlendirilmektedir. Küçük ve orta ölçekli işletmelere, kişisel verilerin korunması yasalarına uyumluluğu için eğitim materyalleri, eğitim ve araçlar da dahil olmak üzere erişilebilir ve uygun eğitim ve sertifikasyon programlarına dahil olmaları sağlanabilir (Güleç ve Kişman, 2021).

Teknolojinin hızlı gelişimi ve verilerin hayatımızdaki giderek artan önemi göz önüne alındığında, AB kişisel verilerinin korunması devam eden bir zorluktur. Kişisel veri koruması için güçlü bir temel oluşturulsa da yukarıda özetlenen sorunların çözümü sürekli çaba ve uyum gerektirir. AB, önerilen çözümleri uygulayarak ve yeni zorluklar karşısında tetikte kalarak, kişisel verilerin korunmasında ve vatandaşlarının mahremiyet haklarının desteklenmesinde öncülük etmeye devam etmektedir. Bu sadece bireylere fayda sağlamakla kalmayacak, aynı zamanda dijital ekonomide güveni ve yeniliği de teşvik edeceği değerlendirilmektedir. Kişisel verilerin bilgi güvenliği kapsamında korunması, bireylerin mahremiyetinin sağlanması ve veri koruma düzenlemelerine uyumun önemli bir unsurudur. Bilgi güvenliği uygulamaları, verileri yetkisiz erişime, ihlallere ve diğer kötüye kullanım biçimlerine karşı korumak için tasarlanmıştır (Bilir, 2021).

4.2. Ulusal Düzenlemeler

Birçok ülke, sınırları içindeki tehditlere karşı özel siber güvenlik yasaları çıkarmıştır. Bu yasalar genellikle veri koruma, kritik altyapı koruması ve siber suçlara yönelik cezalara ilişkin hükümler içerir.

Avrupa Birliği'nin kişisel verileri koruma yönetmeliği gibi düzenlemeler, veri korumaya yönelik standartları belirlemektedir (Dolma, 2023). Bu düzenlemeler, kuruluşların bireylerin kişisel verilerini korumasını ve veri ihlallerinde ciddi para cezaları uygulamasını zorunlu kılmaktadır. Birçok Avrupa Birliği üyesi ülke enerji, ulaşım ve sağlık gibi kritik altyapı sektörlerini siber tehditlerden korumak için yasa ve düzenlemeler geliştirmiştir. Bu yasalar genellikle bu sektörlerdeki kuruluşların belirli güvenlik önlemlerini uygulamasını gerektirmektedir. Çeşitli ülkelerdeki bilgisayar suçları yasaları, yetkisiz

erişim, veri hırsızlığı ve kötü amaçlı yazılım dağıtımı gibi siber suçlarla ilgili suçları özetlemektedir. Bu yasalar, siber suçluların kovuşturulmasına ilişkin yasal dayanağı belirlemektedir (Köksoy, 2020).

Yargı alanındaki zorluklar, siber uzay sınırların ötesinde faaliyet göstermektedir ve bu da siber suçları kovuşturmaktan sorumlu olan yargı yetkisinin belirlenmesini zorlaştırmaktadır. Bu zorluğun çözümü uluslararası iş birliğini gerektirmektedir. Bir siber saldırının kaynağını belirlemek karmaşık olabilir ve yanlış konum bilgileri ile niteliğin belirlenmesi hukuki işlem açısından çok önemli hale gelmektedir (Atlı, 2020). Güvenlik ve gizlilik dengesi ile siber güvenlik önlemleri ile bireysel gizlilik arasında doğru dengeyi kurmak, hukuk sistemlerinin bu ikisi arasındaki gerilimi gidermek için sürekli olarak gelişmesi nedeniyle süregelen bir zorluktur (Köksoy, 2020). Yasal çerçevenin, devlet destekli aktörler ve gelişmiş kalıcı tehditler gibi hızla gelişen siber tehditlere uyum sağlaması gerekmektedir.

5. KİŞİSEL VERİLERİN KORUNMASI ve VERİ İHLALİ BİLDİRİMLERİ

Günümüzün dijital çağında, kişisel verilerin korunması küresel olarak giderek daha önemli bir konu haline gelmekte, Türkiye'de birçok ülke gibi kişisel verilerin korunmasının önemini kavramış ve bireylerin bilgilerinin mahremiyetini ve güvenliğini sağlamak amacıyla çeşitli düzenleme ve uygulamaları hayata geçirmiştir. Türkiye'nin kişisel verilerin korunmasına yönelik yolculuğu, Kişisel Verilerin Korunması Kanunu'nun (KVKK) 2016 yılında kabul edilmesiyle başlamıştır. KVKK, Avrupa Birliği'nin Genel Veri Koruma Yönetmeliği ile yakından uyumludur ve kişisel verileri üzerinde daha fazla kontrole sahip bireyler ortaya çıkmaktadır (Bilir, 2021). KVKK, kanun hükümlerinin gözetimi ve uygulanması amacıyla Kişisel Verileri Koruma Kurumu kurulmuştur. KVKK'da kişisel veri, kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi olarak tanımlanıyor ve "veri sahibi" olarak anılıyor. İsimler, kimlik numaraları, fiziksel, fizyolojik, genetik, ekonomik, kültürel ve sosyal bilgiler dahil olmak üzere çok çeşitli verileri kapsamaktadır (Karakaş, 2020). KVKK, işlemenin gerekliliği, rıza, amaç sınırlaması, veri minimizasyonu, doğruluk, saklama sınırlaması, bütünlük ve gizlilik ve hesap verebilirlik dahil olmak üzere kişisel verilerin hukuka uygun işlenmesine ilişkin temel ilkeleri belirlemektedir. Kuruluşların kişisel verileri işlerken bu ilkelere uymalarını sağlamaları gerekmektedir (Özer Deniz, 2023).

KVKK, veri sahiplerine; bilgi edinme, verilere erişme, düzeltme, silme ("unutulma hakkı"), veri taşınabilirliği ve veri işlenmesine itiraz etme hakkı dahil olmak üzere çeşitli haklar vermektedir. Veri sahipleri bu haklarını veri sorumlularına talepte bulunarak kullanabilirler (Karakaş, 2020). KVKK, kişisel verilerin işlenmesinde iki temel rolü tanımlamaktadır, veri denetleyicileri ve veri işleyenlerdir. Veri sorumluları, veri işleme amaçlarını ve araçlarının belirlenmesinden sorumludur; veri işleyenler ise veri sorumluları adına verileri işle, her ikisi de yasaya uymak ve veri korumasını sağlamakla yükümlüdür (Özer Deniz, 2023). Kişisel verilerin Türkiye dışına aktarılması belirli kısıtlamalara ve şartlara tabidir. Uluslararası veri aktarımları sırasında yeterli güvenlik önlemleri alınmalı ve veri sahiplerinin hakları korunmalıdır. KVKK, kuruluşların veri sahipleri açısından yüksek risklere yol açabilecek kişisel verileri işlerken Veri Koruma Etki Değerlendirmeleri yapmalarını zorunlu kılmaktadır (Kağıtcıoğlu, 2016). Veri Koruma Etki Değerlendirmeleri, veri işleme faaliyetlerindeki potansiyel gizlilik risklerinin belirlenmesine ve azaltılmasına yardımcı olmaktadır.

Kişisel veri ihlali durumunda veri sorumluları, durumu gecikmeksizin hem Kişisel Verileri Koruma Kurumuna hem de etkilenen veri sahiplerine bildirmekle yükümlüdür. Bu, bireylerin kendilerini korumak için uygun önlemleri alabilmelerini sağlar. KVKK, Kişisel Verileri Koruma Kurumuna kanunları uygulama yetkisi vermektedir. Uyumsuzluğa ilişkin cezalar para cezalarını, uyarıları ve idari yaptırımları içerebilir; bu da kuruluşların düzenlemelere uyma konusunda güçlü bir teşvike sahip olmasını sağlamaktadır. Türkiye'de hükümet, çeşitli kuruluşlarla birlikte, bireyleri ve kuruluşları kişisel verilerin korunmasının önemi konusunda bilgilendirmek amacıyla kamuoyunu bilinçlendirme kampanyaları ve eğitim programları yürütmektedir. Bu, ülkede veri gizliliği kültürünü teşvik etmektedir (Yosif, 2021). Türkiye'de kişisel verilerin korunması, başta Avrupa Birliği'nin Genel Veri Koruma Yönetmeliği olmak üzere uluslararası veri koruma standartlarına uyumlu olan Kişisel Verilerin Korunması Kanunu (KVKK) kapsamında düzenlenmektedir. Bu kapsamlı yasal çerçeve ve Kişisel Verileri Koruma Kurumunun rolü, veri sahiplerinin haklarının ve gizliliğinin korunmasını sağlamaktadır.

Türkiye'deki kuruluşların kişisel verilerin hukuka uygun işlenmesini sağlamak için KVKK ilke ve yükümlülüklerine uymaları gerekmektedir. Çeşitli endüstriler ve profesyonel kuruluşlar, kişisel verilerin korunmasına yardımcı olmak için veri koruma standartları oluşturmuştur (Turan Başara, 2020). Ödeme Kartı Sektörü Veri Güvenliği Standardı, ödeme kartı bilgilerinin güvenliğine yönelik gereklilikleri belirleyen, ödeme kartı endüstrisinde dikkate değer bir örnektir.

6. ELEKTRONİK HARP VE KAMU YÖNETİMLERİNDE BİLGİ GÜVENLİĞİNİN ÖNEMİ

Elektronik harp, karıştırma, müdahale ve sinyal istihbaratını ve elektronik teçhizat ile gerçekleştirilen her türlü siber uzay ve istihbarat faaliyetlerini kapsamaktadır. Elektronik harpte devlet davranışını düzenleyen kural ve normları oluşturmak için uluslararası hukuki ve diplomatik tartışmalara daha çok yer verilmesi gerekmektedir. Elektronik harbe ilişkin uluslararası anlaşmaların oluşturulmasına yönelik çalışmalar devam etmektedir. Bilgi savaşının ulus devletlerle sınırlı olmadığını belirtmek önemlidir; hacktivist gruplar, suçlular ve hatta bireysel aktörler bu taktiklerin bazılarını kendi amaçları doğrultusunda kullanabilir, kesinti potansiyeli ve saldırıları ilişkilendirmenin zorluğu göz önüne alındığında, bilgi savaşı dijital çağda önemli bir endişe kaynağı olmakta ve bu tehditlere karşı savunmak için uluslararası iş birliği ve güçlü elektronik harp önlemleri şart olmaktadır (Güntay, 2019).

Devlet kurumları, belediyeler ve kamu kurumları da dahil olmak üzere kamu idarelerine büyük miktarda hassas veri emanet edilmektedir. Bu veriler vatandaş bilgilerinden mali kayıtlara ve gizli hükümet belgelerine kadar çeşitlilik göstermektedir. Bu bilgilerin korunması çok önemlidir ve bunu etkili bir şekilde yapabilmek için kamu idarelerinin sağlam bilgi güvenliği uygulamaları ve politikaları oluşturması gerekmektedir (Güntay, 2019). Elektronik harp, elektronik sistemleri manipüle etmek veya bozmak için çeşitli strateji ve taktikleri kapsayan çok yönlü bir disiplindir (Schleher, 2004). Elektronik gözetleme, e-postalar ve telefon çağrıları gibi elektronik iletişimlerin dinlenmesi ve izlenmesi elektronik harp faaliyetleri arasında yer almaktadır. Karıştırma, Kablosuz iletişim, radar ve navigasyon sistemlerini bozmak veya bunlara müdahale etmek için radyo frekansı sinyallerinin yüksek güç ile yayılmasını ifade etmektedir (Schleher, 2004). Siber saldırılar, genellikle verileri çalmak, değiştirmek veya yok etmek amacıyla bilgisayar ağlarına ve sistemlerine sızarak şeklinde bir elektronik harp bileşeni olarak ortaya çıkmaktadır (İzzetgil, 2021).

Gelişmiş siber tehditler, elektronik harp alanındaki siber saldırılar giderek daha karmaşık hale gelerek, ulus devletler, organize suç grupları ve bilgisayar korsanları güvenlik önlemlerini ihlal etmek için gelişmiş teknikler kullanmaktadır (Atlı, 2019). Dijital çağ, kişisel verilerin katlanarak büyümesine yol açmış, veriler çeşitli platformlarda oluşturuldukça, paylaşıldıkça ve depolandıkça onu korumak daha zor hale gelmektedir. Birbirine bağlı cihazlar, nesnelerin interneti, saldırı yüzeyini genişleterek kişisel verilere erişmek için birbirine bağlı cihazlardaki güvenlik açıklarından yararlanmaktadır (Özkaya ve Toprak, 2022).

Dijital çağ benzeri görülmemiş kolaylıklar getirdi ancak aynı zamanda bireyleri ve kuruluşları, kişisel verilerin güvenliğini tehlikeye atabilecek elektronik harp dahil yeni tehditlere de maruz bıraktmaktadır. Kişisel verilerin korunmasına odaklanan bilgi güvenliği, elektronik harp taktiklerine karşı korunmada çok önemli bir rol oynamaktadır (Özkaya ve Toprak, 2022).

Elektronik harp, hem bireyler hem de kuruluşlar açısından kişisel veri güvenliği bakımından önemli bir tehdit oluşturmaktadır (Atlı, 2019). Dijital bilgi alışverişi çağında kişisel verilerin korunması en büyük önceliktir. Veri şifreleme, erişim kontrolü ve güçlü izleme gibi bilgi güvenliği uygulamaları, kişisel verilerin elektronik savaş taktiklerine karşı korunmasında önemli bir rol oynamaktadır. Elektronik harp taktikleri gelişmeye devam ettikçe bireylerin ve kuruluşların bilgi güvenliği önlemlerinde dikkatli ve proaktif olmaları zorunludur. En iyi uygulamalara bağlı kalarak, güçlü savunmalar uygulayarak ve ortaya çıkan tehditler hakkında bilgi sahibi olarak kişisel veriler, giderek karmaşıklaşan elektronik harp ortamına karşı korunabilir ve bunu yaparak bireyler ve kuruluşlar, dijital güvenlik açığı çağında kişisel verilerin gizliliğini, bütünlüğünü ve kullanılabilirliğini koruyabilirler (Schleher, 2004).

Siber saldırı teknikleri sürekli gelişiyor ve bireylerin ve kuruluşların dikkatli kalmasını ve etkili karşı çözümler uygulamasını hayati önem taşımaktadır. Siber güvenliğe kapsamlı bir yaklaşım, sürekli değişen tehdit ortamına karşı savunma sağlamak için teknik önlemlerin, kullanıcı eğitiminin ve devam eden güvenlik değerlendirmelerinin bir kombinasyonunu içermektedir (Kutlu, 2023). Bu saldırı tekniklerini anlayarak ve bunlara karşı farkındalık ile proaktif önlemler alarak dijital varlıklarımızı ve verilerimizi daha iyi koruyabiliriz (İzzetgil, 2021).

Elektronik harp, dünya çapında kamu idarelerinin modern savunma ve güvenlik stratejilerinde çok önemli bir rol oynamaktadır. Teknoloji ilerlemeye devam ettikçe, elektronik ve elektromanyetik araçların saldırı, savunma ve keşif amaçlı kullanımı giderek daha karmaşık hale gelmektedir (Nezgıtlı ve Benzer, 2020). Bununla birlikte, elektronik harbin kamu idareleri tarafından uygulanması, ulusal güvenliğin korunması ile yasal sınırların korunması arasında bir denge sağlamak için hukuk çerçevesinde hareket etmeli ve kamu idareleri tarafından yürütülen elektronik harp, ulusal ve uluslararası yasal çerçevelere kapsamında olmalıdır (Sandilaç, 2022). Siber operasyonlar da dahil olmak üzere silahlı çatışmalarda güç kullanımı, uluslararası teamül hukuku ve anlaşmalar da dahil olmak üzere uluslararası hukuka tabiidir. Kamu idareleri, orantılılık, ayrım ve askeri gereklilik ilkelerini içeren uluslararası insan hakları hukukuna uyumu sağlamak zorundadır (Kurudal, 2020).

Kamu yöneticileri, elektronik harp uygulamalarını yürütürken ulusal yasa ve yönetmeliklere uymak zorundadır. Bu yasalar, veri koruma, mahremiyet ve siber yeteneklerin saldırgan amaçlarla kullanılması gibi konuları düzenlemektedir. Örneğin kişisel verilerin korunması kanunu v.b. gibi veri koruma yasaları, kişisel verilerin işlenmesine ilişkin katı gereklilikler getirmektedir. Elektronik harp uygulamalarından olan siber saldırıların gerçek kaynağını belirlemek, siber uzayın doğası gereği zor olabilmektedir (Aydın vd., 2017). Kamu idareleri, siber olayların sorumluluğunu doğru bir şekilde atfetmek için proaktif mekanizmalara sahip olmalı ve siber atıf, siber tehditlere yanıt verirken yasal ve diplomatik amaçlar için kritik öneme sahip olmaktadır (Kurudal, 2020).

Siber casusluk, elektronik harbin önemli bir yönüdür. İstihbarat toplama uluslararası hukuk tarafından açıkça yasaklanmamakla birlikte, kamu idareleri siber casusluk faaliyetlerinin yasal ilkelere uygun olmasını ve diğer ulusların egemenlik veya mahremiyet haklarını ihlal etmemesini sağlaması gerekmektedir (İzzetgil, 2021). Etik hususlar, elektronik harbi yöneten yasal çerçeve ile iç içe geçmiş durumda olup, kamu yönetimleri, siber operasyonların potansiyel faydalarını ve risklerini tartmalı ve eylemlerin yasal gereklilikler ve etik ilkelerle uyumlu olmasını sağlamalıdır (Sandilaç, 2022). Siber uzayda istikrarı desteklemek için siber yeteneklerin sorumlu kullanımı esas olmaktadır. Hızla gelişen dijital ortamda bilgi güvenliği ve elektronik harp, ulusları, kuruluşları ve bireyleri siber tehditlerden korumada ve hassas verilerin bütünlüğünü ve gizliliğini sağlamada ve istihbarat toplanmasında kritik rol oynamaktadır (Kuntoğlu, 2021). Bilgi güvenliği, bilgileri ve dijital varlıkları yetkisiz erişim, ifşa, değiştirme veya imhadan korumak için tasarlanmış bir dizi uygulama, teknoloji ve politikayı kapsamaktadır. Verilerin gizliliğini, bütünlüğünü ve kullanılabilirliğini ele alan çok yönlü bir disiplindir.

Bilgi güvenliği ve elektronik harp birbirini tamamlayan aynı zamanda birbirine karşı zıt iki disiplin olarak nitelendirilebilir. Elektronik harp uygulamalarından olan elektronik korunma pratikleri bilgi güvenliğinin sağlanması ve bilginin zarar görmemesine olanak tanımaktadır (Szczepaniuk vd., 2020). Bilgi güvenliği ve elektronik harp arasında girift bir ilişki bulunmakta olup, kamu yönetimlerinde bilginin güvenli bir şekilde korunması ve savunulması için elektronik harp uygulamalarına ihtiyaç duyulmaktadır. Devlet yönetiminde yer alan kamu yöneticileri ve kamu personelleri hassas ve kıymetli bilgilerin korunması ve vatandaşların kişisel verilerinin koruması için elektronik harp hakkında bilgilendirilmeli ve eğitim programlarında elektronik harbe yer verilmesi gerekmektedir (Nezgıtlı ve Benzer, 2020).

Kamu yönetimlerinde bilgi güvenliği son derece önemlidir. Kamu idareleri, sosyal güvenlik numaralarından sağlık kayıtlarına kadar çok çeşitli vatandaş verilerini toplar ve saklamakta, bu bilgilerin ihlali kimlik hırsızlığına, mali dolandırıcılığa ve vatandaşlar açısından diğer ciddi sonuçlara yol açabilmektedir. Birçok devlet kurumu, ulusal güvenlikle ilgili gizli veya hassas bilgileri ele alarak, yetkisiz erişim veya sızıntılar bir ülkenin güvenliği ve çıkarları için tehdit oluşturarak kamu güvenliğini tehlikeye atabilir. Kamu idareleri çok sayıda veri koruma kanununa ve düzenlemesine tabii olarak,

bunlara uyulmaması hukuki sonuçlara yol açabileceği gibi idarenin itibarının zedelenmesine neden olabilmektedir (Karakaş, 2020). Kamu idareleri hizmetlerini giderek dijitalleştirirken, çevrimiçi portalların ve veri tabanlarının güvenilirliği ve güvenliği kritik hale gelmekte, e-devlet hizmetlerinin güvenli ve kullanılabilir olmasını sağlamak vatandaşların güveni ve memnuniyeti açısından hayati öneme sahip olmaktadır.

Bilgi güvenliği uygulama ve politikaları, kamu idarelerinin işledikleri hassas bilgileri koruma çabalarının omurgasını oluşturmaktadır. Dijitalleşmenin ve siber tehdit potansiyelinin arttığı bir çağda, veri gizliliğini, bütünlüğünü ve kullanılabilirliğini korumak yalnızca en iyi uygulama değil aynı zamanda yasal ve etik bir zorunluluktur. Bilgi güvenliği uygulamalarının ve politikalarının etkili bir şekilde uygulanması yalnızca verileri korumakla kalmaz, aynı zamanda vatandaşların güvenini, mevzuat uyumluluğunu ve kamu idarelerindeki ulusal güvenlik çıkarlarını da desteklemektedir (Atlı, 2019). Kamu idareleri, bilgi güvenliğine öncelik vererek, veri ihlalleri ve siber saldırılarla ilişkili riskleri azaltırken, vatandaşlarına daha iyi hizmet vermeyi amaçlamaktadır.

SONUÇ

Günümüzde kullanılan sosyal medya uygulamaları, mesajlaşma programları ve benzeri bütün elektronik uygulamalar günlük hayatımızı kolaylaştıran uygulamalardır. Bu uygulamaların tümü kişisel verilere erişim ile gerçekleşmektedir. Elektronik harp günümüze kadar daha çok askeri ve istihbarat faaliyetlerinde kullanılmaktaydı. Teknoloji çağı olan bugünlerde ise elektronik harp, bireysel ve uluslararası erişim imkanları ile sivil gündelik hayatımıza dahil olmaktadır. Kişisel verilerin korunması, bilgi yönetimi ve bilgi güvenliği, dijital güvenlik bütün bu alanlardaki argümanların birer elektronik harp bileşeni olduğu ve hayatımızı kolaylaştıran bu uygulamalar olmadan teknolojiyi aktif ve etkin kullanmanın mümkün olmayacağı açıkça ortadadır. Bu çalışma ile sosyal bilimler de elektronik harp 'in yerini alması ve elektronik harp üzerinde daha fazla çalışma yapılması gerekliliğine vurgu yapılmaya çalışılmıştır. Çünkü kamu yönetimlerini doğrudan ilgilendiren ulusal güvenlik ve bilgi güvenliğinin elektronik harp ile bağlantılı olduğuna dikkat çekilmeye çalışılmıştır.

Kamu yöneticilerinin görevlerinin ifa ederken bilgi güvenliği ve elektronik harp bileşenleri hakkında bilgilendirilmeli ve bilişim teknolojilerinin hızlı gelişiminden dolayı, elektronik harp sürekli eğitim merkezlerinin oluşturularak kamu yöneticilerinin ve kamu da görev yapan personelin bilgilendirilmesi gerekmektedir. Elektronik harp hakkında oluşabilecek endişelerin başında yer alan etik konusunda da kamu yöneticilerinin eğitilmesi gerekmektedir.

Kişisel verilerin korunması ile ilgili ulusal ve uluslararası mevzuatında gözden geçirilerek bir birleri ile uyumlu olması sağlanmalı, kişisel mahremiyetin korunması noktasında gereken hassasiyetin gösterilmesi gerekmektedir. Etkin ve rekabet edebilir bir kamu yönetim sistemi için elektronik harp tüm bileşenleri ve yönleriyle değerlendirilmelidir.

KAYNAKÇA

Alagöz, A. & Allahverdi, M. (2011). Kurumsal bilgi güvenliği ve muhasebe bilgi sistemi. *Muhasebe ve Vergi Uygulamaları Dergisi, 4*(3): 47-60.

Aliusta, C. ve Benzer, R. (2018). Avrupa siber suçlar sözleşmesi ve Türkiye'nin dahil olma süreci. *Uluslararası Bilgi Güvenliği Mühendisliği Dergisi, 4*(2): 35-52.

Aslay, F. (2017). Siber saldırı yöntemleri ve Türkiye'nin siber güvenlik mevcut durum analizi. *International Journal of Multidisciplinary Studies and Innovative Technologies, 1*(1): 24-28.

Atılgan, D. (2009). Bilgi yönetimi kavramı ve gelişimi. *Türk Kütüphaneciliği Dergisi, 23*(1): 201-212.

Atlı, T. (2019). Kişisel verilerin önleyici, koruyucu ve istihbari faaliyetler amacıyla işlenmesi. *Necmettin Erbakan Üniversitesi Hukuk Fakültesi Dergisi 2*(1): 4-22.

Atlı, T. (2020). Kişi haklarının ihlali durumunda internet erişiminin engellenmesi. *Necmettin Erbakan Üniversitesi Hukuk Fakültesi Dergisi 3*(1): 4-32.

Aydın, H. (2022). Yönetim bilgi sistemlerinde (ybs) siber güvenliğin önemi. *Bilgisayar Bilimleri ve Teknolojileri Dergisi*, *3*(2): 1-8.

Aydın, Ö. vd. (2017). Elektronik harp ile toplanan verilerin veri madenciliği yöntemleri ile analiz edilmesi. *Acta Infologica, 1*(1): 12-22.

Baran, S. & Şener, E. (2020). Örgütlerde bilgi güvenliğini etkileyen bir unsur: Örgütsel bilgi paylaşımı. *Pamukkale Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, *41*, 410-427.

Bilir, F. (2021). Kişisel verilerin korunması kişinin kendisinin korunmasıdır. *Trt Akademi Dergisi*, *6*(11): 172-181.

Can, E. (2023). Yapay zeka sistemlerinin siber suçlarla mücadaleki rolü: Uluslararası hukuk incelemesi. *Ankara Hacı Bayram Veli Üniversitesi Hukuk Fakültesi Dergisi*, *27*(3): 345-382.

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

Çahmutoğlu, E. (2020). Siber uzayda güç ve siber silah teknolojilerinin küresel etkisi. *Analytical Politics*, *1*(1): 1-17.

Çakır, H. ve Arınmış Uzun, S. (2021). Türkiye'nin siber güvenlik eylem planlarının değerlendirilmesi. *Ekonomi İşletme Siyaset ve Uluslararası İlişkiler Dergisi*, *7*(2): 353-379.

Çalışkan**,** A. (2023). Siber savaş: Bilgi krizi mi yoksa güvenliği mi?. *Savunma ve Savaş Araştırmaları Dergisi, 33*(1): 1-32.

Çam, H. Aslay, F. ve Özen, Ü. (2019). Yükseköğretim kurumlarında bilgi güvenliği farkındalık düzeylerinin ölçümlenmesi. *Yönetim Bilişim Sistemleri Dergisi*, *5*(2): 1-11.

Çelik, S. (2018). Siber uzay ve siber güvenliğe mutlidisipliner bir yaklaşım. *Academic Review of Humanities and Social Sciences, 1*(2): 110-119

Dayıoğlu, E. (2016). Kamu idarelerinde bilgi sistemi güvenlik risklerinin yönetimi. *Denetişim, 4*, 71-81.

Demirtaş, Ö. & Karaca, M. (2018). Siber mobbing: Kavramsal çerçeve, öncülleri ve sonuçları. *International Journal Entrepreneurship and Management Inquiries Dergisi*, *2*(2): 20-34.

Dolma, Ö. (2023). Siber güvenlik ihbarcılarının korunması açısından ABD ve AB yaklaşımlarının karşılaştırılması. *Pamukkale Üniversitesi İşletme Araştırmaları Dergisi*, *10*(2): 615-631.

Edegbeme-Belaz, A. & Kerti, A. (2022). A new approach to ınformation security auditing in public administration, *Hadmernok*, *17*(3): 109-131.

Efendioğlu, A. & Sezgin, E. (2007). E-Devlet uygulamalarında bilgi ve paylaşma güvenliği. *Ç.Ü. Sosyal Bilimler Enstitüsü Dergisi, 16*(2): 219-236.

Eldem, T. (2021). Uluslararası siber güvenlik normları ve sorumlu siber egemenlik. *İstanbul Hukuk Mecmuası, 79*(1): 347-378

Güldoğan, M. V. & Işıklı, Ş. (2022). Siber savaşta mütekabiliyet. *Academic Journal of Information Technology, 13*(51): 289-319.

Güleç, Ö. & Kişman, Z.A. (2021). Uluslararası ilişkiler açısından siber güvenlik ve NATO'nun siber güvenlik stratejileri. *Akademik Açı*, *1*(1): 127-154.

Güngör, U. & Güney, O. (2017). Uluslararası ilişkilerde güvenliğin dönüşümü çerçevesinde bilgi güvenliği ve siber savaş. *Karadeniz Araştırmaları Merkezi*, *15*(55): 131-146.

Güntay, V. (2018). Siber güvenliğin uluslararası politikada etki aracına dönüşmesi ve uluslararası aktörler. *Güvenlik Stratejileri Dergisi*, *14*(27): 79-111.

Güntay, V. (2019). 21.Yüzyıl paradoksu olarak siber uzay ve uluslararası hukuk. *Novus Orbis: Siyaset Bilimi ve Uluslararası İlişkiler Dergisi*, *1*(2): 87-109

İleri, Y.Y. (2017). Örgütlerde bilgi güvenliği yönetimi, kurumsal entegrasyon süreci ve örnek bir uygulama. *Anadolu Üniversitesi Sosyal Bilimler Dergisi*, *17*(4): 55-72.

İzzetgil, E. (2021). Bilimsel – teknolojik gelişmelerin terörizme etkisi olarak siber terörizm ve türkiye için siber terör tehdidi. *Uluslararası Kriz ve Siyaset Araştırmaları Dergisi*, *5*(2): 837-878.

Kağıtcıoğlu, M. (2016). Kişisel verileri koruma kurumuna idare hukuku çerçevesinden bir bakış. *İstanbul Kemerburgaz Üniversitesi Sosyal Bilimler Dergisi*, *1*(2): 77-99.

Karaca, M. ve Gül, E. (2021). Kritik altyapılara yönelik bilişim suçları, Türkiye ve AB uygulamaları. *Bilişim Hukuku Dergisi*, *3*(1): 1-30.

Karakaş, M. E. (2020). Dijital geçmişin internet erişiminden kaldırılması "unutulma hakkı" ve türk hukukunda görünümü. *Necmettin Erbakan Üniversitesi Hukuk Fakültesi Dergisi*, *3*(2): 262-289

Karaoğlan Yılmaz, G. Yılmaz, R. & Sezer, B. (2014). Üniversite öğrencilerinin güvenli bilgi ve iletişim teknolojisi kullanım davranışları ve bilgi güvenliği eğitimine genel bir bakış. *Bartın Üniversitesi Eğitim Fakültesi Dergisi***,** *3*(1): 176-199.

Karasoy, H.A. ve Babaoğlu, P. (2021). Türkiye'de siber güvenlik: Yasal ve kurumsal altyapı. *Yasama Dergisi***,** *44*, 124-155.

Kayacı, M. (2019). Kamu yönetiminde etik bağlamında güvenlik hizmetleri etiğine bir bakış. *Sosyal Bilimler Akademi Dergisi*, *2*(1): 50-69.

Korucu, O. (2021). Yeni normal dünya düzeninin siber güvenlik ve bilgi güvenliği etkileri. *Yönetim Bilişim Sistemleri Dergisi*, *7*(1): 44-60.

Köksoy, F. (2020). Avrupa Birliği'nin siber güvenlik politikası: Kurumsalcılık mı tutarlılık mı?. *Güvenlik Stratejileri Dergisi*, *16*(35): 635-674.

Kuntoğlu, Ö. F. (2021). Elektronik ticarette kişisel verirlerin korunması. *Bilişim Hukuku Dergisi*, *3*(1): 176-229.

Kurudal, O. (2020). Bilişim çağında siber saldırılar. *Dünya İnsan Bilimleri Dergisi, 2*, 132-158.

Kutlu, F.B. (2023). Eski iki müttefik için yeni bir alan: AB ve NATO'nun siber güvenlik yaklaşımları (2016-2020). *Diplomasi Araştırmaları Dergisi*, *5*(1): 25-41.

Marşap, A. Akalp, G. & Yeniman, E. (2010). Sağlık işletmelerinde insan kaynağının kurumsal bilgi güvenliği kültürü gelişimi. *Bilişim Teknolojileri Dergisi*, *3*(1): 31-40.

Martinn, V. ve Pehlivan ,İ. (2010). ISO 27001:2005 bilgi güvenliği yönetim standartı ve Türkiye'deki bazı kamu kuruluşu uygulamaları üzerine bir inceleme. *Mühendislik Bilimleri ve Tasarım Dergisi*, *1*(1): 49-56.

Nezgıtlı, S. ve Benzer, R. (2020). Avrupa Birliği siber güvenlik kanunu. *Bilişim Sistemleri ve Yönetim Araştırmaları Dergisi*, *2*(1): 11-18.

Nurata, Z. C. (2021). Hukuksal, örgütsel ve etik bir sorun olarak iş yerinde elektronik gözetim. *Gazi İktisat ve İşletme Dergisi*, *7*(3): 214-225.

Orak, M. (2021). Siber ordular ve siber savaşlar. *Kaytek Dergisi*, *3*(2): 214-226.

Önen, S.M. ve Kurnaz, S. (2017). Siber güvenlik politikalarının kamu yönetimine yansıması. *Turgut Özal Uluslararası Ekonomi ve Siyaset Kongresi IV*, 732-752.

Önok, M. (2013). Avrupa konseyi siber suç sözleşmesi ışığında siber suçlarla mücadelede uluslararası işbirliği. *Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi, 19*(2): 1229-1270.

Özbilen, T. & Çağlar, A. (2020). Türk kamu sektöründe bilgi ve bilişim güvenliği. *Kamu Yönetimi ve Teknoloji Dergisi*, *1*, 72-93.

Özdemir**,** A. & Uluyol, Ç. (2021). Kamu kurum ve kuruluşlarında bilgi güvenliği farkındalığı. *Türkiye Sosyal Araştırmalar Dergisi*, *25*(3): 649-666.

Özer Deniz, M. (2023). Kişisel verilerin işlenmesi sözleşmesinin türleri ve hukuki nitelikleri**.** *Necmettin Erbakan Üniversitesi Hukuk Fakültesi Dergisi*, *6*(1): 97-114.

Özkaya, Ö. & Toprak, İ. (2022). Türkiye'de güvenlik faaliyetleri kapsamında kişisel verilerin işlenmesi. *MANAS Sosyal Araştırmalar Dergisi*, *11*(3): 1291-1305.

Renda, K. K. (2022). Avrupa siber güvenlik politikalarının gelişimi: Eşgüdümcü rol'den siber güce. *Ankara Avrupa Çalışmaları Dergisi*, *21*(2): 467-495.

Sandilaç, N. (2022). Siber suç, siber terör ve siber savaş üçgeninde siber dünya. *Bilişim Hukuk Dergisi, 4*(1): 141-190.

Schleher, D. C. (2004). *Bilgi çağında elektronik harp*. Çev. Berna Kara 1.Baskı, , Ankara: Doruk Yayımcılık

Sertçelik, A. (2015). Siber olayler ekseninde siber güvenliği anlamak. *Medeniyet Araştırmaları Dergisi*, *2*(3): 25-42.

Szczepaniuk, E. K. ve diğerleri (2020). Information security assessment in public administration. *Computers & Security*, *1*(90): 1-11.

Şenol, M. (2017). Türkiye'de siber saldırılara karşı caydırıcılık. *Ulusal Bilgi Mühendisliği Dergisi*, *3*(2): 1-9.

Tunca, S. (2019). Modern çağda siber güvenlik kavramı. *Dumplupınar Üniversitesi İİBF Dergisi*, *3*(4): 1-7.

Turan Başara, G. (2020). Kişisel veri işleme sözleşmesi. *Uyuşmazlık Mahkemesi Dergisi*, *8*(16): 57-90.

Türkoğlu Üstün, K. (2023). Açık devlet verileri ve bilgi edinme hakkıyla ilişkisi. *Akdeniz Üniversitesi Hukuk Fakültesi Dergisi***,** *13*(1): 301-338.

Uysal, Y. (2020). Klasik kamu yönetiminden yeni kamu işletmeciliği ve post-yki'ye kamu hizmetlerinin değişimi ve dönüşümü üzerine bir değerlendirme. *International Journal of Management and Administration*, *4*(7): 112-135.

Ülker, M. Canbay Y. & Sağıroğlu, Ş. (2017). Nesnelerin internetinin kişisel, kurumsal ve ulusal bilgi güvenliği açısından incelenmesi. *Türkiye Bilişim Vakfı Bilgisayar Bilimleri ve Mühendisliği Dergisi, 10*(2), 28-41.

Vural, Y. & Sağıroğlu, Ş. (2008). Kurumsal bilgi güvenliği ve standartları üzerine bir inceleme. *Gazi Üniversitesi Mühendislik ve Mimarlık Fakültesi Dergisi*, *23*(2): 507-522.

Yılmaz, C. Doğan, A. & Topal, E. (1989). Yönetim bilgi sistemi. *Erciyes Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi, 1*(8): 39-48.

Yılmaz, H. (2014). TS ISO/IEC 27001 bilgi güvenliği yönetim standardı kapsamında bilgi güvenliği ve yönetim sisteminin kurulması ve bilgi güveniği risk analizi. *Denetişim, 15*, 45-59.

Yılmaz, O. S. (2016). Sistem denetiminde iç denetimin rolü ve bilgi güvenliği. *Denetişim*, *8*, 49-59.

Yosif, U. (2021). Kişisel verilerin işlenmesi şartları ve 6698 sayılı kişisel verilerin korunması kanunun ruhu olarak genel ilkeler. *Selçuk Üniversitesi Adalet Meslek Yüksek Okulu Dergisi*, *4*(1): 1-22

EXTENDED ABSTRACT

Today, information consists of all kinds of data specific to individuals and institutions that give people an identity about them. In practice, information security and information security management systems can be achieved as a result of the integration of basic principles such as confidentiality, integrity and accessibility. Confidentiality in information security aims to ensure the confidentiality of data, meaning that only authorized persons or systems can access and view important information. Information security involves implementing encryption, access controls and other measures to prevent unauthorized access. Information security strategies include methods that detect and prevent unauthorized changes in data and maintain its reliability. With the principle of accessibility in information security, information should be accessible to authorized users when necessary. Information security measures include backups, and resilient systems to ensure data can be accessed even in the face of outages or attacks. Establishing and implementing security policies and procedures in information security is vital for organizations. Security policies and procedures are essential for training employees in best security practices, conducting regular security audits, and responding to incidents.

In the study, investigations regarding information security and protection of personal data and their use in daily life are evaluated. Information classification is examined in the information management process. Issues regarding which classes of information and what type of data are processed are examined. Information management covers the entire data processing cycle, from creation and storage of information exchange and destruction. Effective information management is achieved by integrating security measures into the system and comprehensive implementation of encryption protocols, access controls and authentication mechanisms to protect sensitive information from unauthorized access, disclosure or modification. Risk management, compliance and governance, user training and awareness and technology integration constitute the main backbone of the information security management system. Information management and security are closely linked to regulatory compliance and governance. Organizations must comply with legislation regulating the processing, storage and protection of sensitive information, accompanied by special regulations and standards. Compliance ensures that legal obligations are met and helps to build trust among stakeholders.

Human factors are critical in both information security and management. Education and awareness raising among users about best security practices, data processing policies, and the potential risks of misuse of information are important elements of a comprehensive information security approach. The synergy of information and communication technologies, utilizing advanced tools for data analytics, threat detection and secure storage solutions, and being open to innovations help increase the effectiveness of information security. Today, to ensure data integrity, it is necessary to update both risk factors and security policies by closely monitoring technologies such as artificial intelligence-based security measures and blockchain.

Knowledge is classified and explained as superficial knowledge, deep knowledge, technical and applicable knowledge, interpretation-based knowledge, explicit and implicit knowledge. In the study, the situation is evaluated on how to use information effectively and actively on issues related to the concept of information, information management, digital information and information security, risk management and preparation of risk analysis reports, and the definition and elements of electronic warfare are included.

Electronic warfare reshapes the conflict and defense dynamics in modern military strategies, allowing manipulation, counter-attack and defense when needed, covering critical and communication networks. The study also reveals the prediction that the most advanced technologies that shape the future of electronic warfare are included in the scope of electronic warfare. Many technological developments such as artificial intelligence, the internet of things, and machine learning directly or indirectly affect the electronic warfare systems to gain superiority through their moves. In the study, the multifaceted impact areas of electronic warfare are mentioned and the complexities and applications of electronic warfare are emphasized. Electronic warfare refers to openness to the development of radio frequencies and radar signals within the electromagnetic spectrum. Technological developments, capabilities to adapt to dynamic and evolving threats, autonomous systems and threat elements consisting of drones provide both challenges and opportunities in the field of electronic warfare, adding a new dimension to electronic warfare in theory and practice. Today, cybersecurity includes a variety of practices, technologies, and processes designed to protect computer systems, networks, and data from unauthorized access, attacks, and damage. As our dependence on digital platforms increases, protecting sensitive information becomes more important, making electronic warfare the cornerstone of a resilient and secure society. As cyber security is a part of electronic warfare, it is stated in the study that in today's technological age, the concept of new generation electronic warfare should be more comprehensive and gathered under a single roof and the legal basis should be created with the power of international agreements and contracts.

Governments from around the world are highlighting the difficulty of preparing the legal basis governing cyberspace. It does not currently seem possible to talk about the existence of a generally accepted legal

infrastructure within the framework of international law. However, issues such as legislation and directives, protection of personal data, violation reporting and sanctions against cyber crimes come to the fore. The main problems associated with cybercrime are the anonymous nature of many cyber attacks, making it difficult to identify perpetrators and attribute responsibility. Prosecution issues further complicate legal responses and underscore the need for coordinated international efforts to prosecute cybercriminals. The connection between cybersecurity and law is a dynamic and evolving field that requires constant attention and adaptation. As technology continues to reshape the world, a harmonious relationship between legal frameworks and cybersecurity measures is essential to create a resilient and secure digital border.

It demonstrates the importance of working to overcome the challenges of electronic warfare while protecting fundamental rights and principles through international cooperation, legal innovation and interdisciplinary cooperation. Successful information security and electronic warfare management requires collaboration between departments. ICT teams, legal departments, and business units must work together to create comprehensive policies, respond to evolving threats, and ensure information is effectively managed and secured. The intricate relationship between information security and electronic warfare becomes essential in today's digital age. A holistic approach that integrates secure practices throughout the data lifecycle, complies with regulatory requirements, incorporates technological advances, and promotes a culture of security awareness is crucial for organizations aiming to protect valuable information assets. In the study, it is emphasized that the dynamic nature of technology and evolving threat environment emphasizes the need for continuous adaptation and improvement of both information security and electronic warfare strategies.