T.C.
NECMETTİN ERBAKAN ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
SİYASET BİLİMİ VE KAMU YÖNETİMİ ANABİLİM DALI

BİLGİ GÜVENLİĞİ BAĞLAMINDA KİŞİSEL VERİLERİN KORUNMASI VE ELEKTRONİK HARP

MEHMET ALİ KOÇMAN

YÜKSEK LİSANS TEZİ

ÖĞRETİM ÜYESİ:
DOÇ. DR. ERDAL BAYRAKCI

KONYA-2023

T.C.
NECMETTİN ERBAKAN ÜNİVERSİTESİ
Sosyal Bilimler Enstitüsü

Bilimsel Etik Sayfası

	Adı Soyadı	Mehmet Ali KOÇMAN		
	Numarası	19810402060		
	Ana Bilim / Bilim Dalı	Siyaset Bilimi ve Kamu Yönetimi		
	Programı	Tezli Yüksek Lisans	X	
		Doktora		
	Tezin Adı	BİLGİ GÜVENLİĞİ BAĞLAMINDA KİŞİSEL VERİLERİN KORUNMASI VE ELEKTRONİK HARP		

Bu tezin hazırlanmasında bilimsel etiğe ve akademik kurallara özenle riayet edildiğini, tez içindeki bütün bilgilerin etik davranış ve akademik kurallar çerçevesinde elde edilerek sunulduğunu, ayrıca tez yazım kurallarına uygun olarak hazırlanan bu çalışmada başkalarının eserlerinden yararlanılması durumunda bilimsel kurallara uygun olarak atıf yapıldığını bildiririm.

ÖNSÖZ

Çalışmam boyunca bilgi ve deneyimlerinden yararlandığım, ahlaki değerleri ile de örnek aldığım, öncelikle danışmanlığımı üstlenen araştırmanın yürütülmesine dek beni sınırlamayıp özgür bırakan, birlikte çalışmaktan onur duyduğum ve bu süreçte göstermiş olduğu hoşgörü ve sabırdan dolayı değerli hocam Doç. Dr. Erdal BAYRAKCI'ya, tez savunma jürisinde yer alarak değerli görüşleri ile araştırmanın şekillenmesini sağlayan Prof. Dr. Erhan ÖRSELLİ ve Prof. Dr. Mehmet GÖKÜŞ' e sonsuz teşekkürlerimi sunarım.

Tez çalışmalarım sırasında ihtiyaç duyduğum her an, zaman mefhumu gözetmeksizin yanımda olan, maddi ve manevi yardımlarını esirgemeyen, çalışmayı bitirmem konusunda motive eden Ahmet Can TUNCA' ya desteklerinden dolayı teşekkürü borç bilirim.

Hayatımın her anında yanımda olan, maddi ve manevi yardımlarını esirgemeyen, zorlu ve stresli zamanlarda güçlü kalmamı sağlayan sevgili annem Sevim KOÇMAN, babam Osman KOÇMAN, ağabeyim Ali KOÇMAN' a ve ailemin her bir ferdine sonsuz teşekkür ederim.

Bu yüksek lisans tezi, mensubu olmaktan her zaman şeref duyduğum ve malulen emekli olduğum "*Zaferleri ve mazisi insanlık tarihi ile başlayan, her zaman zaferlerle beraber medeniyet nurlarını taşıyan kahraman* ***Türk ordusu!*****" 'na**, "*Ya İstiklâl Ya Ölüm*" parolasıyla başlattığı ve bütün imkânsızlıklara rağmen büyük fedakârlık ve kahramanlıklar göstererek eşsiz bir zaferle taçlandırdığı Türk İstiklal Harbi neticesinde kurulan ve kendi vatanı üzerinde bağımsız yaşama iradesinin vücut bulduğu bir eser olan Cumhuriyet'in 100'üncü yılına erişmesinde Türk birliğinin, Türk kudret ve kabiliyetinin, Türk vatanseverliğinin çelikleşmiş bir ifadesi olan **tüm şehitlerimize** ve Ebedî Başkomutan Mustafa Kemal **ATATÜRK' e** ithaf edilmiştir.

ÖZET

Öğrencinin	Adı Soyadı	MEHMET ALİ KOÇMAN		
	Numarası	19810402060		
	Ana Bilim / Bilim Dalı	SİYASET BİLİMİ VE KAMU YÖNETİMİ		
	Programı	Tezli Yüksek Lisans	X	
		Doktora		
	Tez Danışmanı	DOÇ. DR. ERDAL BAYRAKCI		
	Tezin Adı	BİLGİ GÜVENLİĞİ BAĞLAMINDA KİŞİSEL VERİLERİN KORUNMASI VE ELEKTRONİK HARP		

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. Bilginin önemi kadar bilginin yönetilmesi de ayrı bir çalışma alanı olarak incelenmektedir. 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 hakkında açıklanmaktadır. Bilgi yönetim sisteminde, bilginin sınıflandırılması ve verilerin işlenişini detaylı olarak ele alınmıştır. Çalışma da yer alan, bilgi kavramı, bilgi yönetimi, dijital bilgi ve bilgi güvenliği, risk yönetimi ve risk analiz raporlarının hazırlanmasına ilişkin konulara bilginin etkin ve aktif olarak nasıl kullanılacağına dair durum değerlendirilmesi yapılmakta ve elektronik harp' in tanımı ve unsurlarına yer verilmektedir.

Anahtar Kelimeler: Elektronik Harp, Bilgi Güvenliği, İstihbarat, Dijital Dönüşüm, Sosyal Medya İstihbaratı, Veri Madenciliği,

ABSTRACT

ABSTRACT

Author's	Name and Surname	Mehmet Ali KOÇMAN		
	Student Number	19810402060		
	Department	Political Science and Public Administration		
	Study Programme	Master's Degree (M.A.)	X	
		Doctoral Degree (Ph.D.)		
	Supervisor	Assoc. Prof. Dr. Erdal BAYRAKCI		
	Title of the Thesis/Dissertation	PROTECTION OF PERSONAL DATA AND ELECTRONIC WARFARE WITH IN CONTEXT OF INFORMATION SECURITY		

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. Today, the formation of knowledge is formed as a result of the data formed in the minds of individuals, activating people and making the data meaningful as a whole. The management of knowledge is examined as a separate field of study as well as the importance of knowledge. In the study, information security and the 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.

Keywords: Electronic Warfare, Information Security, Intelligence, Digital Transformation, Social Media Intelligence, Data Mining

İÇİNDEKİLER

ÜÇÜNCÜ BÖLÜM
ELEKTRONİK HARP

KISALTMALAR

AI : Articifical Intelligence
AM : Amplitude Modulation
BGSY : Bilgi Güvenliği Yönetim Sistemi
CD : Compact Disk
CDMA : Code Division Multiple Access
COMINT: Communication Intelligence
ED : Elektronik Destek
EH : Elektronik Harp
EK : Elektronik Korunma
ELINT : Electronic Intelligence
EMS : Elektromanyetik Spektrum
ET : Elektronik Taarruz
FDMA : Frequency Division Multiple Access
FM : Frequency Modulation
GHz : Giga Hertz
GPS : Global Positioning System
GSM : Global System for Mobile
HF : High Frequency
IMINT : Image Intelligence
İDA : İnsansız Deniz Araçları
İHA : İnsansız Hava Araçları
İKA : İnsansız Kara Araçları
LTE : Long-Term Evolution
MHz : Mega Hertz
MODEM: Modulateur and Demodulateur
NATO : North Atlantic Treaty Organization

RF : Radyo Frekans

SIGIN : Signal Intelligence

SOCMINT: Social Media Intelligence

TECHINT: Technical Intelligence

UHF : Ultra High Frequency

UMTS: Universal Mobile Telecommunications System (3G: Üçüncü Nesil)

VHF : Very High Frequency

WCDMA: Wideband Code Division Multiple Access

WiFi : Wireless Fidelity

WWW: Word Wide Web

Giriş

Bilginin özgürce aktığı ve teknolojinin hayatımızın her alanına nüfuz ettiği günümüzün birbirine bağlı dünyasında, sağlam bilgi güvenliği ihtiyacı hiç bu kadar kritik olmamıştır. Kuruluşlar, hükümetler 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 talep eden en önemli endişe haline gelmektedir. Bu çalışma, bilgi güvenliği alanını derinlemesine inceleyerek önemini, zorluklarını ve kapsamlı koruma stratejileri için zorunlu ihtiyacı ortaya koymaktadır.

Günümüzün karmaşık ve hızla gelişen dijital ortamında kuruluşlar, hassas bilgilerini tehlikeye atabilecek ve operasyonlarını kesintiye uğratabilecek bir dizi güvenlik tehdidi ve güvenlik açığıyla karşı karşıyadır. Bu zorlukları etkili bir şekilde aşmak için birçok kuruluş Bilgi Güvenliği Yönetim Sistemlerine yönelmiştir. Bilgi Güvenliği Yönetim Sistemi, bir kuruluşun bilgi varlıklarını yönetmek ve korumak için politikalar, prosedürler ve kontroller oluşturan kapsamlı bir çerçeveyi ifade etmektedir. Risklerin belirlenmesi, güvenlik önlemlerinin uygulanması ve bilgi güvenliği uygulamalarının sürekli olarak izlenmesi ve iyileştirilmesi için yapılandırılmış ve sistematik bir yaklaşım sağlamaktadır. Çalışmanın ilk bölümünde, Bilgi Güvenliği Yönetim Sistemleri alanını inceleyerek, önemlerini, temel bileşenlerini ve değerli bilgilerini korumada kuruluşlara sundukları avantajlardan bahsedilmektedir.

Giderek birbirine bağlanan dünyamızda, kişisel verilerin korunması çok önemli bir endişe kaynağı olarak ortaya çıkmaktadır. Dijital teknolojilerin katlanarak büyümesi ve kişisel bilgilerin yaygın olarak toplanması, saklanması ve işlenmesi ile bireyler, mahremiyetlerine ve güvenliklerine yönelik benzeri görülmemiş risklerle karşı karşıya bırakmaktadır. Kişisel verilerin korunması, yalnızca bireyler için değil, aynı zamanda bu tür bilgileri işlemekle görevlendirilen kuruluşlar ve hükümetler için de en önemli hale gelmektedir. Çalışmanın birinci bölümünde bilgi güvenliği ve kişisel verilerin korunması alanını derinlemesine inceleyerek önemini, zorluklarını ve kişisel

bilgilerin gizliliğini ve güvenliğini sağlamak için sağlam önlemlere olan zorunlu ihtiyacı ortaya koymaktadır.

Son yıllarda, dijital dönüşüm kavramı çeşitli sektörlerdeki kuruluşların dikkatini çekmiştir. Teknolojinin hızlı gelişimi ve işletmelerin işleyişi üzerindeki derin etkisi ile uyum sağlama ve yenilikçilik, dijital çağda rekabetçi kalabilmek için çok önemli hale gelmiştir. Dijital dönüşüm, süreçleri, büyük veri, yapay zekâ, veri madenciliği ve veri komisyonculuğu, blok zinciri, akıllı sistemler ve insansız ordular başlığı altında, müşteri deneyimlerini ve iş modellerini temelde yeniden şekillendirerek, dijital teknolojilerin ve stratejilerin bir organizasyonun tüm yönlerine entegrasyonunu gerektirdiği anlatılmaktadır. Dijital dönüşüm kavramını, önemini, temel itici güçlerini ve giderek daha fazla dijitalleşen bir dünyada gelişmek isteyen kuruluşlar için sahip olduğu dönüştürücü potansiyeli araştırılmaktadır.

Teknolojinin askeri operasyonların ayrılmaz bir parçası haline geldiği modern savaş alanında, elektronik harp kritik bir disiplin olarak ortaya çıkmıştır. Elektronik sistemlere ve ağlara artan güven ile askeri güçler hem kendi elektronik varlıklarını koruma hem de rakiplerinin güvenlik açıklarından yararlanma yeteneklerine sahip olmalıdır. Elektronik harp, tümü elektromanyetik spektrumda stratejik bir avantaj elde etmeyi amaçlayan elektronik karşı önlemlerden elektronik istihbarat toplamaya kadar geniş bir faaliyet yelpazesini kapsamaktadır. Çalışmada 21. Yüzyılda elektronik harbin sadece askeri alanda kalmayıp sosyal hayatın bir parçası haline gelen elektronik cihazların kullanımından elde edilen veri toplama ve analiz süreçlerini ve elektronik harp alanını inceliyor, önemini, gelişen zorlukları ve çağdaş askeri operasyonlarda oynadığı hayati rolü araştırmaktadır.

Dijital teknolojinin ortaya çıkışı çeşitli alanlarda devrim yarattı ve sosyal bilimler ve politik iletişim de bir istisna değil. 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. E-yönetişim ve e-devlet uygulamaları, dijital teknoloji, sosyal bilimler

ve politik iletişimin kesişimini araştırarak, dijital platformların ve yöntemlerin toplum, politika ve bilginin paylaşılma ve tüketilme biçimlerine ilişkin anlayışımız üzerindeki dönüştürücü etkisini vurgulamaktadır.

Çalışmanın üçüncü bölümünde yer alan elektronik harp ile gerçekleştirilen istihbarat faaliyetlerinden bahsedilmektedir. İstihbarat toplama alanında, teknik istihbarat, çeşitli aktörlerin yetenekleri, güvenlik açıkları ve niyetleri hakkında kritik bilgiler sağlamada çok önemli bir rol oynar. Teknik istihbarat, teknik sistemler, teknolojiler ve bilimsel gelişmelerle ilgili veri ve bilgilerin toplanmasını, analiz edilmesini ve yorumlanmasını içerir. Radar sistemleri, iletişim ağları, silah platformları ve ileri teknolojiler gibi teknik kaynaklardan istihbarat elde etmek için mühendislik, fizik ve bilgisayar bilimi dahil olmak üzere çok çeşitli disiplinleri kapsamaktadır. Teknik istihbarat alanı, istihbarat topluluğundaki önemini ve eyleme geçirilebilir istihbarat için teknik verileri elde etmek ve analiz etmek için kullanılan metodolojileri araştırmaktadır. İstihbarat toplama alanında, elektronik istihbarat (ELINT), çeşitli varlıkların elektronik sistemlerine ve iletişimlerine ilişkin kritik bilgiler sağlamada çok önemli bir rol oynamaktadır. Elektronik istihbarat, radar sistemleri, iletişim ağları ve diğer elektronik kaynaklar tarafından yayılan elektromanyetik sinyallerin toplanmasını, analiz edilmesini ve kullanılmasını içermektedir. Elektronik harp uygulayıcıları, bu sinyalleri yakalayıp analiz ederek, potansiyel düşmanların yetenekleri, niyetleri ve güvenlik açıkları hakkında değerli istihbarat elde edebilmektedirler. Elektronik istihbarat, modern istihbarat operasyonlarındaki önemini ve eyleme geçirilebilir istihbarat için elektromanyetik sinyalleri toplamak, işlemek ve analiz etmek için kullanılan elektronik harp uygulamalarının bir bölümüdür.

Sinyal istihbaratı (SIGINT), istihbarat toplama alanında kritik bir disiplindir ve çeşitli varlıklar tarafından bilgi iletimi ve iletişimi hakkında paha biçilmez bilgiler sağlamaktadır. Sinyal istihbaratı, radyo, radar ve diğer iletişim sinyalleri dahil olmak üzere elektronik sinyallerin toplanmasını, analiz edilmesini ve yorumlanmasını içermektedir. Sinyal istihbarat uzmanları tarafından, bu sinyalleri yakalayıp deşifre ederek potansiyel düşmanların faaliyetleri, niyetleri ve yetenekleri hakkında hayati

istihbarat toplama faaliyeti gerçekleştirilmektedirler. Elektronik harp ile gerçekleştirilen diğer bir faaliyet muhabere istihbaratı (COMINT), çeşitli varlıkların iletişimlerine ve bilgi alışverişlerine ilişkin kritik öngörüler sağlamada kritik bir rol oynamaktadır. Muhabere istihbaratı, ses, veri ve diğer elektronik iletişim biçimleri dahil olmak üzere, ele geçirilen iletişimlerin toplanmasını, analiz edilmesini ve yorumlanmasını içerir. Muhabere istihbaratı uzmanları tarafından, bu muhabereleri yakalayarak ve şifrelerini çözerek, potansiyel düşmanların faaliyetleri, amaçları ve elektronik alt yapıları hakkında değerli istihbarat bilgilerine ve modern istihbarat operasyonlarındaki önemini ve eyleme geçirilebilir istihbarat için ele geçirilen iletişimleri toplamak, analiz etmek ve kullanmak için kullanılan yöntemlerden bahsedilmektedir.

Görüntü istihbaratı (IMINT), çeşitli kaynaklardan elde edilen görsel bilgilere ve görüntülere değerli ön görüler sağlayarak, istihbarat toplama alanında, nesneler, konumlar, faaliyetler ve zaman içindeki değişikliklerle ilgili kritik bilgileri elde etmek için görüntülerin, fotoğrafların ve görsel verilerin toplanmasını, analiz edilmesini ve yorumlanmasını kapsamaktadır. İstihbarat uzmanları ile gelişmiş görüntüleme teknolojilerinden ve analitik tekniklerden yararlanarak gizli kalıpları ortaya çıkarabilir, anormallikleri tespit edebilir ve fiziksel çevre hakkında kapsamlı bir anlayış kazanılmasına olanak tanıyabilmektedir.

Sosyal medya istihbaratı (SOCMINT), istihbarat toplama faaliyetlerinde, halkın duyarlılığı, eğilimleri ve davranışları hakkında değerli bilgiler sağlayan güçlü bir araç olarak ortaya çıkmaktadır. Sosyal medya platformlarının yaygınlaşması ve kullanıcı tarafından oluşturulan içeriğin çok büyük olmasıyla birlikte sosyal medya istihbaratı, çevrimiçi toplulukların dinamiklerini anlamada ve eyleme geçirilebilir istihbarat elde etmede temel bir disiplin haline gelmiştir. Sosyal medya verilerini izleyerek, analiz ederek ve yorumlayarak bireyler, gruplar, olaylar ve ortaya çıkan tehditler hakkında değerli bilgiler elde edilebilmekte, sosyal medya istihbaratı alanını, modern istihbarat operasyonlarındaki önemini ve eyleme geçirilebilir istihbarat için sosyal medya verilerini toplamak, analiz etmek ve kullanmak için kullanılmaktadır. Siber istihbarat, istihbarat toplama alanında kritik bir bileşen haline geldi ve hızla

gelişen siber tehditler, saldırılar ve güvenlik açıkları ortamına ilişkin önemli bilgiler sağlanılmasına imkân vermektedir. 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 temel düşüncesi olan ulusal güvenliği koruma üzerindeki dönüştürücü etkisini ve elektronik harp ’in önemi çalışmanın genel anlamında ortaya çıkmaktadır.

Kişisel verilerin korunması, dijital güvenlik ve elektronik harp konusu içine giren günümüz bilgi ve iletişim araçlarının tümünü kapsayan ve bilginin korunmasını, saklanması ve paylaşım esnasındaki uygulamalara yer verilmiştir. Çalışmanın amacı, bilginin güvenli bir şekilde saklanması, iletimi ve kişisel verilerin korunmasına ilişken 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.

BİRİNCİ BÖLÜM

BİLGİ GÜVENLİĞİ VE KİŞİSEL VERİLERİN KORUNMASI

1.1. Bilgi Kavramı

Bilgi, insanların temel ihtiyaçlarını giderebilmesi ve yaşamsal faaliyetlerinin yerine getirilmesi için pazar araştırmasının yapılması olarak tanımlanabilir. Bireyin, sahip olmak istediği ürün hakkında veri toplaması bilginin oluşum aşamalarından fiziksel araştırma sürecini meydana getirmektedir. Bireylerin yaşamsal faaliyetlerini yerine getirmesi içinde bulunduğu muhitte pazar araştırması yapması, bireylerin kendileri için elverişli olan ürüne ulaşmasını sağlamaktadır[1].

Bireylerin fiziksel araştırma sürecinde elde etmiş olduğu sonuçların tümü bireye ürün hakkında bir veri sunmaktadır. Kişinin uluşmak istediği ürünün, temel özellikleri ve piyasa performans verileri bir araya getirilerek ürün hakkında daha geniş bilgi meydana gelmesine imkân tanımaktadır. İnsanların toplamış olduğu veriler, elde edinmek istenen ürün hakkında bireyin kesin bir karar vermesine değil karar sürecinin güçlendirilmesine yardımcı olmaktadır.

Bilginin meydana geliş süreçlerinde, insanların yaşamsal faaliyetleri için, kişisel çıkarlarına ve bireysel ihtiyaçlarının giderilmesinde, toplanan verilerin kullanım amaçlarına göre sıralanması ve gruplandırılması enformasyon olarak tanımlanmaktadır[2]. İnsanların bir ürün hakkında topladığı verilerin tamamı, dış ve açık kaynaktan meydana gelmektedir. Bireylerin enformasyon sürecine kadar ürün hakkında kişisel görüşleri bulunmamaktadır. İnsanların karar verme aşamasına yardımcı bu birikimlerin, verilerin tümü insanlarda objektif bir fikir oluşturmaktadır. "*Enformasyonun, bireyin ihtiyaçları doğrultusunda anlaşılması, kıyaslanması ve analiz edilmesiyle bilgi oluşur. Bilgi, enformasyonun; bireyin görüşleri, becerileri,*

---

[1] Recep Yücel, "Bir Disiplin Olarak Bilgi Yönetimi ve Eğitimi", **Bilgi Yönetimi Disiplini ve Uygulamaları,** Ed. Mustafa Sağsan, 1.Baskı, Siyasal Kitabevi, Ankara, 2010, s.16

[2] Yücel**, a.g.e.** s.17

yetenekleri, yaratıcılığı ve değerlendirilmesi doğrultusunda analiz edilme işleminden geçerek oluşur"[3].

Meydana gelen bilgi yoruma açıktır. Kişiler arasında eleştirel ve yoruma açık olması bilginin göreceli bir kavram olarak oluştuğunu göstermektedir. Bilginin oluşumunda, fiziksel araştırma süreci, bireylerin karar verme aşamaları ve bir şey hakkında tecrübe kazanmak için detaylı bir pazar araştırması yapılması gerekmektedir[4]. Araştırma neticesinde elde edilen bilginin, bir başka birey için aynı anlamı ifade etmesi söz konusu olmayabilir. Bilgi, nesnel ve göreceli veri topluluklarından oluştuğu anlaşılmaktadır.

"Bilgi, bir insan faaliyetidir, düşüncelerden geriye artan kalıntı, anlık olarak yaratılır, topluluklara, gruplara ait olup bilgi topluluklarda birçok farklı yoldan dolaşım sağlayarak yeni bilgiler ve yeni bilgiler eski bilgilerin sınırları içerisinde üretilir" olarak McDermott tarafından tanımlanmaktadır[5].

Bilgi, bireylerin kişisel özelliklerinden ortaya çıkan ve günlük yaşamda aktif olarak iletişim ortamında kullanılan veri veya veri topluluklarından meydana gelmektedir. Aynı zamanda özel işletmeler ve kurumlar hakkında her nevi döküman ve elektronik ortamda çevrimiçi ve çevrimdışı verilerin tamamını kapsayan veri yığınları olarak bilinmektedir. En temel anlamıyla bilgi, bireylerin ve kurumların, isimleri, iletişim adresleri ve açık kaynak üzerinden erişim imkânı veren veriler olarak ortaya çıkmaktadır[6].

Bilgi, bireylerin davranışlarının harekete geçmeden belirli aşamalardan geçerek bireyin karar vermesine yardımcı olan ve elde edilen verilerin işlenmesiyle, karar vermek için anlamlandırılan, kategorilere ayıran ve yoruma açık verilerin bir

---

[3] Yücel **a.g.e**. s.17

[4] Ahmet Ağır, "Bilişim Toplumuna Geçiş Sürecinde Bilgi Yönetimi Yaklaşımı", **İstanbul Üniversitesi İletişim Fakültesi Dergisi**, Cilt 0, Sayı 30, 2007, s. 4

[5] Richard McDermott, "Why Information Technology Inspired But Cannot Deliver Knowledge Management", **California Management Review**, Cilt 4, Sayı 41, 1999 s. 103

[6] Faruk Çubukçu, **Bilgi Güvenliği Yönetim Sistemi**, 1.Baskı, Pusula 20 Teknoloji ve Yayıncılık A.Ş, İstanbul, 2018, s.2

araya gelmesiyle oluşmaktadır[7]. Bazı simgelerin bir araya gelerek meydana getirmiş olduğu veri toplulukları, rasyonel bilgiyi ortaya çıkartmaktadır. Rasyonel bilgi, bireylerin, kurumların ve toplumların sürdürülebilir bir yaşam için en önemli olgu olarak ifade edilmektedir. "*Bilgi ve veri, ses, görüntü veya metin gibi herhangi bir nesne olabilir"*[8]. Bilginin oluşumunda yer alan girdiler daha anlamlı ve harekete geçmek için işlenerek rasyonel hayata çıktı olarak geçmektedir.

Bilginin yalnız bir türe özgü bir yapısı mevcut olup kullanılmaktadır. Bilginin belirli bir süreç içinde bir kıymete, kanaate, inanma ölçüsü ve güvenirlilik ile doğrudan ilişkisi vardır[9]. Veriler ve verilerin işlenerek çıktı olarak hayata geçmesi neticesinde ortaya çıkan ürüne bilgi denilmektedir. Veriler belirlenen hedefler doğrultusunda düzenlenerek bir amaç için düzenleyen birey ve kurumlara anlamlı bir ürün sunmaktadır. Kısacası bilgi, verilerin düzenlenerek bir amaç doğrultusunda işe yarar hale gelmesinden oluşmaktadır[10].

Elde edilen veya var olan işlenmemiş verilerin anlamlı bir bütün hale gelmesinden, nesnel olarak üretilen bilgiyi kontrol etmek ve yönlendirmek için organizasyonlar vasıtasıyla bilgi yönetimi gerçekleştirilmektedir. İşlenmemiş verilerin anlamlı bir bütün biçiminde sentezleyerek depolanması, kullanıcıların erişimine ve yönetilmesine bilgi yönetim süreçleri ile mümkün olmaktadır.

1.2. Bilgi Yönetimi

Bilgi yönetimi dar çerçevede ele alındığında, inceleme çerçevesinde bütün kamu birimleri, özel işletmeleri ve yönetim organizasyonlarını kapsamaktadır. Bilgi yönetiminin meydana gelişi tikelden tümele şeklinde olmuştur. Organizasyonları meydana getiren insan faktörünün bilgiye ulaşma ve bilginin paylaşımı neticesinde, bilgiyi etkin ve doğru kullanımının önemi bilgi yönetiminin gelişimine yardımcı

---

[7]Fehmi Volkan Akyön, "Bilgi Kavramı Ve Yönetimi", **Öneri Dergisi**, Cilt. 4, Sayı. 15, 2001, s.167

[8] Akyön, **a.g.e.** s.170

[9] Nezahat Güçlü ve Kseanela Sotirofski "Bilgi Yönetimi", **Türk Eğitim Bilimleri Dergisi**, Cilt.4, Sayı.4, 2006, ss.351-371

[10] Güçlü ve Sotirofski, **a.g.e.** ss.351-371

olmaktadır. Bilgi yönetimi, bilginin örgütler için verimliliğin maksimum seviyede kullanılması ve örgütlerin dış etmenlerden daha az etkilenmesi için zaruri bir ihtiyaç haline gelmektedir[11].

Bilginin oluşum aşamalarında, verilerin bir araya gelerek anlamlı bir bütün hale gelmesi ve bir amaç doğrultusunda kullanılması, çoğaltılması, etkin bir şekilde örgüt yararına kullanılması ile bilgi yönetimi ve bilgi yönetimi uygulamaları objektif bir realiteyi meydana getirmektedir[12].

Bilgi yönetimi basit bir tanımla, insanların ve örgütlerin bilgisini yönetme sürecidir. İnsanların ve örgütlerin bilgi yönetmesindeki temel amaç, sürdürülebilir bir yaşam sağlamaktır. Bilgi yönetimi, insanların yaşamlarını ve örgütlerin faaliyetlerini kolaylaştırabilmek için farkında olarak veya farkında olmadan bilgiyi kullanma ve yönetme faaliyetlerinin bir süreç olarak doğrudan kapsamaktadır[13]. Bilgi yönetimi, insan yaşamında var olan bilgiyi hayata geçirme süreci olarak nitelendirilebilir.

Bilgi yönetiminin örgütsel bir eylem olarak gerçekleştirilmesi, bilginin üretilmesi, iş birliği ile uygulanması, diğer insanlar ve örgütler ile paylaşılması, yeni bir ürün veya kavram elde etmek için kullanılan sürecin tamamını kapsamaktadır. Bilgi yönetimi uygulamalarını gerçekleştirebilmek için insanlara ve organizasyonlara ihtiyaç duyulmaktadır[14].

Araştırma ve geliştirme organizasyonlarında görev alan insanların, yeni bir ürün veya kavram elde edilmesi için gerçekleştirilen çalışmalar, yeni ürün veya kavramın pazarlanması/tanıtılması, lojistiğinin sağlanması ve açık kaynak veri tabanları üzerinden paylaşılması nihai olarak kullanıcılara ulaştırılması sürecinin, bilgi

---

[11]Mehmet Toplu, "Ekonomik Dönüşüm ve Gelişmelerin Bilgi Yönetimine Etkileri", **Bilgi Yönetimi Disiplini ve Uygulamaları,** Ed. Mustafa Sağsan, 1.Baskı, Siyasal Kitabevi, Ankara, 2010, s. 56

[12] Recep Yücel, **a.g.e**. s. 15

[13] Emir Ülger, "Epistemik Perspektiften Bilginin Kamusal Algılanışı ve Değişimi", **Bilgi Yönetimi Disiplini ve Uygulamaları,** Ed. Mustafa Sağsan, 1.Baskı, Siyasal Kitabevi, Ankara, 2010, s. 84

[14] Hakkı Okan Yeloğlu ve Senem Oğuz, "Kamu Sektöründe Örgütsel Yeniliklerin Algılanması ve Yenilik Kapasitesinin Belirlenmesine Yönelik Görgül Bir Çalışma", **Bilgi Yönetimi Disiplini ve Uygulamaları,** Ed. Mustafa Sağsan, 1.Baskı, Siyasal Kitabevi, Ankara, 2010, s. 224

yönetiminin kapsamı dahilinde gerçekleşmesi ve bilgi yönetimi uygulamalarının önemini ön plana çıkartmaktadır.

Bilgi yönetimi, işlenmemiş veri ve işlendikten sonra ortaya çıkan anlamlandırılmış olan veri kavramlarını bir bütün halde bilgi olarak ortaya çıkartmaktadır. Verilerin istatiksel olarak işlenerek, yorum, tartışma ve iletişim kanallarıyla gerçek bilgiye ulaşılabilmesi mümkün hale gelmektedir. Gerçek bilgi, birtakım sembollerin ve veri topluluklarının evrensel olarak kabul görmesiyle ortaya çıkmaktadır[15].

Bilgi yönetiminin araçları, incelenen verilerin ve bilgilerin yazılı olarak işlenmesiyle, somut belgeleri ile rasyonel hayatta kullanılmaktadır. Toplumlar, bilgi yönetim sistemleri ile yönetilmektedir. Bilgi sistemlerinin oluşumunda bilgi yönetiminin önemi ön plana çıkmaktadır. Bilgi yönetim sistemlerinde bilgi, öğrenme ve anlamlandırmak için kullanılan bir araç iken yönetim ise, belirli amaçlar doğrultusunda bireyler, toplum ve kurumların örgütsel faaliyetlerinin işlendiği süreç olarak nitelendirilmektedir[16].

"*Bilgi yönetimi, temel olarak örgüt ortamında sürekli artan bilgi kapasitesini güncelleyen, oluşan bilgileri ulaşılabilir kılan, gerekli bilgiye ulaşmak için gerekli olan işlemleri tanımlayan ve gerekli bilginin şirket çalışanlarıyla paylaşılmasını sağlayan bir disiplin"* olarak ifade edilmektedir[17].

Günümüzde üretilen bilginin, korunması için gerçekleştirilen çalışmaların yanı sıra bu bilgilerin korunması ve saklanmasının önemi artmıştır. Bilgi güvenliği bağlamında, bilgi yönetimi uygulamaları kişilerin ve kurumların temel güvenlik ihtiyaçları arasında yer almaktadır. Günümüzde bireylerin veya dış etmenlerin bilgiye ulaşmak için veya bilgi hırsızlığına yol açacak güvenlik açıklarından faydalanarak haksız bilgi üretimine ve bilgi yönetiminde telafisi mümkün olmayan hataların

---

[15]Hussain Alsaffar, "Operations and Information Management", https://www.researchgate.net/publication/346096473 , (Erişim Tarihi: 20.03.2023).

[16] Güçlü ve Sotirofski, **a.g.e.** ss.351-371

[17] Harrison R. ve Kessels J., "**Human Resource Development İn a Knowledge Economy**", s.355'den akt. Güçlü, **a.g.k.**

meydana gelmesine yol açmaktadır. Bilgi yönetiminin önemi burada anlaşılacağı üzere ön plana çıkmaktadır.

Bireylerin ve kurumların bilgi üretilmesindeki maliyetlerinden daha çok, bilginin korunması ve saklanması için gerçekleştirilen güvenlik yatırım maliyetlerini artmasına neden olmaktadır. Bilgi yönetimini meydana getiren yazılım ve donanım bileşenleri ile birlikte verinin işlenerek bilgi ve belge olması için bilgi yönetimine gereksinim duyulmaktadır[18].

İşletmelerin ve kurumların kendi içerisinde kapalı devre bilgi yönetim sistemleri, dışarıdan gelecek olan donanım veya yazılım saldırılarına karşı daha güvenli olmaktadır. Kurumların öznel elektronik bilgi yönetim sistemleri geliştirerek, bireysel işletmeler ve kamu sektöründe bilgi yönetimi ve bilgi güvenliğinde kapalı devre bilgi yönetim sistemlerinin önemi ön plana çıkmaktadır.

Kapalı devre elektronik bilgi yönetim sistemleri, işletmelerin veya kurumların imkân tanıdığı ölçüde bireylere erişim izni vermektedir. Erişim izni olmayan kurum çalışanları bu bilgilere ulaşamamakta ve kişilere bilgi yönetimde sınırlı erişim sağlayarak bilgi güvenliği sağlanmaktadır[19]. Kurum içerisinde bütün personel gerektiği kadar bilgi sahip olma prensibine göre erişim imkânı tanınarak bilginin önemi ve korunması sağlanmaktadır.

Elektronik bilgi yönetim sistemleri, kapalı devre olarak kurumlara hizmet verirken, diğer kurumlar ile bilgi alışverişi için açık kaynak sunucular ile bir bağlantı imkanına ihtiyaç duyulmaktadır. Açık kaynak bilgi yönetim sistemleri, kurumu ait belgelerin korunabilmesi ve saklanabilmesi bilgi güvenliği politikalarını ve kişisel verilerin korunması yasalarına göre zaruri bir ihtiyaç olarak görülmektedir. Kurumlar arasında gerçekleştirilen bilgi ve belge alışverişi çevrimiçi olarak açık kaynak

[18]Fahrettin Özdemirci, Cengiz Aydın, " Kurumsal Bilgi Kaynaklar ve Bilgi Yönetimi", **Türk Kütüphaneciliği Dergisi**, Cilt. 21, Sayı.2, 2007, s.167.

[19] Mehmet Kara, "**Kurumsal Bilgi Güvenliği**", 1.Baskı, Papatya Yayıncılık, İstanbul, 2018, s.41.

sunucular vasıtasıyla, kurum içi çevrimdışı bilgi alışverişi ise elektronik bilgi yönetim sistemlerinin yönettiği kurum içi kapalı devre uygulamalar ile gerçekleştirilmektedir[20].

İşletmeler ve kurumlarda üretilen, kullanılan veya saklanan her türlü bilginin güvenilir bir şekilde saklanması ve dış tehditlerden korunması için elektronik arşiv oluşturulması bilgi güvenliği maliyetlerini azaltmaktadır. Elektronik arşiv uygulamaları insan gücü olarak daha maliyetli görünse de bu uygulamaları kullanacak nitelikli personel ve her türlü elektronik tehditlere karşı güvenlik politikalarının oluşturulması bilgi yöneticileri tarafından gerçekleştirilmektedir. Elektronik arşiv yönetimi ve bilgi güvenliğinin tesis edilmesinde ihtiyaç duyulan personelin, kurumların içinde uzun zamandan beri görev yapan kişilerden olmasının önemi ortaya çıkmaktadır[21].

Elektronik bilgi yönetim sistemleri uzmanlık gerektiren ve profesyonel bir çalışma ekibiyle bilgi güvenliği bağlamında kurumların temel güvenlik personeli arasında yer almaktadır. Elektronik bilgi yönetiminde görev alan tüm birimlerin ve kurum teşkilatının kendi içerisinde birbirine entegre olması gerekliliktir.

Kurumların bilgi yönetimi sistemleri ve bilgi güvenliği maliyetlerine daha fazla kaynak ayrılmasıyla yönetilenlere ve yöneticilere elektronik bilgi yönetimi uygulamaları zaman ve güvence kazandırdığı zaman ve güven verdiği öngörülmektedir. Bilgi yönetimi uygulamaları, teknik ve yönetim çalışanlarına elektronik bilgi yönetim imkanları sunması gerekmektedir[22].

Bilgi yönetimi disiplininde, bilgi yüzeysel ve derin bilgi, teknik bilgi, uygulanabilir bilgi, bireysel ortak yoruma dayalı bilgi, açık ve örtülü bilgi şeklinde sınıflandırılabilir[23]. Bilgi yönetiminde, bilgi sınıflandırılmasından;

---

[20] Faruk Çubukçu, **a.g.e**., s. 93.

[21] Manuel Joaquim Sousa Pereira vd.; "Digital Transformation in Organizations and Its Impact on Knowledge Management" https://www.researchgate.net/publication/363847760 , (Erişim Tarihi: 13.03.2023).

[22] Özdemirci, **a.g.e.,** 2007, s.170.

[23] Güçlü ve Sotirofski, **a.g.e.** ss.351-371

Yüzeysel bilgi, sorunların ve çözümlerin minimum seviyede çözüme kavuştuğu bilgilerden oluşmakta,

Derin bilgi, bireylerin ve kurumların belirli bir zaman içerisinde kazanmış oldukları birikimler neticesinde uzmanlık gerektiren bilgilerden meydana gelmekte,

Teknik bilgi, uygulama esnasında kullanılan araç gereç ve dokümanların işleyişini, uzmanlık derecesinde ele alınan verilerin bir araya gelerek ortaya çıkarmış olduğu bilgilerden oluşmakta,

Yoruma dayalı bilgi, insanların hayat tecrübelerinden oluşan ve insanın his ve duygularının bu tecrübeler vasıtasıyla ürettiği verilerden oluşan bilgiler,

Örtülü bilginin oluşumunda, kitle iletişim araçlarının yardımlarıyla meydana gelen iletişim transferleri esnasında örtülü bilgi oluşmakta,

Açık bilginin tanımı ise metin, belge, süreli ve süresiz yayınlardan elde edilen basılı ve sözlü iletişim araçları vasıtasıyla oluşan bilgiler, olarak söz edilmektedir[24]. Bilginin interaktif olarak çalışmasını, yönetilmesini ve netice alınması sürecinde bilgi yönetiminin önemi anlaşılmaktadır. Verinin işlenerek belirlenen amaç doğrultusunda çalışanlardan alınan geri dönüşler ile aktif bilgi yönetimi gerçekleştirilmektedir.

Bilgi yönetiminin amacı, iş bölümlerinin, personelin ve ihtiyaç duyulan teknolojik araç gereçlerin, kurumların işleyişi ile entegrasyonu sağlamaktır. Elde edilen bilginin, çalışanlar ve muhataplarına ulaşabilmesi için bilginin paylaşılması ve sonuç alınması gerekmektedir. Alınan sonuçların değerlendirilmesi, kurumların eksiklikleri, hata tespiti ve güvenlik zafiyetlerinin ortaya çıkarılmasına olanak tanımaktadır.

[24] Awad E. ve Ghaziri H., "**Knowledge Management**", s. 45'ten akt. Güçlü, **a.g.k.**

1.3. Bilgi Yönetiminin Önemi

21.yüzyılda örgütler, bilginin önemini, bilgi ile sağlanacak faydanın önemini bilgi yönetimi uygulamalarının örgüt kültüründe bulunmasının gerekliliği ön plana çıkmaktadır. Bilginin önemi, insanların bilgiye erişimi, veri tabanları ve bilgi ve iletişim teknolojileri vasıtaları aracılığı ile bilginin aktif ve doğru kullanımının farkındalığı artmaktadır[25]. Ancak teknoloji çağında, erişim kolaylığından kaynaklanan, gereksiz ve yanlış bilgilerin serbest dolaşımı bilgi kirliliğinin oluşmasına ve doğru bilgiye erişmenin güçlüğünün ortaya çıkması dezavantaj olarak görülmektedir.

Bilgi yönetimi uygulamaları organizasyonlarda;

- Teknoloji çağında daha fazla rekabet ortamının oluşmasına,
- Yeniliklerin hızının artmasına ve inovasyona açık olunması,
- Örgütlerin değer yaratma konusunda yarışına,
- Nitelikli insan sayısının gün geçtikçe azalması sebebiyle tecrübe ve zaman yerini teknolojilere bırakıyor olması ve teknoloji yönetiminde ihtiyaç duyulması,

bilginin ademi merkeziyetçi bir model ile yönetilmesi için bilgi yönetimi uygulamalarına ihtiyaç duyulmaktadır[26].

Bilgi yönetimi uygulamaları sürecinde, net ve belirgin bilgi üzerinden yorum yapmak objektif bir bilgi yönetimi organizasyonu olarak nitelendirilmeyecektir. Açık ve örtülü bilginin, bilgi yönetimi sürecinde eldeki mevcut belgeler üzerinden oluşması ve bireysel tecrübeler ile bilgi yönetimi sürecinin ortaya çıktığı görülmektedir.

Bilgi yönetimi uygulamaları, kamu kurumları ve özel işletmelerde bilginin paylaşımı kapalı devre iletişim ortamları ile meydana gelmektedir. Kurumların bilgi

---

[25]H.Agus Maulana, "Model SECI Knowledge Management", https://www.researchgate.net/publication/352559412 , (Erişim Tarihi: 13.03.2023).

[26]Min Yang, "Information Security Risk Management Model for Big Data), https://www.hindawi.com/journals/am/2022/3383251 , (Erişim Tarihi: 10.03.2023)

güvenliği bakımından, bilginin iletimi sırasında meydana gelebilecek risklerin en aza indirgenmesi, kapalı devre iletim ortamlarının oluşturulması ile sağlanmaktadır. Bilginin iletim esnasında şifrelenmesi ve veri iletim yollarının dışarıdan gelebilecek tehditlere mahal vermemesi için bilgi yönetimi uygulamaları ve bilgi güvenliğinin önemi ön plana çıkmaktadır[27]. Bilgi güvenliğinin sağlanabilmesi için, bilgi yönetimi uygulamalarına yer verilmesi zaruri bir ihtiyaç olarak görülmektedir. Bilgi yönetimi uygulamaları, örgütlerin içerisinde, bilginin özümsenmesi ve kurumsal nitelik bakımından örgütlerin güvenlik açıklıklarının ortadan kaldırılmasına yardımcı olmaktadır.

Bilgi kamu kurumları ve organizasyonların dinamik gelişimini sağlayan bir olgudur. Bilginin etkin bir şekilde kullanımı için bilgi yönetimi uygulamalarına ihtiyaç duyulmaktadır. Bilgi yönetimi uygulamaları, bilgiyi geliştirmek, korumak, etkin kullanmak ve paylaşımına imkân tanıyan bir süreç olarak değerlendirilmektedir[28]. Bilgi yönetimi uygulamalarının amacı, ulaşılmak istenen bilgi ve tüm yönetim süreçlerinin tespitinin yapılması ve bilginin doğru bir şekilde analiz edilmesidir.

Bilgi yönetimi sürecinde, bilginin sosyal çevrelerde kitle iletişim araçları veya bireysel iletişim kanalları kullanılarak sosyalleşme sağlanabilmektedir. Elde edilen bilginin genişletilmesi veya daha kapsamlı bir anlam ifade etmesi için açık kaynak bilgilerden faydalanılması var olan bilginin güncellemiş ve daha aktif kullanılabilir hale gelmesine olanak tanımaktadır[29].

Bilgi, sosyal çevre harici kaynaklar ile bir bütün haline geldiği zaman, elde edilen yeni bilgi kurum ve organizasyonların hedefleri doğrultusunda benimsenerek maksimum fayda sağlayacak duruma gelmektedir. Kurum veya organizasyonların

---

[27] K. Ali Akkemik, "Bilgi Ekonomileri ve Ekonomik Kalkınma: Bir İktisadi Model Yardımıyla Çeşitli Senaryoların Sonuçları", **Bilgi Yönetimi Disiplini ve Uygulamaları,** Ed. Mustafa Sağsan, 1.Baskı, Siyasal Kitabevi, Ankara, 2010, ss. 122-141

[28]Mert Akal, "Bilişim Firmalarında Bilgi Güvenliği Farkındalığı", **Yüksek Lisans Tezi**, Ufuk Üniversitesi, Ankara, 2022, s. 24

[29]Sadi Evren Seker, "Bilgi Yönetimi", **YBS Ansiklopedi**, Cilt.1, Sayı.2, 2014 ss.10-17

uygulama sürecinin yerine getirilmesi, bilginin anlamlı bir bütün ve geliştirilebilir olduğunun göstergelerinden bir tanesidir.

Bireysel ve örgütsel tecrübelerin bilgi yönetimine sağlayacağı fayda SECI yönetim modeli olarak ifade edilmektedir[30]. Bilgi, soyut bir kavram olarak bireylerin zihinlerinde oluşmadan önce, önceden meydana gelmiş olan açık kaynak bilgilere ulaşarak insan beyninde bilgi birikimi olarak kalmaktadır. Bilginin bireyler tarafından işlenerek rasyonel hayatta rol almasıyla, örgütler ve organizasyonlar tarafından işlenerek somut bir olgu, iş ve tecrübe elde edilmektedir[31].

Bilginin yazılı ortamlarda veya dijital ortamlar vasıtası ile paylaşılması daha anlamlı ve işlene bilirliği aktif yeni bilgi üretimine olanak tanımaktadır. Örtülü bilgi bireylerin harekete geçmeden önce soyut olarak geliştirilen ve işlenen verilerden oluşmaktadır. Açık bilgi ise örtülü bilginin rasyonel hayatta kullanıcılara bir eylem ve kavram bütünü olarak kullanılmasına imkân vermektedir. Örgütler, bilgiyi kullanarak içinde bulundukları örgütlere bir kazanım sağlamakta, dış faktörler olan örgüt dışı iletişim ve paylaşımı arttırarak ve her türlü bilgiden fayda sağlamayı amaç edinmektedir[32].

Bilgi yönetimi, açık bilgi ve örtülü bilginin organizasyonların amaçları doğrultusunda bilgiyi işleyerek kullanılması veya olduğu gibi var olan bilgiyi yönetme sürecidir. Bilgi yönetimi, organizasyonların amaçları doğrultusunda, bilginin yanı sıra personel ve örgüt yönetiminin kapsamında bulunmasından dolayı organizasyon içinde bilgi yönetimi önemi göz ardı edilmemelidir. Bilgi yönetimi, bilginin depolanması, saklanması ve gerektiğinde kullanıma sunması gibi eylemleri gerçekleştirmektedir.

İnsanların ve organizasyonların belirli bir yönetim sistemi içerisinde, bilgi üretmeyi organize bir şekilde gerçekleştirmesi bilgi yönetimi disiplinini meydana getirmektedir. Bilgi yönetimi sürecini oluşturan temel etmenler, bilgiyi; üretmek,

---

[30] Seker, **a.g.e.,** ss.10-17

[31] Malik Yılmaz, "Enformasyon ve Bilgi Kavramları Bağlamında Enformasyon Yönetimi Ve Bilgi Yönetimi", **Ankara Üniversitesi Dil ve Tarih – Coğrafya Fakültesi Dergisi,** Cilt.49, Sayı.1, 2009, s.108

[32] Yılmaz, **a.g.e.,** 2009, s.112

paylaşmak ve pratik yaşamın bir parçası haline getirerek yönetmekten geçmektedir[33]. Ayrıca bilgi yönetiminin yardımcı bileşenleri olan örgüt kültürü, zaman ve ihtiyaç duyulan alt yapının sağlanması ile bilgi yönetimi uygulamaları kurumların ve yönetim faaliyetlerinin bir parçası olmaktadır.

Bilgi yönetiminin temel öğelerinden birisi olan kullanıcıların erişimi ve bilginin paylaşılması ile verimli ve etkin kullanılmasıdır. Paylaşılan bilgi, farklı görüşlerin ortaya çıkması ve etkileşimi ile yeni bir ürün veya kavramın meydana gelmesine imkân tanımaktadır.

Bilginin paylaşılmadığı organizasyonların gelişimi daha yavaş ve rekabetten uzak kalmaktadır. Bilgi yönetimini oluşturan bileşenlerin ve yardımcı bileşenlerin bir arada olması ile ancak yeni bir ürün ya da kavram yaratılması mümkün hale gelmektedir[34].

İnsanların faydalı bir şekilde ürün veya bilgi üretmeleri için organizasyon kültürünün oluşması gerekmektedir. Organizasyon/kurum kültürü, yeni bilginin meydana gelişinde motivasyon ve disipline yer verilmesi elde edilecek olan yeni bilgiye pozitif katkı sağlaması ve bilgi yönetimi sürecinde zamanın etkin kullanılmasını sağlamaktadır[35].

Bilgi yönetimi sürecinde, kurumların ya da organizasyonların doğru bir kurum kültürüne ve disipline sahip olmaları gerekmektedir. Kurum veya örgüt kültürü oluşturulmadan bilgi yönetimi sürecinin işlemesi zor ve telafisi mümkün olmayan hataların yapılmasına olanak tanıması değerlendirilmektedir.

Bilgi yönetimi insanlara ve örgütlere, geçmişte yapılan hataların tekrarlanmamasına imkân tanımaktadır. Bilgi yönetimi süreci, insanların bilgi

---

[33] Jamal Abdulsalam Mohamed Elattresh, "Bilgi Güvenliği Hizmet Yönetimi: Bilgi Güvenliği Yönetimine Bir Hizmet Yönetimi Yaklaşımı ve Bir Kurumun Müşterilerinin Memnuniyeti ve Güvenirliği Üzerindeki Etkisi", **Doktora Tezi**, Kastamonu Üniversitesi, Kastamonu, 2022, s. 38

[34] Zeynep Akdoğan, "Kamu Kurumlarında Bilgi Güvenliği Yönetim Sistemleri Politika Geliştirme Metodolojisi", **Doktora Tezi**, Ankara Üniversitesi, Ankara, 2022, s. 99

[35] Ömer Şaban Fidancı, "Kurumlar İçin Bilgi Güvenliği Yönetim Sisteminin Oluşturulması", **Yüksek Lisans Tezi**, KTO Karatay Üniversitesi, Konya, 2022, s. 16

paylaşımı ve tecrübeleri, farklı organizasyonların geçmişte yapmış oldukları hataları göz önüne alarak yeni bir bilgi veya ürün üretiminde hataların minimum seviyede olması bilgi yöneticilerinin değerlendirmeleri neticesinde gerçekleştirilmektedir[36].

Bilgi yönetimi uygulamaları, farklı alanlarda çalışan insanların tecrübelerini bir araya getirmek suretiyle objektif bir bakış açısı ve farklı görüşlerin bilgi yöneticileri tarafından derlenmesi sonucu ortaya çıkmaktadır. Bilgi yönetimi sürecinde, karar verici konumunda bulunan yöneticilerin, diğer çalışanlara örgütlerin bilgi ve tecrübelerin aktarılmasına olanak tanınmaktadır.

Bilgi yönetimi uygulamaları, eldeki mevcut bilgilerin işlenmesi yöneticiler tarafından kurum veya örgüte entegre edilecek olan bilgi hakkında hazırlık ve eğitim planların yapılması ile kurum içi oryantasyonun tamamlanmasını sağlamaktadır.

Yeni bilginin uygulanmasında, kullanıcılar tarafından yeni ürün veya bilgi hakkında soruların hazırlanması, örgütlerin farklı birimlerinden üst düzey yöneticiler ve çalışanların görüşlerinin toplanması ve farklı bakış açılarına sahip örgüt dışı araştırmalara yer verilmesi gerekmektedir[37]. Kurum veya örgütlerin yukarıdaki yönetim yaklaşımını belirlemeleri ile bilgi yönetimi hakkında genel çerçevenin oluşması kurumlarda bir örgüt kültürünün benimsenmesine olanak tanınmaktadır.

Bilgi yönetiminin odağında, planlı uygulamalar ile bilginin yönetilmesi ve korunması bulunmaktadır. Bilgi yönetimi kurum ve organizasyonlara, günümüzde artan bilgi kirliliği ve önemli veya önemsiz tüm bilgilerin sentezlenerek örgütlerin amaçları doğrultusunda kullanılması gerektiğini vurgulamaktadır.

Teknoloji çağında bilginin bireysel ve kurumsal olarak bilgi yönetimi uygulamalarına yer vermek rekabet olgusunun gelişmesine ve verimli bilgi kullanımına imkânı sunmaktadır. Örgütlerin karar aşamalarında, eldeki mevcut bilgilerle yöneticilerin karar sürecini hızlı ve güvenilir olmasına avantaj

---

[36] Kemal Karakoçak, "Bilgi Üretiminin Verimliliğe Etkisi: TBMM Örneği", **Bilgi Yönetimi Disiplini ve Uygulamaları,** Ed. Mustafa Sağsan, 1.Baskı, Siyasal Kitabevi, Ankara, 2010, s. 163

[37] Kemal Karakoçak, **a.g.e.**, s.165

sağlamaktadır. Güçlü bir enstrüman olan bilginin doğru kullanımı, kurum ve örgütlerin amaçları doğrultusunda yönetim faaliyetleri ve bilgi güvenliğinin sağlanması, kurumların ve bireylerin daha geniş bir perspektif ile geleceğini yönlendirmesine olanak tanımaktadır.

Bilgi yönetimi uygulamalarında erişilebilirlik, kalite, tutarlılık, birleştirici olma gibi prensiplere yer verilmesi gerekmektedir. Bilgi yönetimi, stratejik iş amaçlarının kurumsal çerçeve ile bilgi yönetimi prensiplerine uyumun ve bilgi paylaşımının güvenli hale getirilmesi, bilgi yönetimine bağlılık temel işlevsel alan olarak kabul edilmektedir[38]. Bilgi yönetimi, örgütlerde ve insanlar arasında işlevsel olarak rekabetin sonucu olarak meydana gelmektedir.

Bilgi yönetimi sürecini iyi yönetmiş bir organizasyon rakiplerinden avantajlı bir konumda bulunacaktır. Günümüzde fiziksel güç ve fiziksel uğraşlar yerini bilginin gücüne bırakmıştır. Bilginin doğru kullanımı örgütlere ve bireylere rekabet ortamında bilgi yönetimi uygulamalarını kullanan birey ve örgütlerin başarılarının arttığı görülmektedir.

Bilgi çağında bilgi, insanlara ve organizasyonlara stratejik üstünlük sağlayan bir kaynaktır. Bilginin etkin kullanımı sağlanmadığı taktirde insanlara ve örgütlere fayda sağlaması beklenmemektedir. Bilgi yönetiminin önemi bilginin doğru ve etkin kullanımı ile ortaya çıkmaktadır[39].

Bilgi yönetimi aynı zamanda, bilginin korunması, dış saldırılara karşı bilgi güvenliği önlemlerini alması, her türlü saldırılara ve tehditlere bilgi güvenliği politikaların uygulanmasından sorumlu olmaktadır. Bilgi güvenliği, bilginin üçüncü kişilerin eline geçmemesi için alınan birtakım önlemler olarak değerlendirilmektedir.

---

[38] Roberto Prieto, "Knowledge Management", https://www.researchgate.net/publication/363541812 , (Erişim Tarihi: 30.03.2023).

[39]Julie J.C.H. Ryan, "Political Engineering in Knowledge Security", **VINE**, Cilt.36, Sayı.3, 2006, ss.265-266

1.4. Bilgi Güvenliği

Bilgi güvenliği, verilerin ve üretilen bilgilerin dijital ortamlarda korunması, bilginin doğrudan iletiminde, iletim yollarının yazılım uygulamaları vasıtasıyla saldırılara karşı güvenli bir şekilde iletilmesi ve bilgi depolandığı ortamlarda farklı kullanıcılara erişime engellenmesi maksadıyla gerçekleştirilen faaliyetleri kapsamaktadır[40].

Elektronik ortamda yer alan verilerin dışarıdan gelecek saldırılara karşı, silinmesi, değiştirilmesi ve izinsiz erişim ile üçüncü taraf kişiler tarafından elde edilmemesi için güvenlik protokolleri ve politikalarına yer verilmektedir. "*Bilgi güvenliği, bilginin varlık olarak hasarlardan korunması, doğru teknolojinin, doğru amaçlar ve doğru şekilde kullanılarak bilginin her türlü ortamda, istenmeyen kişiler tarafından elde edilmesini önleme şeklinde tanımlanabilmektedir*"[41].

Bilginin saklandığı harici bellek, dahili ve taşınabilir belleklere karşı uygulanan fiziki olmayan birtakım yazılımlar tarafından saldırılar gerçekleştirilmektedir. Bilgi güvenliğinin gerçekleştirilmesi ve verinin güvenilir bir şekilde saklanması için, bilginin gizlilik ve bütünlük içinde korunması, doğru zamanda kullanımı için erişilebilir olması gerekmektedir.

Gizlilik, istenmeyen kişiler tarafından bilgilerin erişimine engel olmak, bilginin amacı dışında kullanılmasına olanak tanıyarak oluşabilecek zararları minimize etmeyi bilgi güvenliği ile hedeflenmektedir. Bilginin açık kaynak dolaşımlarda izinsiz olarak paylaşımı, internet bağlantılarına uygulanan birtakım saldırılar ile bilgi güvenliğini ve gizliliğini zayıflatarak bilgi güvenliğinin önemi ortaya çıkmaktadır[42].

İstemeyen kişiler ve kullanıcı seviyesindeki personel, bilgi depolarının farkında olarak veya farkında olmadan, bilgiler üzerinde yeni işlem gerçekleştirilerek

---

[40] Gürol Canbek ve Şeref Sağıroğlu, "Bilgi, Bilgi Güvenliği ve Süreçleri Üzerine Bir İnceleme", **Politeknik Dergisi,** Cilt.9, Sayı.3, 2006, s.167

[41] Canbek ve Sağıroğlu, **a.g.e.,** s.169

[42] Mehmet Kara, **a.g.e.** s.15

bilginin öz kaynağına zarar vermesinin bütünlük kavramıyla bu gibi eylemlerin önüne geçilebileceği öngörülmektedir. Bilgi güvenliği sisteminin işlene bilirliği için, erişimin kullanıcılar tarafından bilgi ve veri kaybına veya zarar verilmek istenebilir personelin bilgi güvenliği hakkında bilgilendirilmesi gerekmektedir. Personele her zaman emniyetli ve gizlilik şartlarının yerine getirilmesi ile erişim ve kullanım imkânı sunulmalıdır[43].

Bilginin yönetiminde kullanıcılar ile üçüncü taraf kişiler arasında gerçekleştirilmesi gereken gizlilik sözleşmelerine yer verilmesi bilgi güvenliği açısından önem arz etmektedir. İşletmeler ve kurumların bünyelerinde oluşan örgüt kültürü ile insanlar üzerindeki sorumlulukların farkında olmaları sağlanarak, bilgi güvenliğinin üst düzey seviyelerde kalması öngörülmektedir[44].

Bilgi güvenliğinin sağlanabilmesi için gerek duyulan gizlilik, bütünlük ve erişebilirlik prensiplerine yer verilmesi gerekmektedir. Bilgi güvenliği prensiplerini meydana getiren kimlik tespiti ve doğrulama, emniyetli bir sistem kurulumu ve güvenilirlik, kullanıcılar arasında bilgiye zarar veren uygulamalara engel olunması, bilginin ve verinin yanı sıra sistem mahremiyetine önem verilmesi gerekmektedir[45].

Bilgi ve iletişim teknolojilerinin son zamanlardaki hızlı gelişimi, aynı zamanda bilginin korunması için birtakım açıklıkların da meydana gelmesine olanak tanımaktadır. Bilgi sistemlerinin korunması ve bilginin her türlü saldırı ve tehditlere karşı korunması için, bilgi güvenliği sistem risk faktörleri göz önünde bulundurarak, güvenilir bir bilgi depolama ve paylaşım ortamı oluşturulmalıdır.

Bilginin varlık değerinde, bir kayıp meydana gelmesinin önlenmesinde risk değerleme faktörleri ön plana çıkmaktadır. Bilginin en iyi şekilde korunması ve saklanmasında kurumların veya şirketlerin eldeki bilgiyi en doğru şekilde kullanarak

---

[43] Kara, **a.g.e**., s.16

[44] Çubukçu **a.g.e.** , s.3

[45]Mehmet Tekerek, "Bilgi Güvenilği Yönetimi", **KSÜ Doğa Bilimleri Dergisi**, Cilt.11, Sayı.1, 2008, s.136

maksimum fayda sağlamakta ve bilginin güvenli bir şekilde depolanarak korunması zaruri bir güvenlik önlemi haline gelmektedir[46].

Risk değerlendirilmesi, var olan bütün bilginin detaylı dökümleri, gizlilik seviyesine göre önemliden en önemsize bir derecelendirme yapılarak, tehdit unsuru oluşturabilecek risklerin değerlendirmeleri ile birlikte mevcut bilginin durumu belirlenir[47]. Risk değerlendirilmesine göre meydana gelebilecek olumsuzlukların önüne geçilebilmesi için yöneticilerin öncelik sırasına göre risk yönetimi kararları oluşturulur. Risk yönetimi kararlarının oluşturulmasındaki amaç, risk tanımını yapılması, alınması gereken önlemlerin ne olduğunun bilinmesi ve risk analiz raporunun oluşturulmasıdır[48].

Risk yönetiminde, örgütlerin riski minimum seviyede tutarak bilgi güvenliğini sağlamak ve bilgi ile maksimum fayda sağlanması amaçlanmaktadır. Risk yönetimi planlama aşamasında, "*korumaların maliyet etkinlik analizini içeren risk analizinin yapılması, korumaların gerçekleşmesi, yeniden gözden geçirilmesi ve sürdürülmesi*" şeklinde planlaması gerekmektedir[49].

Bilgiye karşı meydana gelebilecek tehditlerin önlenmesi, kurumların ve organizasyonların olası meydana gelebilecek hataları en alt seviye tutmaları ve bilgi güvenliği yöneticilerine, personel ve alt yapıya önem verilmesinden geçmektedir. Organizasyonlarda yer alan basit kullanıcı seviyelerinden, güvenlik ve risk yönetim sürecindeki personellerde dahil, görev ve sorumluklarının dışında kalan erişimlerin kısıtlanması gerekmektedir[50].

---

[46] Mehtap Çetinkaya, "Kurumlarda Bilgi Güvenliği Yönetim Sisteminin Uygulanması", https://ab.org.tr/ab08/kitap/Bildiriler/MCetinkaya_AB08.pdf , (Erişim Tarihi: 27.03.2023).

[47] Çetinkaya **a.g.k.**

[48] Çetinkaya **a.g.k.**

[49] Kara **a.g.e.** s.26

[50] Mete Eminağaoğlu ve Yılmaz Gökşen, "Bilgi Güvenliği Nedir, Ne Değildir, Türkiye'de Bilgi Güvenliği Sorunları ve Çözüm Önerileri**", Dokuz Eylül Üniversitesi Sosyal Bilimler Enstitüsü Dergisi**, Cilt.11, Sayı.4, 2009, ss. 1-15

Bilgi güvenliğinin eksiksiz olarak sağlanabilmesi için, gizlilik, bütünlük, erişilebilirlik, kimlik doğrulama ve inkâr edememe prensiplerinin uygulanması gerekmektedir.

1.4.1 Gizlilik

Gizlilik, bilginin erişim sağlayıcıları ve bilgi yönetimi yöneticileri haricinde kalan yetkisiz erişimlerden korunmasıdır. Gizlilik ilkesinde temel amaç, verilerin erişim izini olmayan üçüncü taraf kişilerin eline geçmesini engellemektir. Bilgi güvenliği prensipleri birbirlerinden bağımsız gibi ilkeler olarak görünse de her bir prensip bir bütün olarak bilgi güvenliği kavramını meydana getirmektedir[51]. Gizlilik prensiplerinde oluşabilecek aksaklıklarından doğrudan bilgi güvenliği uygulamaları etkilenmemesi mümkün değildir.

Bilginin niteliğinin anlaşılması, kişilere ve kurumlara göre önem derecesi fark etmeksizin her türlü bilgi, rekabet ortamında ve karşıt bir organizasyonun eylemlerine yöne vermesine olanak sağlanmaması gizlilik prensibinin doğru bir şekilde uygulanması ile mümkün hale gelmektedir. Bilgi güvenliğinde gizlilik prensibinin göz ardı edilmesi, hangi çalışma alanında olursa olsun bilginin yetkisiz kişiler tarafından erişimine imkân tanıyacak ve bilgi güvenliğinde açık verilmesine neden olacaktır[52].

Gizlilik prensibinin hedefi, bilginin erişim izini olmayan kişiler tarafından ele geçirilmesini önlemek ve bilginin orijinalliğinin korunmasıdır. Bilginin her türlü ortamda saklanması, korunması ve paylaşılması sırasında yetkisiz kişilerin eline geçmesini engellemek, gizlilik prensibinin uygulanmasının önemini ortaya çıkartmaktadır. Kamu kurumlarında ve diğer organizasyonlarda görev alan insanların,

---

[51] M. Yu. Zakharov vd., "Sociology of Knowledge Security in the Digital Educational", **Vestnik Universiteta Journal**, Cilt.1, Sayı.3, 2020, ss.154-159

[52] Amjad Mahfuth, "Security Knowledge Required to Improve Employee Security Behavior in Information Security Culture", **International Journal of Comuputer Science and Information Security**, Marc 2022, ss. 1-10

gizlilik politikaları hakkında bilgilendirilmesi ve eğitimler planlanması bilgi güvenliğinin yüksek seviyelerde kalmasını sağlayacaktır[53].

1.4.2. Bütünlük

Bütünlük ilkesi, bilginin özünde değişim yapılmadan korunmasıdır. Bilginin, erişim izini olmayan kişiler tarafından bilgiye ulaşılmasını engelleme, meydana gelebilecek olası tehditlerden korunması bütünlük ilkesini meydana getirmektedir[54]. Kullanıcıların etkin olarak bilgiyi kullanabilmeleri için bütünlük ilkesine yer verilmektedir.

Bilginin hatasız ve eksiksiz olarak korunması, bilgi yöneticileri tarafından kullanıcıların bütünlük ilkesini yerine getirmeleri ile sağlanmaktadır. Bilgi içeriğinin değiştirilmeden orijinal hali ile kullanılması ve olası tehditlerden korunması bütünlük ilkesinin benimsenmesi ile mümkün olacaktır.

Bütünlük prensibi, olası tehditlerin tanımlanması, tehditlere karşı alınacak tedbirlerin tespit edilmesi neticesinde örgütlerin ve bireylerin bilgiyi verimli bir şekilde yararlanmasını amaçlamaktadır. Kamu kurumları ve diğer organizasyonlarda bilgi güvenliğinin sağlanabilmesi için maksimum gizlilik ve bilgiye zarar verecek tehditlere olanak tanımadan korunması ve risk faktörlerini dikkate alarak bütünlük prensibi uygulanması gerekmektedir[55].

Bütünlük ilkesi ile yetkisiz kişilerin bilgiye ulaşmasını, bilginin dezenformasyona uğramasını ve değiştirilmesine engel olmaktadır. Aynı zamanda bilginin depolandığı fiziksel ortamlarının hassasiyetle korunması gerekmektedir. Bütün prensibinin amacı, bilginin saklandığı fiziksel ortamın güvenlik tedbirleri ve yetkisiz kullanıcıların depolama ortamlarına erişim imkânı vermemek, bilginin

---

[53] Susanne Krasmann, " On The Boundaries of Knowledge: Security, the Sensible and the Law", https://www.researchgate.net/publication/293827664 , (Erişim Tarihi:30.03.2023).

[54] M. Yu Zakharov vd., **a.g.e.** ss.154-159

[55] Mahfuth, **a.g.e.,** ss. 1-10

kopyalanması, taşınması, değiştirilmesi ve olası tüm tehditlerden korunmasıdır[56]. Bilginin amacı dışında kullanılması, silinmesi ve değiştirilmesini engellemek, bilginin orijinalliğinin korunması bütünlük ilkesini meydana getirmektedir.

1.4.3. Erişilebilirlik

Erişilebilirlik, bilginin erişimine izin verilen kişiler tarafından veya bilginin kullanım amacına ve zamanına göre kullanılmasını sağlamaktır. Kullanıcıların yetkilerine göre erişim imkanını sunmak ve yetkisiz kişilerin bilgiye ulaşmasına engel olmak erişilebilirlik ilkesi ile mümkün olmaktadır.

Erişilebilirlik ilkesi ile bilgi güvenliği yöneticileri tarafından, kullanıcı seviyelerinin tespit edilmesi, erişim zamanının belirlenmesi ile bilginin değiştirilmesini veya muhtemel tehditlerin önüne geçilmesi amaçlanmaktadır[57]. Erişilebilirlik prensibi ile bilginin saklandığı ortamların fiziksel güvenliğinin sağlanması, insanların bilgi güvenliği farkındalıklarının arttırılması ve bilmesi gerekenler prensibinin oluşturulması hedeflenmektedir.

Bilginin doğru zamanda ve yetkili kişiler tarafından kullanılmasını sağlamak erişilebilirlik prensibini meydana getirmektedir. Önem ve gizlilik derecesine göre herkes tarafından erişmemesi gereken bilgiler, yetkilendirme ile erişim imkânı verilerek bilginin zarar görmesine engel olunmaktadır[58]. Erişilebilirlik ilkesi kısaca, ihtiyaç duyulduğu zaman ve sadece ihtiyaç duyulan bilginin yetkilendirilen kişiler tarafından kullanılmasıdır.

1.4.4. Kimlik Doğrulama

Kimlik doğrulama, bilgiyi kullanacak olan kişinin, kimlik bilgilerinin alınması ve bilgiye erişen kişinin kim olduğunun tespit edilmesi veya açıklanması işlemlerini kapsamaktadır. Kamu kurumlarının veya diğer organizasyonların, çalışanlarına

---

[56] Susanne Krasmann, **a.g.k.**

[57] Susanne Krasmann, **a.g.k.**

[58] M. Yu Zakharov vd., **a.g.e.** ss.154-159

tanımlamış olduğu, kurum kimlik numarası, personel sicil numarası veya kurum içi kullanıcı isimlerinin oluşturulmasıdır[59]. Kullanıcı bilgilerinin, kimlik doğrulama ve erişim izinlerinin oluşturulması, bilgi güvenliğinde bilginin değiştirilmesi ve muhtemel tehditlerin ortadan kaldırılmasına yardımcı olmaktadır.

Kimlik doğrulama aynı zamanda kaybolan, değiştirilen kısacası bilginin zarar görmesini engelleyen bir bilgi güvenliği prensibidir. Kurum çalışanları üzerinde sorumluluk ve disiplinin sağlanması, hesap verilebilirliğin şeffaf bir şekilde uygulanması kimlik doğrulamanın gerçekleştirilmesi ile mümkündür. Kimlik doğrulama ile bilgi güvenliğinin en iyi seviyede kalması, yetkilendirme işlemlerinde kolaylık, erişim kısıtlamalarında zamandan kazanç ve erişim kolaylığı sağlanmaktadır[60].

Kimlik doğrulama ilkesi insanların bilgiye erişim zamanını ve meydana gelebilecek olası veri kayıplarının hangi kullanıcı tarafından yapıldığının tespit edilmesine olanak tanımaktadır. Kimlik doğrulama ile kullanıcı profillerinin oluşturulması, kullanıcıların sisteme veya kurumlara girişi çıkış işlemlerinin kontrol edilmesi bilgi güvenliğinin sağlanmasına imkân tanıyan bir kavramdır.

Kimlik doğrulama uygulamaları; manyetik personel kartlarının, ziyaretçi kartları, parmak izi ve biyolojik kimliklerin tanımlanması, kullanıcı isimleri ve parolaların oluşturulmasıdır[61].

1.4.5. İnkâr Edememe

Bilgini paylaşımı esnasında, bilgiyi gönderen ve alıcı arasında meydana gelebilecek problemlerin en aza indirgenmesidir. İnkâr edememe, kullanıcılar arasındaki iletişim sorunlarının ortadan kaldırılmasına ve oluşan problemlerin hızlı bir

[59] Mahfuth, **a.g.e.,** ss. 1-10

[60] **a.g.e.,** ss. 1-10

[61] M. Yu Zakharov vd., **a.g.e.** ss.154-159

şekilde çözümüne olanak tanımaktadır[62]. Kullanıcılar arasındaki anlaşmazlıkların giderilmesine ve anlaşmazlıklara yer verilmemesi hedeflenmektedir.

Bilgi güvenliği prensiplerinden inkâr edememe, kullanıcıların sorunları görmezden gelmesine imkân vermemektedir. Aynı zamanda, bilginin değiştirilmesi, silinmesi, kısman ya da tamamen zarar görmesi ve yetkisiz kişilerin erişimlerine olanak vermemektedir.

İnkâr edememe özetle, bilginin iletimi esnasında meydana gelebilecek anlaşmazlıkların, bilgiyi gönderen ile alıcı arasındaki problemlerin ortadan kaldırılması ile bilgi güvenliğinin sağlanmasına yardımcı olmaktadır[63]. Bilgi güvenliğinin eksiksiz olarak yerine getirilmesi, yukarıda açıklanan prensiplerin tümünün aynı anda uygulanması ile mümkün olmaktadır.

1.5. Bilgi Güvenliği Yönetim Sistemi (BGYS)

Kamu kurumları ve organizasyonlarda, bilgi güvenliğinin sağlanabilmesi için mevcut bilgilerin ayrıştırılması ve bilgi haritası hazırlığı yapılması gerekmektedir. Bilgi güvenliği yönetim sistemi, bilgi varlıklarının tespit edilmesi, örgüt içi iş kollarının ve faaliyet alanlarının yönetim süreçlerinin desteklenmesi, ihtiyaç halinde bilgiye erişim kolaylığı sağlanabilmesi için bilgi haritasının oluşturulması ve bilgi güvenliğinin eksiksiz olarak işlemesine olanak tanımaktadır[64].

Kamu kurumlarının ve diğer organizasyonların bilgi güvenliği yönetim sistemi ile stratejik hedeflerin belirlenmesi, bilgi türünün tespitinde de örgüt içerisinde stratejik boşluk oluşmasına engel olmaktadır[65]. Bilgi türünün tespitinde, kamu

---

[62] M. Yu Zakharov vd., **a.g.e.** ss.154-159

[63] Susanne Krasmann, **a.g.k.**

[64] Roland Yaw Kudozia, "Organizational Knowledge Management Practices Among Ghanaian Enterprises: Assessing Knowledge Management Practices In The Service Industry İn Accra", **Aspen Journal of Scholary Works**, Cilt.3, Sayı.1, 2023, ss.212-229

[65] Ramy Al-Sehrawy, vd., "A Knowledge Management Strategy for Urban Digital Twins", https://www.researchgate.net/publication/362127397_ (Erişim Tarihi: 13.03.2023).

kurumları ve diğer organizasyonların yönetim faaliyetlerinde bilinmesi gerekenleri ve eksik veya mevcut bilginin neler olduğunun belirlenmesi gerekmektedir.

Bilgi güvenliği yönetim sistemi ile mevcut bilgi ve yeni bilginin oluşumunda stratejik hedefler doğrultusunda yönetim faaliyetleri gerçekleştirilmektedir. Bilgi güvenliği yönetim sistemi, kamu kurum ve yönetim organizasyonlarının veri tabanlarında depolanan bilgileri, bilgi ve iletişim teknolojileri vasıtasıyla kullanıcıların doğrudan bilgiyi üretene kişilerle etkileşim kurmadan bilgiye erişim imkânı sunulmaktadır[66]. Aynı zamanda bilgi güvenliği yönetim sistemi ile açık kaynak bilgi erişiminden faydalanarak rekabeti pekiştirici bilgi transferleri ile örgütlerin stratejik hedeflerine ulaşmasına yardımcı olunmaktadır.

Örgütlerin stratejik hedefleri doğrultusunda, eldeki mevcut bilginin korunması, rakip unsurlar tarafından ele geçirilmesi veya bilgiyi ortadan kaldırabilecek tehditlere karşı tedbirlerin, bilgi güvenliği yönetim stratejilerinin tespit edilmesi ile güvenli bir şekilde saklanması, korunması ve bilginin orijinal kalması hedeflenmektedir[67].

Bilgi güvenliği yönetim sisteminin amacı, mevcut bilgilerin muhtemel tehditlere karşı korunması, yeni bilginin rekabet ortamında bilgiye yeni yorumların eklenmesi veya yeni bilginin oluşumdaki tehditlerin ortadan kaldırılması ve örgütlerin stratejik hedefleri doğrultusunda bilginin işlenmesini sağlamaktır.

Bilgi güvenliği yönetimi sistemlerinin hedeflerini gerçekleştirebilmesi için yalnızca yönetim süreçlerine ve teknolojiye bağlı kalmaksızın, bilgi ve insan kaynaklarına verilen önem ile başarılı bir yönetim faaliyeti meydana gelmektedir[68].

Bilgi güvenliği yönetim sisteminin, yönetici ve kullanıcı performansları ile doğrudan bağlantısı bulunmasından dolayı, özel işletmelerin veya kamu kurumlarının

---

[66] Selma Baran ve Emine Şener, "Örgütsel Bilgi Paylaşımı Reddi ile Bilgi Güvenliği Kültürünün İlişkisinin İncelenmesi", **İnsan ve Toplum Bilimleri Araştırmaları Dergisi**, Cilt 1, Sayı 9, 2020, ss. 299-325.

[67] Jeb Webb, ve diğerleri, "Information Security Risk Management: An Intelligence-Driven Approach", **Australasian Journal of Information Systems**, Cilt 18, Sayı 3, 2014, ss. 391-406.

[68] Atif Ahmad ve Rachelle Bousa, "Protecting Organizational Competiteve Advantage: A Knowledge Leakage Perspective", **Elsevier (Computers & Security)**, Cilt 1, Sayı 42, 2014, ss. 27-39.

aktif yönetim faaliyetlerinde bilgi güvenliği yönetim sistemlerinin faydalı bir yönetim aracı olarak kullanıldığı değerlendirilmektedir.

Bilginin genel anlamda pozitif olduğu düşünülmektedir. Ancak bilginin her zaman pozitif ve iyi olduğunu kabul etmek, bireyler ve örgütler için imkânsız görülmektedir. Bilginin bireylere ve organizasyonlara sürdürülebilir bir tartışma ve rekabet ortamı sunduğu ve toplumun gelişimine katkı sağladığı kabul görmektedir[69].

Sürdürülebilir bir rekabet ortamında mevcut bilginin üzerine yeni verilerin eklenmesi veya yeni bilginin oluşumu örgütlerin bilgi güvenliği yönetim sistemlerinin stratejik hedefleri doğrultusunda ilerlediği taktirde gelişmesi ve hedeflere ulaşılması mümkün olması beklenmektedir[70]. Sürdürülebilir bir tartışma ve rekabet ortamının oluşmaması bilginin olumlu kullanıldığı varsayımını ortadan kaldırmaktadır. Bilgi güvenliği yönetim sistemleri örgütlere sürdürülebilir bir rekabet ortamı ve gelişim açık imkanlar sunmaktadır.

Bilgi güvenliği yönetim sistemi, örgütlere rekabet avantajını sağladığı ve gelişime sağladığı yenilikler ile yeni hedefler doğrultusunda aktif bir yönetim imkânı tanımaktadır. Bilgi güvenliği yönetimi ile mevcut bilgiyi, aktif kullanma ve yönetme yeteneğinin bulunması örgütler arasındaki rekabetin ve gelişimin sürdürülebilir olması, yönetim faaliyetlerinde bilgi güvenliği yönetim sisteminin önemini ön plana çıkartmaktadır[71].

Bilgi güvenliği yönetim faaliyetlerinde, rekabet ortamının oluşması ve netice elde edilmesi bilginin ve kurumların gelişimini sağlamaktadır. Bilgiyi doğru kullanma

---

[69] Werner Bornman ve Les Labuschagne, "A Framework for Information Security Risk Management Communication", https://www.researchgate.net/publication/220803387 , (Erişim Tarihi:30.03.2023).

[70] Piya Shedden ve diğerleri, "Incorporating a Knowledge Perspective into Security Risk Assessments", https://www.researchgate.net/publication/235297507_ , (Erişim Tarihi: 30.03.2023).

[71] Peter Trkman ve Kevin C. Desouza, "Knowledge Risks in Organizational Networks: An Exploratory Framework", **The Journal of Stategic Infortamation Systems**, Cilt 1, Sayı 21, 2011, s. 9

ve yönetme becerileri ile mevcut bilgiye eklenen yeni yorumlar ile yeni bir kavramın veya ürünün üretilmesi söz konusudur[72].

Bilgi, etkin bir şekilde yönetildiği taktirde kavram karmaşasının ortadan kalkması ve yönetsel faaliyetlerin başarıya ve hedeflere ulaşılmasında avantaj olarak değerlendirilmektedir. Bilgi güvenliği yönetim sistemi, bilgiyi bir varlık olarak geliştirmek, korumak ve kullanıcıların erişimine imkân tanıma sürecini kapsamaktadır. Bilgi güvenliği yönetim sisteminin hedefi, bilgiyi ve yönetim süreçlerinin sonuca ulaşması ve genel olarak bilgi analizinin gerçekleştirilmesini sağlamaktır.

Bilgi güvenliği yönetim sistemi, bilginin optimal seviyede kullanılmasını, bilginin evrensel olarak değerlendirilmesi, bilgi güvenliği yönetim kültürünün oluşturulması ve kullanıcılar arasında bilginin çevrimiçi ve çevrimdışı paylaşımı faaliyetleri ile gerçekleştirilmektedir[73]. Bilgi güvenliği sistemlerinde insan kaynakları, ihtiyaç duyulan bilginin tespit edilmesi ve anlaşılması, bilginin oluşum aşamasında kavramsal eksikliklerinin ve hataların düzeltilmesi, bilgi ve iletişim teknolojileri bilgisinin yeterliliği kullanıcılar, karar vericilerin ve bir örgütün tüm bireylerini kapsamaktadır.

Örgütlerin stratejik hedeflerine ulaşma sürecinde, yeni bilgi üretme, bilgi ve iletişim teknolojilerini aktif kullanarak belirlenen hedeflere en kısa zamanda, rekabet ortamında gelişime açık yeni bilgi ve kavram üretmek maksadıyla insan kaynakları örgütlerin tüm bireylerinin aktif rol aldığı bir yönetimi ifade etmektedir[74].

İnsan kaynaklarının faaliyetleri, örgütlerin stratejik hedefleri doğrultusunda iş süreçlerinin belirlenmesi bilgi güvenliği yönetim sistemleri tarafından

---

[72] David Snetselaar, "Dreams Lab: Assembling Knowledge Security in Sino-Dutch Research Collaborations", **European Security**, Cilt 1, Sayı 1, 2022, ss. 1-20

[73] Joe Mutebi ve diğerleri, "Relative Influence of Social Media Socio-Technical Information Security Factors on Medical Information Breaches in Selected Medical Institutions in Uganda", https://www.researchgate.net/publication/365365748 , (Erişim Tarihi : 20.03.2023).

[74] Hussein Vakhaevich Idrisov, "Information Security in the National Security Systems in the Modern Age", **Fiat Justisia Jurnal Ilmu Hukum**, Cilt 16, Sayı 4, 2022, ss. 321-330.

gerçekleştirilmektedir. Kamu kurumları ve diğer organizasyonların içerisinde, iş tanımlamalarının yapılması, yönetim sürecinde her bir bölümün görev tanımlarının belirlenmesi, çalışanlar ve yöneticiler arasında geçen bu zaman dilimi faaliyet sürecini oluşturmaktadır.

Örgütlerde faaliyetlerin tanımlanması, örgüt içerisinde faaliyet alanlarının bölümlere ayrıştırılması, komuta ve koordinasyon ilişkilerinin geliştirilmesi bilgi güvenliği yönetim sistemlerinde iş süreci olarak nitelendirilmektedir[75]. İş sürecinde, bilginin paylaşılması, bilgi ve iletişim teknolojilerinin aktif kullanımı, örgütlerin stratejik hedeflerine ulaşma amacı ile sürecin sorunsuz olarak faaliyet göstermesi gerekmektedir.

Bilgi güvenliği yönetim sisteminde, bilgi ve iletişim teknolojilerinin aktif kullanılması, organizasyonlar içerisinde kullanılan teknolojiye hâkim olma bilgisinin önemi günümüzde artmaktadır. Bilgi ve iletişim teknolojileri, kamu kurumları ve diğer organizasyonların faaliyetlerinin yerine getirilmesinde ve dış dünya ile teknoloji araçları vasıtasıyla etkileşim içerisinde olmak, kamu kurumlarının ve diğer organizasyonların stratejik amaçlarına ulaşmalarına yardımcı etmenlerdir[76].

Bilgi güvenliği yönetim sistemlerinde, bilgi ve iletişim teknolojilerinin aktif kullanılması, iş süreçlerinin işletilmesinde örgütlere zaman kazandırarak, sürecin hızlı ve etkin olması avantaj sağlamaktadır. Bilgi güvenliği yönetim sistemi, kamu kurumları ve diğer yönetim organizasyonlarına fayda sağlama, yönetim faaliyetlerinde ve karar sürecinde hızlı ve etkililik, faaliyetlerin yerine getirilmesinde zaman tasarrufu

[75] Rasim Alguliyev, ve diğerleri, "Information Security as a National Security Component", **Information Security Journal A Global Perspective**, Cilt 30, Sayı 47, 2022, ss, 1-18.

[76] Rasim Alguliyev, ve diğerler, **a.g.e**., ss. 1-18.

sağlayarak belirlenen stratejik hedefeler doğrultusunda sonucu ulaşmayı hedeflemektedir[77].

1.6. Risk Analizi ve Risk Yönetimi

Risk analizi, riskin hangi tür ve uygulamalar ile zamanı ve belirlenen güvenlik politikalarıyla veya risk oluşumunda önceden kestirilemeyen saldırılar ile meydana gelmektedir. Bilgi güvenliği, gizlilik politikaları, siyasi, stratejik, finansal açıdan risklerin değerlendirilmesi neticesinde risk analizi yapılmaktadır[78].

Kurumların ve organizasyonların, gizlilik ve güvenlik politikalarına yönelik uygulanan plansız ve belirsizlik içinde, gerçekleştirilen saldırıların tümü risk olarak değerlendirilmektedir. Organizasyonların amaçları doğrultusunda, hareket imkân ve kabiliyetlerin engellenmesi ve bir takım veri kayıplarının yaşanmaması için risk analizinin önemi ortaya çıkmaktadır.

Bilgi güvenliği yönetim sisteminin oluştururken, risk yönetimi ve risk analiz raporlarının bulunması, kurumların ve kişilerin hem finansal açıdan hem de güvenli bir bilgi yönetimi sisteminin oluşumu için risk yönetimine dikkat edilmesi gerekmektedir[79].

Risk yönetimi, kurumların amaçlarına ulaşmaları için verilerin korunması, saklanması ve iletiminde meydana gelebilecek her türlü saldırı ve veri kaybını engellemek amacıyla kurumlara ve kişilere yarar sağlamaktadır. Bilgi ve iletişim teknolojilerinin gelişimi ile beraber, organizasyon yöneticilerinin sürekli denetim yapmalarına, bir ekip kurulması, yöneticilerin ve çalışanların bireysel sorunların farkındalığı ile birlikte risk yönetimi uygulamalarında dikkat edilmesi gereken faktörlerdir[80].

---

[77] Peter Trkman ve Kevin C. Desouza, **a.g.e.**, s. 11.

[78] Ebru Bağcı, "Risk Analizi ve Yönetimi", **Turizm İşletmelerinde Güncel Stratejik Yaklaşımlar**, Ed. Ülker Çolakoğlu, Melahat Avşar, H. Erhan Altun ve Ramazan Demir, 1. Baskı, Detay Yayıncılık, Ankara, 2020, ss.161-171

[79] Kara, **a.g.e.** s.33

[80] Canbek, **a.g.e.** 2006, s.170

Risk analizi uygulamaları, belirsizliklerden oluştuğu varsayımı ile önceden kestirilemeyen ve saptanması güç tehdit ve saldırıları önlemeye hedefleyen bir yönetim sistemidir. Bilgi güvenliğinin en üst seviyede olması, diğer kullanıcılar arasındaki veri iletim problemlerini doğurabilmektedir. Açık bir veri aktarım kanalı kullanılması, bilginin kaybolmasına ve değiştirilmesine imkân vermektedir. Veri iletim yollarının elektronik ortamlarda kriptolu ve hızlı iletim kanalları tercih edilmesi gerekmektedir[81].

Günümüzde matbu evrak iletimi güvenli bir transfer gibi görünse de kurumların ve organizasyonların zaman kaybı yaşamasına imkân vermektedir. Elektronik ortam iletişim kanalları kullanılarak bir takım yazılım uygulamaları ile güvenli hızlı bir veri transferi gerçekleştirebilir. Ancak elektronik ortamlara yapılan saldırılar neticesinde veri kaybına yol açması mümkün olduğu için risk yönetimi önemine burada dikkat çekilmesi gerekmektedir[82].

Bilgi ve iletişim teknolojilerinin hayatımızdaki yeri, gün geçtikçe artan kullanımı, bilgiye ulaşmanın ve oluşacak tehditlere karşı güvenlik stratejilerin belirlenmesi ve yönetimi zaruri bir ihtiyaç haline gelmiştir. Güvenlik politikalarının tespiti ve icrası, üçüncü taraf veya erişim izni bulunmayan kişiler tarafından saldırıların önlenmesi, risk analizinin planlanması ve risk yönetimi için insanların bilinçlendirilmesi gerekmektedir.

Bilgi güvenliği yönetim sistemine karşı oluşacak tehditlere karşı bütün organizasyonlarda yönetici kadroların yanı sıra kullanıcı seviyesi personelin bilgi güvenliği eğitimi ile hataları en az seviye indirilmesi ön görülmektedir[83].

Bilgi güvenliği eğitimi öncelikle, bilgi yönetim sistemleri içerisinde istenmeyen yetki dışı veri erişimlerini önlemek, güvenlik protokollerin eksiksiz olarak uygulanması, kitle iletişim araçlarının ve organizasyon varlıkların lüzumsuz olarak

---

[81] Bağcı, **a.g.e.,** ss.161-171

[82] Ertuğrul Aktan ve Belgin Aydıntan, "Cameron-Freeman Örgüt Kültürü Türleri Ekseninde Örgüt Kültürü ve Bilgi Güvenliği Algısı İlişkisi: Devlet Üniversitelerinde Bir Uygulama", **Journal of Business Research Turk,** Cilt.8, Sayı.4, 2016, ss.324-344

[83] Kara **a.g.e.**, s.36

kullanılmasının önüne geçmesini amaçlamaktadır. Yöneticilerin sorumluluklarını yerine getirirken, insan faktörünün olduğu bir organizasyonda hatayı minimuma indirmek, personel eğitimi ve denetimden kaçınılmaması gerekmektedir[84].

Risk analizi, organizasyonların yönetiminde bilgi güvenliği politikaları, organizasyonda yer alan bilgi ve iletişim teknolojileri araç ve gereçlerini, kurum verilerini ve politikalarını aynı zamanda insanların kişisel verilerin korunmasını hedeflemektedir[85].

Kişisel veriler ve kurum verileri, kişilerin ve kurumlara ait marka ve isimlerden, faaliyetlerinden ve çalışan bilgilerin tümünü kapsamaktadır. Olası bir saldırı durumunda bu verilerin korunması insanlara karşı güveni arttırmaktadır. Aynı zamanda kurum kimliğinin zarar görmesine olanak tanımamaktadır.

Kişisel verilerin, bilgi güvenliği ve risk analizi raporlarının hazırlanmasındaki en önemli envanterler olduğu bilinmektedir. Veri kaybını önlemek amacıyla kişisel verilerin korunması ve kişisel veri koruma hukukuna uygun yönetim tarzı seçilmelidir. Bilgi güvenliği yönetim sisteminin, kişisel verilerin işlenmesinde ve hukuki sorumluluklarının yerine getirilmesi için ihtiyaç duyulan güvenlik protokollerini ve kişisel verilerin korunmasına yönelik politikaların belirlenmesinde en önemli görev ve sorumlulukları arasında yer almaktadır.

---

[84] Kara, **a.g.e**. , s.37

[85] **a.g.e.** , s.27

1.7. Kişisel Verilerin Korunması

1.7.1. Tarihsel Süreç

18. yüzyıl endüstri devriminin Avrupa Kıtasında ortaya çıkmasıyla birlikte, yerleşim yerlerindeki bütünlüğün artması ve devlet yönetimlerinin ilişkileri arttığı görülmüştür. Endüstri alanın da gerçekleştirilen yenilikler neticesinde, artan işletme ve bireysel iletişim ile kişisel verileri ortaya çıkmıştır[86].

Sanayi alanında gerçekleşen artışın, üretim alanlarının ve devletler arası politikaların 19. Yüzyıl ortalarında veri artışına, verilerin saklanması ve korunması ihtiyacı ortaya çıkmıştır. Teknolojik gelişmelerin etkisi ile bilgi ve iletişim teknolojileri araçları olan, elektronik iletişim kanalları, kamu alanında ve özel sektörlerde kişisel verilerin korunmasının önemi daha da artmıştır.

Avrupa insan hakları sözleşmesinde, özel hayatın gizliliği, kişilerin temel hak ve özgürlüğün korunması Avrupa konseyi tarafından sözleşmede yerini almasını sağlamaktadır. Kamu sektöründe, finans ve diğer özel işletmelerin kişisel verilerin korunması hakkında yasal süreçleri ilk kez Kıta Avrupa'sında ve Amerika Birleşik Devletleri'nde görülmüştür[87]. Bilgi ve iletişim teknolojilerin kendini sürekli yenilemesi ile 1970'li yıllarda birçok Avrupa ülkesinde elektronik ortamlarda kişisel verilerin korunması ve işletilmesi yasal olarak başlandığı bilinmektedir[88]. Yerel yönetimler denetimi ve resmi makamlar kişisel verilerin korunması, kişisel verileri kontrol edenleri ve kişisel verilerin işlenmesini, halk tarafından karşı gelinmesi ile

[86] Kadir Can Özel, "Ana Hatlarıyla Kişisel Verilerin Korunmasının Tarihsel Süreci ile Amacı ve Kişisel Verilerin Korunması Hakkı", **İstanbul Barosu Dergisi**, Cilt.94, Sayı.2, 2020, ss.242-255

[87] Özel, **a.g.e.,** ss.242-255

[88] **a.g.e.,** ss.242-255

kişisel verilerin korunmasının yasal olarak devletler tarafından dikkate alındığı ve kanunlaştırarak uygulamalara yer verildiği anlaşılmaktadır[89].

Kişisel verilerin korunması, hukuki olarak bireylerin ve kurumların talepleri doğrultusunda, kişisel verilerin korunmasına ilişkin kanunda yer alan hükümler dışında kalanların sorumluluklarını kapsamaktadır. Kişisel verilerin korunması, ulusal boyutu ile kişisel verileri hukuka aykırı olarak kullanılan veri sahibinin, kişisel verilerin korunmasına ilişkin Avrupa İnsan Hakları Sözleşmesinden doğan haklarının ihlali ile tespit olunmaktadır.

Yasal sürecin başlaması kişilere, kurumlara ve özel işletmelere hukuki olarak yükümlülükleri yerine getirme sorumluluğunu ortaya çıkartmaktadır[90]. Kanunlar, şikayetlerin ve kişisel veri ihlallerinin tespiti ve cezai yaptırımların gerekliliklerini yerine getirmesini emretmektedir.

1.7.2. Kişisel Veri Kavramı

Kişisel veri, "*belirli ya da belirlenebilir nitelikteki bir kişiye ilişkin her türlü bilginin kişisel veri olduğu ve kişiyi belirlemeye yarayan bilgilerden oluştuğu anlaşılmaktadır*"[91]. Kişisel veri, kişilerin tespitini oluşturan isim, soy isim, kimlik bilgilerine ilişkin verilerin dışında sosyal ekonomik özellikler fiziksel özellikler ve bireye özel olan bütün verileri kapsamaktadır. Soyut kavramlar ile birlikte kişinin tespiti ve kişilere özel olan somut verilerin tamamı, kişisel veri kavramı içinde yer almaktadır.

---

[89] Zhivka Mateeva, "Protection of Persons of Personal Data Before The National Supervisory Authoriy", **Eastern Academic Journal**, Cilt.3, Sayı.1, 2020, ss.39-49

[90] Mateeva, **a.g.e.,** ss.39-49

[91] Murat Volkan Dülger, "Kişisel Verilerin Korunması Hukukunun Getirdikleri ve Yapılması Gerekenler", https://www.researchgate.net/publication/349533304 , (09.04.2023).

Kişisel veriler, gerçek kişilerin tespiti ve tanımının yanı sıra hukuki olarak tüzel kişiliklerinde firma adı, sicil bilgileri, marka yüzleri ve her türlü bilgileri kişisel veri olarak belirtilmektedir[92]. Literatürde yer alan ve kanunlarda da bahse konu her türlü veri, kişisel veri olarak sınırsıza yakın bir tanımı ifade etmektedir. Bilgi ve iletişim teknolojilerinin son asırdaki gelişim hızı ile orantılılık olarak kişisel verilerin korunması, bireyler ve toplumlar hakkında gerçekleştirilen veri madenciliği uygulamaları kişisel verilerin zorunlu olarak korunması gerektiği öngörülmektedir.

Türk Medeni Kanunu'nda, "*kişilik, çocuğun sağ olarak tamamıyla doğduğu anda başlar ve ölümle sona erer. Çocuk hak ehliyetine, sağ doğmak koşuluyla, ana rahmine düştüğü andan başlayarak elde eder*" şeklinde ifade edilmektedir[93]. Kişiliği elde eden anne rahmindeki cenin hakkındaki tüm verilerin kişisel veri kapsamında olduğu anlaşılmaktadır. Ancak ölümle sonuçlanan kişilik neticesinde, kişisel verilerin korunması yükümlülükleri, 6698 sayılı kişisel verilerin korunması kanunu hükümleri dışında kalmaktadır.

Kişisel veri kavramını tanımlarken her türlü veri ve bilgiden meydana geldiği anlaşılmakta olup, vefat neticesinde hayatta bulunmayan kişinin bilgileri kavram dışında kalmaktadır. Vefat eden kişinin, mirasçılarına geçen hak ve miraslar, yeni bir kişilik olarak değerlendirilemeyeceği için vefat etmiş kişi hakkında hükümler geçersiz olacaktır[94].

Özel hayatın gizliliği ve ticaret sırların, kişisel ve kurumlar arasındaki sözleşmeler ile temel hak ve özgürlüklere karşı işlenebilecek suç ve kötü niyetli veri kullanımının önüne geçmektedir. Kişisel verilerin korunmasına ilişkin yasal dayanakların yanı sıra kişilerin ve kurumların ve özel sektör içerisinde yer alan bütün

---

[92] İsmail Sevinç ve Niyazi Karabulut, "Kişisel Verilerin Koruma Kurumu Üzerine Bir İnceleme", **Akademik Hassasiyetler Dergisi,** Cilt.7, Sayı.13, 2020, s.461

[93]Türk Medeni Kanunu, "1. Bölüm Gerçek Kişiler, Kişilik, Madde 28", https://www.mevzuat.gov.tr/MevzuatMetin/1.5.4721.pdf , (Erişim Tarihi: 09.04.2023).

[94]Sefer Oğuz, "Kişisel Verilerin Korunması Hukukunun Genel İlkeleri" , **Bilgi Ekonomisi ve Yönetimi Dergisi,** Cilt.13, Sayı.2, 2018, s.125

faktörlerin görev sorumlulukları, yükümlülüklerinin tümü usul ve esaslara uygun hareket etme zorunluluğu ihtiyacı ortaya çıkmaktadır[95].

Kişisel verilerin korunması kanunlarıyla, istemeyen kişiler tarafından art niyetli kullanımı neticesinde, ikili ve çoklu iletişim ve etkileşimler, açık rıza metini gibi sözleşmeler ile kullanımının yasal olarak tanıyarak, gerçekleştirebilecek olumsuzlukların ve kişilere zarar vermesinin önüne geçmesi düşünülmektedir[96].

1.7.3. Kişisel Verilerin Korunması Gereksinimi

Günümüzde artan elektronik ortam ve etkileşimler neticesinde, özel sektör ve kamu sektöründe insanlar herhangi bir işlem, alışveriş veya başvuru durumlarında, kişisel verilerini paylaşmak zorunda kalmaktadır. Kişisel verilerin, kurumlar tarafından ve etkileşim içinde bulunulan platformlarda kayıt altında kalması, kişilere ait verilerin erişim izni olmayan kişiler tarafından kullanılmasına imkân vermektedir.

Kötü niyetli kullanıcı ve sistemlerde oluşan açıklıkları kullanarak, kişilerin özel hayatın gizliliği ve bireysel hak ve özgürlüklerine saldırı olması mümkün hale gelmektedir[97].

Devletlerin, kişisel verilerin korunmasına yönelik çalışmalara yer vermesi ve kanunlar çıkartması hem kişilerin hem de organizasyon ve kurumların güvenli bir şekilde internet ortamında etkileşime geçmesini sağlamaktadır[98]. Bilgi ve iletişim teknolojilerinin artan kullanımı, bireylerin sosyal medya hesap kullanarak, bu platformlarda resim, video düşünce ve fikirleri yanı sıra elektronik posta adresleri, isim, soy isim ve benzeri bilgilerin tümü açık bir şekilde erişim imkânı bulunmaktadır.

---

[95] Selen Uncular, "Kişisel Verilerin Korunması Kanunu'nda Yer Alan Hakların ve Hükümlülerin İş İlişkisindeki Yansımaları", **Çankaya Üniversitesi Hukuk Fakültesi Dergisi**, Cilt.5, Sayı.1, 2020, ss.3405-3427

[96] Aleksandar Skendzic, v.d., "General Data Protection Regulation – Protection Of Personal Data in An Organisation", https://www.researchgate.net/publication/326708317 , (09.04.2023).

[97] Murat Volkan Dülger, "İnsan Hakları ve Temel Hak ve Özgürlükler Bağlamında Kişisel Verilerin Korunması**", İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi**, Cilt.5, Sayı.1, 2018, ss.72-143

[98] Selçuk Kahraman ve Önder Kutlu, "Türkiye'de Kişisel Verilerin Korunması Politikasının Analizi", **Siyaset, Ekonomi ve Yönetim Araştırmaları Dergisi,** Cilt.5, Sayı.4, 2017, ss.45-62

Açık kaynak erişimler üzerinden, bir takım yazılım programlarıyla insanların sosyal medya hesaplarından kişisel verileri alarak, kötü niyetli olarak kullanılması kişisel verilerin korunmasına engel teşkil etmektedir[99]. Kişisel verilerin açık rıza göstermeden kullanılması, hukuki olarak siber suçlar kavramı içerisinde yer almaktadır. Son yıllarda yeni bir suç kavram olarak ortaya çıkan siber suçlar, devletlerin kişisel verilerin yanı sıra temel hak ve özgürlüğün korunmasına yardımcı olmaktadır.

Erişim izni olmayan kişiler tarafından insanları kandırılması, şantaj yoluyla ekonomik bir kazanç elde etmeyi amaç güden kötü niyetli insanlardan, bireysel olarak insanların bilinçlendirilmesi ve devletlerin bu alanda hukuki çerçevede cezai yaptırımlara yer vererek, caydırma politikaları uygulaması gerekmektedir[100]. Özel hayatın gizliliği, finansal bilgilerin korunması ve izinsiz paylaşımların önüne geçilmesi, temel hak ve özgürlüklerin bireyler üzerinde çekince yaşamadan güvenli bir erişim ve veri paylaşımı yapmaları için, devletler tarafından kişisel verilerin korunmasına ilişkin politikalara yer verildiği görülmektedir[101].

1.7.4. Kişisel Verilerin Korunmasına İlişkin Uygulamalar

Kişisel verilerin korunması, özel hayatın gizliliği ve temel hak ve özgürlüğün bireylere tam ve eksiksiz olarak bu hakların yerine getirilmesine imkân vermektedir. Özel sektör işletmeleri, kamu kurumları ve sivil toplum kuruşları, insanların kişisel verilerini, veri tabanları oluşturarak saklamaktadırlar. Depolanan verileri, özel

---

[99] Önder Köktürk, "The Protection Of Personal Data – Kişisel Verilerin Korunması (Turkish)", https://www.researchgate.net/publication/335813724 , (Erişim Tarihi:09.04.2023).

[100] İlke Gürsel, "Protection Of Personal Data in İnternational Law And The General Aspects Of The Turkish Data Protection Law", **D.E.U Hukuk Fakültesi Dergisi**, Cilt.18, Sayı.1, 2016, s.38

[101] Sevinç ve Karabulut **a.g.e.,** 2020, s.465

işletmelerin reklam ve iletişim politikaları doğrudan insana ulaşmak, kendi kampanya ve reklamları kitle iletişim araçları ve mobil araçlarla gerçekleştirmektedirler[102].

Devlet yöneticileri, 21. Yüzyılda ortaya çıkan elektronik devlet politikaları ile vatandaşlarına, kamu kurumlarına gitmelerine gerek kalmadan internet ortamında sağlık, ulaşım, eğitim ve benzeri hizmetlerini sunmaktadır. Elektronik devlet uygulamalarında, insanların kişisel verilerini kullanarak gerçekleştirdiği işlemlerde ve hizmetlerde kamu personeli ile muhatap olmadan işlemlerini gerçekleştirebilmektedirler.

Gerçekleştirilen işlemler, internet ortamında bireyin kimseyle muhatap olmaması, kişisel verilerin kamu personellerine ulaşmadığı için bütün sorumluluk kişiler üzerinde kalmaktadır[103]. Bu uygulamalar devletlerin kırtasiye ve personel yanı sıra hizmet binası ve benzeri imkanlardan daha az sayıda bulundurarak tasarruf sağlamalarına imkân tanımaktadır[104].

Ülkemizde ve birçok Avrupa ülkesinde kişisel verilerin korunmasına ilişkin yasalar çıkartılmıştır. Anayasal haklar arasında yer alan, yaşama, maddi ve manevi varlığının korunması, özel hayatın gizliliği ve temel hak ve özgürlükler, devletler tarafından anayasal güvence ile korunmaktadır[105]. "*Amerika Birleşik Devletleri'nde kişisel verilerin korunması anayasal bir hak olmayıp, bu konuda sektörel çözümlere yer verilmiştir*"[106].

Kişisel verilerin anayasa tarafından korunması, Amerika Birleşik Devletleri'nde finansal olarak, negatif etkileri olabileceği öngörülmüş ve bu konunun ekonomik bir hak olduğu nitelendirilmiştir. Kişisel verilerin, bireylerin ekonomik

---

[102]Türkay Henkoğlu ve Nazan Özenç Uçak, "Protection Of Personal Data in University Libraries", **Bilgi Dünyası**, Cilt.16, Sayı.1, 2015, ss. 45-74

[103]Elvira Talapina, "Legal Protection Of Personal Data in France", https://www.researchgate.net/publication/341600038 , (Erişim Tarihi: 09.04.2023).

[104] Uncular, **a.g.e.,** ss.3405-3427

[105] Gürsel, **a.g.e.**

[106] Dülger, **a.g.e.** , 2018, ss.72-143

hakları arasında olduğu görüşü, bireylerin kişisel verilerin kendi ekonomik çıkarları doğrultusunda kullanmaları yönünde değerlendirilmiştir[107].

Kişisel verilerin korunması, fikri mülkiyet hakları arasında bir değer görüşü olduğu savunulmaktadır. Kişilerin manevi haklarından olan mülkiyet hakkı, kişisel verilerin kullanılmasına yönelik bireylerin inisiyatifi hukuki çerçevede değerlendirilmesi bireysel olarak vatandaşlara sunulmaktadır.

Kişisel verilerin korunmasına ilişkin, ülkeler arasında farklılıklar görünse de genel düşünce kişisel verilerin tek bir yasa altında korunarak bireylere bu yönde güvence verilmesi gerektiği değerlendirilmektedir. Kişisel verilerin korunması, çağın gerekliliklerinden olan bilgi ve iletişim teknolojilerinin bir takım sistematik açıklıklarından faydalanılmaktadır.

Kişisel verileri, kötü amaçlı kişiler tarafından bilgi ve iletişim teknolojileri vasıtasıyla elde edilerek kişiler üzerinde baskı, tehdit ve şantaj yapılmasına neden olmaktadır. Siber güvenlik açıklıklarından faydalanan kötü niyetli kişilerin, kişisel verilerin izinsiz erişim sağlayarak kendi çıkarları doğrultusunda kullanmaktadırlar[108].

Hukuksal olaraktan, siber suç kavramı içerisinde yer alan bu veri hırsızları, devletler tarafından ceza hukuku alanındaki suçlar kapsamına girmektedirler. Verinin, hangi amaçlar doğrultusunda kullanıldığı kişilere, kurumlara ve organizasyonlara vermiş olduğu zararın tazmin yükümlüklerine yer verilmektedir[109].

Yasadışı erişimlerin önüne geçilememesi, bilgi ve iletişim teknolojilerin hızlı gelişiminden ve kişilerin bireysel zaaflarının kullanmasından dolayı, veri kayıplarına yol açılmaktadır. İzinsiz erişim ile kullanılan casus yazılımlar aracılığıyla, ekonomik

---

[107] Jonatas S. De Souza, ve diğerleri, "The General Law Principles For Protection The Personal Data And Their İmportance", **AIRCC Publishing Corporation**, Cilt.10, Sayı.11, 2020, ss.110-120

[108] Serkan Gönen ve Ercan Gürcan Yılmaz, "Bilişim Alanında İşlenen Suçlar ve Kişisel Verilerin Korunması", **Bilişim Teknolojileri Dergisi**, Cilt.9, Sayı.3, 2016, ss.229-236

[109] Gönen ve Yılmaz, **a.g.e.,** ss.229-236

kazanç ve tehdit unsurlarını açıkça kişilere ve devletlere, kötü niyetli kişiler tarafından uygulamaktadırlar.

Siber suçlarla mücadele birimleri tarafından çoğu zaman tespiti mümkün olmayan noktalardan bu işlemler gerçekleştirilmekte, devletlerin siber savunma alanına yönelik çalışmalar yapması ihtiyacını ortaya çıkartmaktadır[110].

1.8. Bilgi Harbi Kavramı

Bilgi harbi, bilgi merkezli devletler arasında gerçekleştirilen taarruz ve savunma teknikleriyle kullanılan elektronik harbin temelini oluşturan bir unsurdur[111]. "*Bilgi tabanlı harp, aynı zamanda siyasi, ekonomik ve sosyal sahalarda gerçekleştirilebilmekte ve hem barış hem de koşulları altında tüm ulusal güvenlik spektrumu üzerinde de uygulanabilmektedir*"[112].

Bilgi harbi, 21.yüzyılda artan teknolojik gelişmeleri ile bilgi ve iletişim teknolojilerinin güvenlik neticesinde bilgi kayıplarına neden olmaktadır[113]. Uluslararası bilgi akışı, çevrimiçi haberleşme uygulamaları, bilgisayar ağları, veri madenciliği ve veri tabanı uygulamalarının tümü birbiri ile bağlantılı ve bu uygulamaların ilişkileriyle gerçekleşmektedir[114].

Elektronik harp, "*bilgiye dayalı bu süreçlerin enerji, finans, sağlık, lojistik, bakım, ulaştırma, personel, kontrol sistemleri (hava, deniz, demiryolu, yol, nehir, boru*

---

[110]Tigran Oganesian, "Protection Of Personal Data: Positions Of İnternational Courts", https://www.researchgate.net/publication/333708289 , (Erişim Tarihi: 09.04.2023).

[111] Grigory L. Tulchinsky, "Information Wars As A Conflict Of İnterpetations: Activating The 'Third Party'", **Russian Journal of Communication**, Cilt.5, Sayı.3, 2013, ss.244-251

[112] D. Curtis Schleher, "**Bilgi Çağında Elektronik Harp**", Çev. Berna Kara 1.Baskı, Doruk Yayımcılık, Ankara, 2004, s. 20

[113]D. V. Shibaev, "Methods To Counter Information War", **Russian Journal of Legal Studies**, Cilt.4, Sayı.9, 2016, ss.60-68

[114]Radoslav Ivancik, "Information War – One Of The Multidisciplinary Phenomennes Of Current Human Society" , https://www.researchgate.net/publication/350963287 , (Erişim Tarihi: 19.05.2023).

hattı ve kanal nakliye sistemleri), istihbarat, komuta kontrol muhabere sistemleri olarak değişiklik göstermesi" mümkün olmaktadır[115].

Elektronik harp ve bilgi harbinin temelini meydana getiren bu bileşenlerin bilgi ve iletişim teknolojileri ile kullanıcılar, bilgi paylaşımı ve bazı elektronik ortamdaki hizmetlerin yerine getirilmesine yardımcı unsurların korunması zorunlu hale gelmiştir. Ülkelerin ulaşım, enerji, finans, sağlık ve istihbarat faaliyetlerinin milli güvenlik açısından önemi açık bir şekilde görülmektedir[116].

Ülkeler belirtilen unsurların 21. Yüzyılda daha çok bilgi ve iletişim teknoloji imkanları ile gerçekleştirmektedir. Bilgili ve iletişim teknolojilerinin olası yaşanabilecek tehdit ve saldırılar ihtimali ile bütün bu hizmetler kesintiye uğraması mümkün olduğu görülmektedir[117]. Elektronik harp unsurlarından, elektronik korumaya en kötü senaryo ile karşı karşıya kalınmadan uygulanabilmesi olasıdır. Elektronik harp ve bilgi harbi bağlamında ülkeler milli güvenliklerindeki elektronik harp unsurlarının önemi anlaşılmaktadır[118].

Elektronik harp anlamında, kişisel veriler ve kurumların verileri erişim izni olmadan bu bilgiler kötü niyetli kullanıcıların eline geçebilmektedir. Bilgi güvenliği, kişisel verilerin korunması, siber güvenlik sorunları, elektronik devlet, elektronik yönetişim, elektronik ticaret, elektronik sağlık, elektronik demokrasi ve benzeri sosyal bilimler alanında giren bütün elektronik kavramların korunması elektronik harp konusu içinde yer aldığı değerlendirilmektedir. Ülkelerin, diğer müttefik ve düşman ülkelere üstünlük sağlamak ve olası siber saldırılara karşı elektronik harp korunma unsurları ile cevap verilmesi mümkün hale gelmektedir.

---

[115] Curtis**, a.g.e.** , s. 23

[116]Marc Jones, "Hacking, Bots and İnformation Wars in The Qatar Spat", https://d1wqtxts1xzle7.cloudfront.net/56335866/POMEPS_GCC_Qatar-Crisis.pdf?1523917784 , (Erişim Tarihi: 19.05.2023).

[117] Iryna Zharovska ve Nataliya Ortinska, "The Information War as A Modern Globalization Phenomenon", https://www.researchgate.net/publication/345734928 , (Erişim Tarihi: 19.05.2023).

[118] Michael A. Peters, "The Information Wars, Fake News and The End Of Globalisation", https://www.tandfonline.com/doi/full/10.1080/00131857.2017.1417200 (Erişim Tarihi: 19.05.2023).

Elektronik harp unsurları, ülkelerin milli güvenlik unsurları arasında yer almalı ve ülkeler güvenlik politikalarının belirlemeleri esnasında ve gelecek planları içerisinde, bilgi çağının gerekliliklerinden birisi olan elektronik harp konusuna yer verilmesi gerektiği değerlendirilmektedir.

İKİNCİ BÖLÜM

DİJİTAL DÖNÜŞÜM

2.1. Elektronik Kavramı

Elektronik kavramı, negatif yük taşıyan atomun bir parçası olan elektronlardan meydana gelmektedir. Elektronik, elektronların davranış biçimi, kontrol edilebilirliği ile haberleşme, bilgi ve iletişim teknolojileri ve günlük yaşamda birçok alanda kullanılan cihazların temelini oluşturan teknoloji alanı olarak bilinmektedir[119]. Elektronik bir bütün olarak iletken ve yarı iletken malzemeler, mantık kapı devreleri, dijital sinyal üreticiler, mikro denetleyiciler ve haberleşme sistemleri dahil birçok etmenin bir arada kullanılmasıyla ortaya çıkmaktadır[120].

Elektronik devreleri oluşturan ve elektron akışının kontrol edildiği, devre elemanlarının uygunluğu yarı iletken malzemelerden oluşmaktadır. İletken ve yarı iletken özelliklerini taşıyan malzemeler yarı iletken olarak ifade edilmektedir[121]. Elektron transferini kontrol etmeye yarayan, transistörler, diyotlar ve kondansatör gibi yarı iletken malzemelerin bir araya gelmesiyle elektronik devreler ve cihazlar ortaya çıkmaktadır. Transistörler, düşük sinyalleri yükseltmek için elektrik akımını kontrol edilerek mantıksal (lojik) kapıların ve işlemlerin gerçekleştiği bir devre elemanıdır[122]. Diyotlar ise elektrik akımının yönünü belirlemek ve kontrol etmek için kullanılmakta olup kondansatörler elektrik yükünün depolanması ve yeniden devre elemanlarına elektrik akımının sağlanmasıyla elektrik akımının devreyi tamamlanması için serbest bırakıldığı yarı iletken elektronik devre elemanları olarak bilinmektedir[123].

---

[119] Alper Atan ve diğerler, "**Elektrik -Elektronik Esasları**", 1.Baskı, Meb Yayınları, Ankara, 2020, s.30.

[120] Erman Uzun, İlker Yakın ve Ali Gök, "**Elektronik Programlama ve Nesnelerin İnterneti**", 1. Baskı, Tübitak Yayınları, Ankara, 2011, s. 11

[121] Atan ve diğerler, **a.g.e.**, s.31.

[122] Mustafa Ergin Şahin, "**Elektronik Laboratuvarı Deneyleri – Bilgisayar Destekli ve Konu Anlatımlı**" , 1.Baskı, Nobel Akademik Yayıncılık, Ankara, 2018, s.47.

[123] Ahmet Kekik ve diğerleri, "**Temel Elektrik-Elektronik Atölyesi**", 1.Baskı, Meb Yayınları, Ankara, 2022, ss. 188-197.

Maddenin temel bir özelliği olan elektrik yükleri, iletken malzemeler olan bakır, gümüş, altın ve platin gibi materyallerin elektrik yüklerinin iletiminde kullanılmakta olup bu maddelerin işlenmesiyle gerçekleştirilmektedir[124]. Elektrik yüklerinin iletken malzemeler üzerinde oluşturduğu elektrik akımı ile üretilen gücün transferi sonucunda günlük yaşamda kullanılan teknolojiler üretilmektedir. Elektrik yüklerinin pratik yaşamda kontrol edilebilir ve yönlendirilebilir olması günlük yaşamı kolaylaştırması ve insanlara birçok avantaj sunmaktadır. Elektronik devreler, elektrik yüklerinin kontrol ve yönlendirilebilir olması, sinyallerin yükseltilmesi, gürültünün baskılanması ve elektrik yüklerinin farklı formlara dönüştürülmesi gibi birçok işlevi elektronik malzemeler vasıtasıyla gerçekleştirilmektedir[125].

Elektronik kavramı literatürde analog ve sayısal (dijital) elektronik olarak iki başlıkta incelenmektedir. Analog elektronik, oluşturulan bir elektronik devrede bilgiyi elektrik yükleri temsil etmektedir. Elektronik devre içerisinde bilgi aktarımı için devre elemanları aracılığıyla sinyaller üretilmektedir. Bilgi temsilcisi olarak üretilen sinyaller günlük yaşamda, ses, video, sensörler ve kontrol devrelerinde kullanılmaktadır[126]. Kısacası analog elektronikte bilgiyi sinyaller temsil etmektedir. Sayısal (dijital) elektronikte ise bilgiyi, ikili sayı sistemleri olan ayrık bilgi sinyalleri temsil etmektedir. 0 ve 1 bilgi sinyallerinden meydana gelen sayısal elektronik, günlük yaşamda bilgisayarlar, cep telefonları ve dijital cihaz olarak nitelendirilen yaşamı kolaylaştıran teknolojilerin tümünde kullanılmaktadır. Güç devreleri ve radyo frekans (RF) devrelerinin tümü elektronikte sıklıkla yer almaktadır. Güç devreleri, yüksek elektrik akım ve voltajı kontrol etmek için güç kaynaklarında, motor kontrol sistemlerinden meydana gelmektedir[127]. Radyo frekans (RF) devreleri ise radyo frekansları ile haberleşme gerçekleştirmek için, cep telefonları, telsiz sistemleri, kablosuz ağlar vb. tüm iletişim yöntemlerinde radyo frekanslarına yer verilmektedir.

---

[124] Atan ve diğerler, **a.g.e.**, s.31.

[125] **a.g.e**., s.42.

[126] Ahmet Zeki Akkaya ve diğerleri, "**Analog-Dijital Elektronik Atölyesi**", 1.Baskı, Meb Yayınları, Ankara, 2020, ss. 22-59.

[127] Akkaya ve diğerleri, **a.g.e**., s.272.

Dijital elektroniğin temelinde mantık (lojik) kapılar yer almaktadır. And (ve), or (veya) ve not (değil) lojik kapıları ikili sayı sistemleri üzerinden mantıksal işlemleri gerçekleştirmektedir. Günlük hayatta kullanılan sayı sistemleri onluk (decimal) olarak bilinmekte olup, sayısal elektronikte yer alan ikilik (binary) ve onaltılık (hexedecimal) sayı sistemlerine yer verilmektedir[128]. Günlük yaşamımızda kullanılan onluk sayı sisteminde 0-9 'a kadar bulunan on adet rakamlar bulunmakta, elektronikte kullanılan ikili sayı sisteminde yalnızca 0 ve 1 bilgileri ve onaltılık sayı sisteminde ise ondalık sayı sisteminde yer alan on adet rakam ve A, B, C, D, E, F harf bilgileri bulunmaktadır[129].

Dijital elektroniği analog elektronik ile kıyasladığımız zaman ortaya çıkan sonuç dijital elektroniğin doğruluğu ve güvenirliği ile sonuçları kesin olarak ortaya çıkartmaktadır. Hata payının analog elektronikte daha fazla olması dijital elektronikte ise düşük hata payı ve insani yanlışlıklar sebebiyle hataların olması dijital elektroniğin güvenirliği ve kesin sonuç vermesinden dolayı tercih edilme sebepleri arasında yer almaktadır.

21. Yüzyıl'da tüketici elektroniği, haberleşme, uzay çalışmaları ve savunma endüstrileri gibi geniş alanda kullanılmaktadır. Sayısal elektronik, mikro işlemcilerin ve mikro denetleyicilerin kullanımı ile karmaşık işlemleri kesin ve verimli sonuçlar elde edilerek dijital entegre sistemlerinin gelişmesine imkân vermekte olup, ikili (binary) sayı sisteminin doğruluğu ve güvenirliği ile desteklenmektedir[130]. Dijital elektroniğin temelini oluşturan ve tüm olasılıkları temsil eden ikili sayı sisteminde bir veri bit olarak anılmaktadır. Sekiz bitlik bir veri grubu bir byte olarak ifade edilmektedir. Basit sayısal değerlerden, karmaşık metin ve multimedya verileri dahil olmaz üzere elektronikte çok çeşitli bilgileri byte olarak temsil edilmektedir[131].

Elektronik sosyal yaşamın her alanında insanların kullandığı, haberleşmenin hızlı ve güvenli olarak gerçekleştirilmesine olanak tanımaktadır. Elektronik cihazlar, teknoloji çağında mikro boyutlara indirgenerek kullanıcılara fiziksel alan, hız ve

---

[128] Akkaya ve diğerleri, **a.g.e**., s.273.
[129] **a.g.e.,** ss.272-279
[130] **a.g.e.,** s.311.
[131] **a.g.e.,** ss.272-315

zaman kazancı sağlamaktadır. Elektronik sistemler, güncel yaşamda ve çalışma tarzımızın belirlenmesinde kritik bir öneme sahip olmaktadır. Günümüzde televizyon, akıllı telefonlar, bilgisayar, medikal teknolojiler, otomotiv ve uzay endüstrisinde kullanılmakta olup hayatın önemli bir argümanı olarak nitelendirilmektedir[132].

Bilgi ve iletişim teknolojilerinin politik ve etik sonuçları, dijital gözlem, siber zorbalık ve çevrimiçi tehditlerin artmasıyla birlikte insan hakları ve demokrasi üzerinde endişelere sebep olmaktadır. Gündelik yaşamın ve çalışma hayatını dönüştürme potansiyeli bulunan yapay zekâ ve robotik gelişmeler etik kaygıların artması aynı zamanda istihdamın düşmesi ve sosyal eşitsizliğin ortaya çıkması ön görülmektedir.

Netice itibari ile sosyal bilimlerde elektronik kavramı, elektronik teknolojilerin sosyal, kültürel, ekonomik ve politik sonuçların inceleyen karmaşık ve disiplinler arası bir alan olarak ifade edilmektedir. Günümüzde insan topluluklarını ve sosyo-kültürel faktörlerin şekillenmesinin önemli etmenlerinden birisi olan elektronik disiplininden yararlanılmaktadır[133]. Bilgi ve iletişim teknolojileri yanı sıra elektronik disiplinindeki gelişmeler, yaşam, çalışma ve etkileşim tarzımızı dönüştürmesi, sosyal bilimlerde elektronik teknolojileri ile ilişkili çalışmaların toplumun geleceğini anlama ve şekillendirme de kritik bir öneme sahip olduğu düşünülmektedir.

2.2. Dijital Bilgi

Dijital kelimesinin Türk Dil Kurumu sözlüğünde, "verilerin *bir ekran üzerinde elektronik olarak gösterilmesi*" olarak tanımlanmaktadır[134]. Bilginin tanımı ise "*veri topluluklarının bir araya gelerek oluşturulan anlamlı yığınlar bilgi meydana getirmektedir*" şeklinde ifade edilmektedir[135]. Dijital bilgi, sayısal biçimde saklanabilen, iletilen ve işlenen veri topluluklarını ifade etmektedir. Dijital bilgiye

---

[132] Elif Küzeci, "Sayı-sal Fil", 1.Baskı, İnkılâp Yayınevi, İstanbul, 2021, s.233.
[133] Küzeci, **a.g.e**., ss. 383-411.

[134] Türk Dil Kurumu Sözlüğü, "Dijital Kelime Anlamı" https://sozluk.gov.tr , (Erişim Tarihi: 21.03.2023).

[135] a.g.k.

metin, resim, ses ve multimedya dosyalarının aynı zamanda veri tabanlarında bulunan yapılandırılmış verileri örnek olarak gösterebiliriz.

Dijital bilgiler, elektronik ortamlarda bireylerin algılayabilmesi için sonuç olarak meydana gelmektedir. Analog bilgiler ise beş duyu organımız olan görme, işitme, tat alma, dokunma, koklama duygularımız ile hayatımıza yön veren eylemlerin tümü aslında analog bilgiye vereceğimiz örnek arasında yer almaktadır. Rasyonel hayatta analog bilgiye örnek verecek olursak, bir ortamdaki hava sıcaklığının hissedilmesi analog bilgi iken bu sıcaklığın bir ekran vasıtasıyla sonuç olarak bizlere gösteren bilgi dijital bilgi olarak tanımlanmaktadır[136].

21.yüzyıl'da teknolojik gelişmelerin hızla artması neticesinde, internet, mobil cihazlar ve günlük hayatımızda birçok elektronik cihaz ile çok büyük dijital veri gruplarını kullanıyor ve kontrol edebiliyoruz. Dijital bilgiler, iletişim kurma, öğrenim hayatı, alışveriş ve eğlence gibi sosyo-kültürel yaşamın ve çalışma hayatımızın bir parçası haline gelmektedir[137].

Dijital bilginin işlenmesi ve iletimi analog bilgiye göre güvenli ve hızlıdır. Günümüz dünyasında dijital bilginin depolanması fiziksel ve maliyet açısından analog bilgiye göre çok kolay ve düşük maliyetli olmaktadır. Örneğin, müzik veya ses kayıtlarının dijitalleştirilmesi zamandan kazanım sağlamakta ve fiziksel olarak saklanmasında çok daha az yer kaplamaktadır. 20. Yüzyılda kullanılan plak, kaset CD (Compact Disk) gibi fiziksel depolama araçları yerini günümüzde bilgisayar ve mobil cihaz içerisinde çevrimiçi ve çevrimdışı uygulamalar vasıtasıyla daha az yer fiziksel alan kaplayarak, emniyetli ve erişimi kolay hale gelmiştir[138].

Dijital bilginin en büyük avantajı iletme kolaylığı ve depolanmasıdır. Dijital bilgiler, sabit disklerde, internet sunucularında yer alan bulut sistemlerinde ve veri

---

[136]Mustafa Engin ve Dilşad Engin, "**Sayısal Elektronik-I**",1.Baskı, Ege Üniversitesi Yayınları, İzmir, 1999, ss.6-41.

[137] Nüket Saracel ve Irmak Aksoy, "Dijital Sürdürülebilirlik, Boyutları ve Koşulları", **Sosyal Bilimler Araştırma Dergisi**, Cilt. 10, Sayı. 2, 2021, ss.347-356.

[138] Esra Kumaş ve Serpil Erol, "Endüstri 4.0'da Anahtar Teknoloji olarak Dijital İkizler", **Politeknik Dergisi**, Cilt.24, Sayı.2, 2021, ss.609-701.

tabanı sunucularında saklanabilinmektedir. Dijital bilgilerin düzenlenmesi, silinmesi veya yeniden oluşturulması diğer avantajlarındandır. Dijital bilgi, zaman ve fiziksel olarak tasarruf imkânı verirken, yöneticilere karar verme sürecinde bilgilendirici ve inovasyonlara açık şekilde öngörülü olma ve farklı fikirlerin ortaya çıkmasına olanak tanımaktadır[139].

Dijital bilginin kullanımında bazı zorluklar ve dezavantajlarda söz konusu olmaktadır. Kişisel ve kurumsal veri gizliliğini ve güvenliğini tehdit eden unsurlar dijital bilgi yönetiminin zorlukları arasında yer almaktadır. Bilgi ve iletişim teknolojilerindeki hızlı gelişmeler neticesinde artan miktarda bilgi kirliliği ve paylaşımları, kişisel ve kurumsal veri ihlallerini ortaya çıkartmaktadır. Teknoloji çağında, erişimde dolaşan aşırı bilgi yüklenmesi gerçek bilgi ile manipülasyonlara müsait bilgilerin aynı ortamda bulunmaları bilgi kirliliğini doğurmaktadır[140].

Dijital bilginin, üretim araç ve gereçlerinin tasarımı, bilginin depolanması, kullanıcılar tarafından bilgiye erişimi, zamandan ve mekândan kazanç sağlaması, bilgi ve iletişim teknolojileri vasıtasıyla programlanabilir ve çevrimiçi ve çevrimdışı kullanımı pratik ve güvenlidir[141]. Rasyonel hayatta birçok veri ve büyüklük olarak yer tutmaktadır. Yukardaki ses, ısı, ağırlık ve benzeri örneklerde olduğu gibi minimum ve maksimum arasında yer alan büyüklükler verilerden meydana gelmektedir. Ancak dijital bilgi (sayısal bilgi), sadece sıfır ve bir değerlerini almaktadır. Dijital bilginin 0,5 gibi bir değer alması söz konusu değildir. Çünkü dijital bilgiler genel olarak somut verilerden meydana gelmekte ve veriyi güvenli ve hızlı olarak işleyerek bir sonuca ulaşmaktadır[142].

Dijital bilgiyi beş duyu organımızdan biri olan görme duyumuz ile sonuç olarak görebiliriz. Analog bilgi dijital bilgiye çevirebilmek de aynı şekilde dijital bilgi analog

---

[139] Saracel, **a.g.e.**, ss.347-356.

[140] Kumaş, **a.g.e.**, ss.691-701.

[141] Engin, **a.g.e.** ss. 6-41.

[142] Engin, **a.g.e**., ss.6-41.

bilgiye dönüştürebilmekte olup bu konu teknik ve mühendislik bilimlerinin uzmanlık alanına girmektedir.

Bilgi ve iletişim teknolojilerinin gelişmesi, bilgi üretimi ve bilgi paylaşımını hızlı bir şekilde artmasından dolayı 21. Yüzyıl bilgi ve teknoloji çağı olarak anılmaktadır[143]. Bilgi ve iletişim teknolojilerinin pozitif gelişimi sebebiyle, dijital bilginin oluşturulması ve kullanımı, aynı zamanda hızlı şekilde yaygınlaşmasıyla bilgi çağında şirketler, kurumlar ve devletler tarafından teknoloji kullanımı zaruri bir ihtiyaç olarak değerlendirilmektedir.

Üretilen dijital içerikler, dünya tarihinde fiziksel somut bilgilerin yazılı bilgilerden çok daha fazla olduğu bilmektedir. Bilginin dijital içerik olarak üretilmesi, dünya nüfusuna oranlandığı takdirde kişi başına 6 milyon kitap olarak karşılık bulmaktadır[144].

Bilgi ve iletişim teknolojilerindeki gelişimin neticesinde, organizasyonlar ve birçok disiplinler çağın gerekliliği olarak teknoloji ile olan oryantasyona mecbur bırakılmaktadır. Dijital bilgi üretimi birçok alanda kendini göstermektedir. Bilgi ve iletişim teknolojilerinin gelişimi, elektronik devlet, elektronik demokrasi, elektronik yönetişim gibi alanların ortaya çıkmasına ve bilimsel çalışmalara yer verilmesine imkân tanımaktadır[145].

Bilgiye erişimin hızla artması ve ulaşılabilirliğini kolaylaştıran kitle iletişim araçları, bilgi ve iletişim teknolojileri çevrimiçi erişim imkanlarıyla bilgiye ulaşmak ve kaynakların artmasına olanak sağladığı gözlemlenmektedir. Toplumların refahını artırmak için devlet yöneticileri ve özel sektör yöneticileri teknolojiyi yakından takip etmektedir.

---

[143] Fadime Şimşek İşliyen, "Dijital Çağda Bilginin Değişen Niteliği ve İnfobezite: Z Kuşağı Üzerine Bir Odak Grup Çalışması", **Selçuk İletişim Dergisi**, Cilt.13, Sayı.1, 2020, s.256.

[144] İşliyen, **a.g.e.,** 2020, s.263.

[145] Salih Gümüş, Aras Bozkurt ve Erdem Erdoğdu, "**Dijital Yayıncılık ve Dijital Yayıncılık Araçları**", 1.Baskı, Anadolu Üniversitesi Yayınları, Eskişehir, 2017, ss.95-125.

Bilgiye ulaşmak ve problemlerin çözümünde kısa sürede problemi ortadan kaldırmak, bilgi ve iletişim teknolojilerinin yardımıyla hızlı ve güvenilir hale gelmektedir[146].“*Küreselleşme, dijitalleşme ve dijital bilgi toplumu temelindeki düşünceler ile yön verilen 21. Yüzyıl dünyasında eğitim sürekli öğrenmeyi, bilgi ye bilmeyi, bilgili olmayı, bilgi üretmeyi, bilgi ile yaşamayı sağlayan bir süreçtir ve bilgi toplumunda bireylerin yaratıcı sorgulayıcı düşünen ve üretebilen insanlar olmaları beklenmektedir*”[147].

Bilgiye ulaşmak için, bilgi ve iletişim teknoloji araçlarının gelişimi insanların öğrenme süreçlerinin hızlı ve güvenli olmasına imkânı tanımaktadır. Dijital bilgi çağında üretilen bilgilerin çokluğu bilgi kirliliğine neden olmaktadır. İnsanlar doğru bilgiye ulaşmak için farklı kaynaklara başvurmakta olup, bireylerin kişisel gelişimine pozitif katkılarda bulunduğu değerlendirilmektedir[148]. İnsanları araştırmaya yönlendiren bilgi üretimindeki artışın dezavantajı olarak bireylerin kişisel verilerin erişmek için casus dijital kaynakların artış göstermiş olması dezavantaj olarak bilinmektedir.

Doğru ve güvenilir bilgi kaynaklarını erişmek için güvenlik protokollerinin maksimum seviyede yerine getirilmesi gerekmektedir. Kişisel verilerin veya kurum, organizasyon verilerinin yönetiminin önemi kadar, bilgi güvenliği konusunda ayrıca önem verilmektedir. Dijital içerik ve bilgi üretmekte önemli olan, bilginin sürdürebilir bir şekilde kullanıcılar tarafından uzun zaman diliminde erişime imkân tanıması önem arz etmektedir[149]. Bilgi güvenliği, üretilen bilginin üretim aşamasında,

---

[146] Aras Bozkurt, v.d. , “Dijital Bilgi Çağı: Dijital Toplum, Dijital Dönüşüm, Dijital Eğitim ve Dijital Yeterlilikler”, **Açık Öğretim Uygulamaları ve Araştırmaları Dergisi**, Cilt.7, Sayı.2, 2021, s.39

[147] Bozkurt vd., **a.g.e.,** 2021, s.41.

[148] Bozkurt vd., **a.g.e.,** 2021, s.42.

[149] Saracel, **a.g.e.**, ss.347-356.

depolanmasında, kullanıcıların erişimi esnasında ihtiyaç duyulan dijital bilgiyi korumayı ve daha uzun süre erişime açık kalabilmesi gerekli görülmektedir[150].

Dijital bilgi, bireylerin ve küçük işletmelerin küresel kitlelere ulaşmasını ve kendinden daha büyük kuruluşlar ile rekabet etme olanağı tanımaktadır. Dijital bilgi kullanıcıları, mal veya hizmetlere ulaşmak için dijital platformlar aracılığıyla paylaşım ekonomisine dayalı modellerin gelişmesine yardımcı olmaktadır. Dijital bilgini ortaya çıkması ile çalışma ve sosyal hayatımızda elektronik postalar, kısa mesajlar, mesajlaşma uygulamaları, sosyal medya gönderileri ve iletişimi, çevrimiçi makale, elektronik kitap gibi birçok bilgiye erişmek ve etkileşim halinde bulunulmasına imkân vermektedir[151]. 21. Yüzyıl teknolojik gelişmeler ve bilgiye erişim kolaylığı ile birçok disiplinde dijitalleşme ve dijital dönüşüm çalışmaları da hız kazanmıştır. Dijital dönüşüm günümüzün kaçınılmaz bir parçası olmuş ve toplumların sosyal yaşamlarında ve kurumsal çalışma hayatına doğrudan etki ve hayatı kolaylaştıran bir etmen olmuştur.

2.3. Dijital Dönüşüm

Siyaset bilimi ve kamu yönetiminde dijitalleşme, kamu hizmetlerinin ve karar verme sürecinin geliştirilmesi, siyasetin modernize edilerek bilgi ve iletişim teknolojilerinin sosyal bilimler disiplinine entegre edilme sürecidir[152]. Yapay zekâ, veri madenciliği, büyük veri (big data) analizi ve akıllı sistemlerin bilgi ve iletişim teknolojileri vasıtalarıyla kamu yönetimi ve siyaset biliminin dijitalleşmesinde önemli rol oynamaktadır[153].

Dijital dönüşüm ile daha etkili ve verimli bir kamu yönetimine, katılımcı vatandaş ortamının oluşturulmasına, adil ve şeffaf yönetim ilkelerine, karar vericilerin

---

[150] Mehmet Oytun Cibaroğlu, "Bilgi Teknolojilerinin Bilgi Erişime Etkileri: Literatüre Dayalı Nitel Bir Çalışma", **Bilgi Yönetimi Dergisi**, Cilt.3, Sayı.1, 2020, s.15.

[151] Kumaş, **a.g.e.**, ss.691-701.

[152] Volkan Göçoğlu, "Kamu Hizmetlerinin Sunumunda Dijital Dönüşüm: Nesnelerin İnterneti Üzerine Bir İnceleme", **Manas Sosyal Araştırmalar Dergisi**, Cilt.9, Sayı.1, 2020, ss. 616-628.

[153] Göçoğlu, **a.g.e**., ss.616-628.

kararlarına doğrudan etki etmektedir[154]. Hükümetlerin politika kararlarının paylaşılması, zaman ve finansal olarak tasarruf etmek için rutin görevlerin dijitalleştirilmesi, devlet kurumları ve vatandaşlar arasındaki iletişim ve katılımı iyileştirmek için dijital dönüşüm ile verilerin toplanılması ve analiz edilmesi kamu yönetimleri ve siyaset bilimi disiplinine yardımcı olduğu bilinmektedir[155].

Siyaset bilimi ve kamu yönetimlerinin dijital dönüşüm ile birlikte gizlilik, güvenlik ve hesap verebilirlik doğrudan veya dolaylı olarak kritik etik ve politik sorunlarda ortaya çıkmaktadır. Dijital dönüşüm yöneticilerin dijitalleşme sürecinde, potansiyel riskleri ve faydaları önemli değerlendirmeleri, toplumun haklarını ve çıkarlarını korumak için muhtemel risklerin ortadan kaldırılması veya en aza indirgenmesi kritik öneme sahip olmaktadır[156]. Yöneticilerin toplum ile etkileşimi, sosyal medya ve farklı dijital platformların kullanımı, hükümet girişimleri hakkında bilgi paylaşımı ve geri bildirimleri almak için dijitalleşme güçlü bir argüman haline gelmektedir[157]. Dijital dönüşüm, devletlerin idari maliyetlerini azaltmalarına ve devlet organlarının verimliliğinin artmasına olanak tanımaktadır. Kamu yönetimi ve siyaset biliminde dijital dönüşüm ve teknoloji, vatandaşlar ile birlikte çalışma ve etkileşim kurma şeklinde günümüzde gelişime açık ve yenililerin entegrasyonu için süreklilik arz eden bir disiplindir[158].

Dijital dönüşüm, analog verilerin dijital forma dönüştürülmesi sürecinin, elektronik belge yönetim sistemleri, dijital imzalar ve elektronik iş akışlarını içeren bilgi ve iletişim teknolojilerini ifade etmektedir[159]. Siyaset disiplininde karar alıcıların

---

[154] Ahmet Özen ve Fatma Nur Gürel, "Kamu Denetiminde Dijital Dönüşüm: Dijital İkiz Yöntemi", **İzmir Sosyal Bilimler Dergisi**, Cilt.2, Sayı.1, 2020, ss.16-23.

[155] Özen ve Gürel, **a.g.e.**, ss.16-23.

[156] Lütfullah Ün, "Kamu Hizmetinde Yeni Konsept: Akıllı Kamu Hizmeti", **Bingöl Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi**, Cilt.6, Sayı.2, 2022, ss.415-440.

[157] Ayşe Asiltürk, "İşletmelerde Dijital Dönüşüm Yönetiminde Nihai Hedef: Dijital Olgunluk", **Alanya Akademik Bakış Dergisi**, Cilt.5, Sayı,2, 2021, ss.647-669.

[158] Ün, a.g.e., ss.415-440.

[159] Hüseyin Özgür ve Saynur Çicek, "Türkiye'de Kamu Yönetimi ve İşletme Eğitiminde Bilişim ve Diğer Teknolojiler: Literatür, Tarihsel Gelişim, Dersler ve Sorunlar", **Pamukkale Üniversitesi İşletme Araştırmaları Dergisi**, Cilt.8, Sayı.1, ss.1-26.

vatandaşlara ulaşmak, yeni politika ve hizmetleri sunmak için mobil uygulamaların ve e-devlet, e-demokrasi vb. gibi uygulama platformları dijital dönüşüm ile mümkün olmaktadır[160]. Başarılı bir dijital dönüşüm için yöneticilerin amaç ve hedefleri ile uyumlu stratejik yaklaşımlar gerekmektedir. Bilgi ve iletişim teknolojileri alt yapısının hazırlanması, kritik öneme sahip alan ve organların tespit edilmesi, eğitimli personel ve kaynaklara yatırımlar ile dijital dönüşüm gerçekleşebilir[161].

Dijital dönüşüm, yeni teknoloji ve süreçleri deneme isteği ve değişen teknoloji koşullarına hızla uyum sağlama yeteneği dahil olmak üzere toplumlarda kültürel bir değişimi kapsamaktadır[162]. 21. Yüzyıl'da teknoloji gelişiminin yükselişi yaşam, çalışma ve sosyo-kültürel etkileşim içinde kalma şeklinin değişimine neden olmaktadır. Dijitalleşme ile karar verme süreçlerini yönetmek ve sürekli iyileşmeyi desteklemek için büyük veri (big data), yapay zekâ, veri madenciliği, akıllı sistemler ve insansız orduların gerçek zamanlı veri analitiği ve yönetimine ihtiyaç duyulmaktadır[163].

2.4. Büyük Veri (Big Data)

Büyük veri kavramı, veri kümelerinin toplanılması, nüfus sayımları, envanter ve geleneksel yöntemler ile ortaya çıkmaktadır. Veri toplamanın sistematik hale gelmesi İngiliz istatikçi John Graunt'un ölüm faturaları üzerine doğal ve politik gözlemler ile gerçekleştirmiş olduğu çalışma veri toplama ve veri analizine yönelik ilk sistematik girişim olarak kabul edilmektedir[164]. Sanayi devrimi ile birlikte veri artışında ciddi büyüklükte veriler ortaya çıkmış olup aynı zamanda Amerika Birleşik

---

[160] Özgür ve Çicek, **a.g.e.**, ss.1-26.

[161] Zeynep Mine Alptekin, "Dijitalleşme ve Dijital Sosyal Sorumluluk İletişimi", **Uluslararası Medya ve İletişim Araştırmaları Hakemli Dergisi**, Cilt.3, Sayı.2, ss.136-155.

[162] Alptekin, **a.g.e**., ss.136-155.

[163] Thomas H. Davenport ve Thomas C. Redman, "**Dijital Dönüşüm Dört Alandaki Yeteneklere Dayanır**", Çev. Ümit Şensoy 1.Baskı, Optimist Yayın Grubu, İstanbul, 2021, ss. 227-234.

[164] Myron Gutmann, Emily Rose Merchant ve Evan Roberts, "Big Data" in Economic History", **The Journal of Economic History,** Cilt.78, Sayı.1, 2018, ss.268-299

Devletleri'nde tarımsal üretim ve satışlar ile ilgili verilerin depolanması büyük veri kavramının temelini oluşturan başlıca etmenler arasında literatürde yer almaktadır[165].

1950'lerde verilerin işlenmesi için bilgisayar maliyetlerinin yüksek olması ve yaygın kullanılmamasından dolayı veri analizlerinin bu süreçteki gelişimi daha yavaş olmuştur. 1990'lı yıllarda internetin etkin olarak kullanılmaya başlanılması ile World Wide Web 'in (www) ortaya çıkışı, bireysel ve kuruluşların veri üretmesi ve veri üretiminin yaygınlaşması veri kümelerinde ciddi artışları beraberinde getirmiştir[166]. Büyük veri kümelerinin kontrol ve analiz edilmesi aynı zamanda saklanılması bilgisayar ve veri tabanlarında depolanmaya başlanılmıştır.

Büyük veri (big data), geleneksel veri işleme teknikleri ile yönetilmesi ve kontrolü zor olan büyük ve karmaşık veri kümelerinin bütünsel olarak ifade edilmesidir[167]. Bilgi ve iletişim teknolojileri ve internet ağlarının gelişimi hızlı kullanımı ile büyük veri gün geçtikçe yaygınlaşmaktadır. Büyük veri kavramı 21. Yüzyılın ilk yıllarında ortaya çıkmış olup, 19. Yüzyılın ortalarında ABD hükümeti, toplum sağlığını ve refahını takip etmek için büyük miktarda veri toplamaya başlamıştır[168]. Toplanan veriler geleneksel yöntemler ile kâğıt üzerinde arşivlenmekte iken ilerleyen zamanlarda dijital disklere aktarılmıştır. Büyük verinin geleneksel veri toplama yeteneklerinin, bilgi ve iletişim teknolojilerindeki gelişmeleri ile birlikte bilgisayar vasıtasıyla veri toplama ve depolama işlemleri gerçekleştirilmiştir[169].

1990'lı yıllarda internet kullanımı yaygınlaşmaya başlaması ile toplanan ve üretilen veri büyüklüğünde afaki artışlar yaşanmıştır. Özel kuruluşların müşterileri hakkında elde ettikleri büyük veri kümeleri, pazarlama kampanyaları ve müşteri

---

[165] Gutmann, Merchant ve Roberts, **a.g.e.,** ss.268-299

[166] Hüseyin Avunduk ve Merve Kızgın, "Büyük Veri ve Sürekli Denetimde Veri Analizi", Journal of Business in The Digital Age, Cilt.3, Sayı.1, 2020, ss.76-83.

[167]Narmatha Pandian, "The Big Data to Innovative in Education", https://www.researchgate.net/publication/370155713 , (Erişim Tarihi:21.03.2023).

[168] Mounir M.El Khatib, Humaid Al Shehhi ve Mohammed Al Nuaimi, "How Big Data and Big Data Analytics Mediate Organizational Risk Management", **Journal of Financial Risk Management**, Cilt.12, Sayı.1, 2023, ss.1-14

[169] Ali Özcan, "Büyük Veri: Fırsatlar ve Tehditler", **Trt Akademi**, Cilt.6, Sayı.11,2021, ss.12-30

hizmetlerini iyileştirmek için stratejiler uygulanmaya başlanılmıştır. Büyük veri kümelerini yönetmek için veri ambarı kavramı yani veri tabanları dahil olmak üzere farklı kaynaklardan verilerin toplanılması ve depolanması işlemleri ortaya çıkmaktadır[170]. Büyük veriler, erişilebilir ve analiz edilebilir hale geldikten sonra özel işletmelerin ve topluma faydalı kuruluşların bilgi edinmek için veri ambarlarından faydalandığı bilinmektedir. 21. Yüzyıl'da bilgi ve iletişim teknolojilerindeki gelişmeler ile özel yazılım şirketleri mühendisleri tarafından büyük veriyi yönetmek için "hadoop" ismindeki yazılım ile büyük veri kümelerini yöneten sistemler geliştirilmiştir[171]. Hadoop sistemi, büyük veri kümelerini geleneksel veri işleme teknikleri kullanarak, geleneksel yöntemler ile işletilmesi mümkün olmayan büyük veri kümelerini işlenebilir hale getirmektedir. Açık kaynak veri tabanlarının programlama modelleri ile devletlerin ve özel şirketlerin büyük veri kümelerini birden fazla sunucuda saklayabilmesi ve işlenebilmesine hadoop sistemi gibi yazılımlar öncü olmuştur[172].

Büyük veri, iş dünyasında işletmelerin çalışma şeklini büyük veri kümelerinin analiz edilmesi ile müşteri yönelimleri, pazar eğilimleri hakkında öngörüler sunmaktadır. İş dünyasının büyük veri kümeleri ile ürünleri, hizmetleri ve pazarlama stratejilerini belirlemesinde ve geliştirilmesinde doğrudan katkı sağlamaktadır.

Küresel anlamda büyük veri, hükümetler tarafından kamu hizmetlerini ve politikalarını iyileştirmek için tercih edilmektedir. Büyük veri aracılığıyla veri analizi ve suç oranlarının yüksek olduğu bölgeleri belirlemek için büyük veri ile devlet arasındaki ilişkiyi ortaya koyan örnek çalışmalar arasında yer almaktadır[173]. Devlet yönetimindeki uygulamalardan bir diğeri sağlık hizmetlerinde büyük veri kümelerinin analiz edilerek hastalık teşhisleri ve tedavi yöntemleri hakkında kıymetli bilgiler elde edilmektedir. Büyük veri kümeleri kamu hizmetleri, sosyal politikalar ve uluslararası

---

[170] Avunduk ve Kızgın, **a.g.e**., ss.76-83.

[171] A. Mcafee ve E. Brynjolfsson, "Big Data: The Management Revoluiton", **Hardvard Business Review**, Vol.90, Issue. 10, 2012, ss.60-68

[172] Khatib vd. , **a.g.e**., ss.1-14

[173] J. Manyika ve diğerleri, "Big Data : The Next Frontier For İnnovation, Competition and Productivity", **McKinsey Global Institute**, Cilt.1, Sayı.4, ss.1-25

politikaların belirlenmesinde yöneticilere ve vatandaşlara doğrudan katkı sağlamaktadır[174].

Büyük veri birçok endüstrinin aynı zamanda hükümetlerin kritik bir bileşeni olarak iyi kararlar alınmasına ve sonuçların iyileştirilebilmesine yardımcı olmaktadır. Teknoloji çağında dijital verilerin büyümesi bilgi ve iletişim teknolojiler ve algoritmalar kullanarak büyük verilerden değerli öngörülerin çıkması sağlanmaktadır. Büyük veri kümeleri hacmi, farklılığı ve hızı ile karakterize edilmektedir. Teknolojik gelişmeler ile gün geçtikçe veri artışının önü kesilemez hale gelmekte günümüzde yaklaşık olarak günlük iki buçuk kentilyon byte veri üretildiği açık kaynak erişimlerde ortaya çıkmaktadır[175]. Büyük veri, yapılandırılmış ve yapılandırılmamış veriler metin, ses, multimedya, resimler ve daha fazlası sosyal medya uygulamaları, çevrim içi platformlar ve farklı kaynaklardan olmak üzere veri çeşitliliğini kapsamaktadır. Büyük veri de veri hızı gerçek zamanlı ve yaklaşık gerçek zamanlı veri işleme gerektiren büyük veri kümelerinin üretilmesi ve işlenmesini ifade etmektedir[176]. Büyük veri kümelerinin bilgi ve iletişim teknolojileri ile bir araya gelmesi neticesinde yapay zekâ uygulamaları, veri komisyonculuğu, veri madenciliği, blok zinciri ve otonom sistemler ortaya çıkmaktadır.

2.5. Yapay Zekâ (AI)

Yapay zekâ, mantıksal akıl yürütme yöntemini kullanarak karmaşık işlemlerin gerçekleştirilmesi için makineler yardımıyla bilginin temsil edilmesi, karmaşık işlemlerin çözümlenmesi ve problemlerin ortadan kaldırılması için mantıksal işlemlerin belirli bir düzende kullanılmasını ifade etmektedir[177]. 20. Yüzyıl ortalarında

---

[174] Zübeyir Özçelik ve Ebru Aykan, "Sosyal Bilimlerde Büyük Veri Kullanımı, Veri Toplamada Akademik Çalışmalara Ne Tür Kolaylıklar Sağlayabilir?", **Anadolu Üniversitesi Sosyal Bilimler Dergisi,** Cilt.20, Sayı.3, 2020, ss.131-142

[175] B. Kao ve C. Tseng, "Big Data And Artificial İntelligence For Supply Chain Management: A Review and Future Research Directions", **International Journal of Production Research**, Cilt.60, Sayı.2, 2022, 618-639

[176] Özçelik ve Aykan, **a.g.e**., ss.131-142.

[177] Eric Brynjolfsson ve Andrew McAfee, "Yapay Zekânın Vaat Ettikleri", **Harvard Business Review Press Artificial Inteligence** , Ed. Utku Umut Bulsun, Çev. Levent Göktem, 1.Baskı, Optimist Yayın Grubu, 2020, ss.19-56

önceden tanımlanmış kuralları uygulamak yerine veri kümelerinden elde edilebilecek makine öğrenimi algoritmalarının gelişimi ile ortaya çıkmıştır. 1990'lı yıllarda internetin geliştirilmesi ve artan bilgisayar kullanımı büyük veri kümelerinin işlenmesi ve analizi sonucunda geliştirilen algoritmalar ile büyük veri kümelerinin makineler aracılığıyla problem çözme ve endüstriyel üretimi destekleyici uygulamalar kullanılmaya başlanılmıştır[178].

21. yüzyıl başlarında yapay zekâ, yazılım dili, bilgisayar merkezli makineler, robotik kodlamalar ve uygulamaları gibi farklı alanlarda yeniliklerin ortaya çıkmasına katkılar sağlamıştır. Büyük veri kümelerinin etkin ve insansız olarak kontrol edilmesi neticesinde faydalı bilgilerin endüstriyel üretimde ve sosyal yaşamda bilgi ve iletişim teknolojileri vasıtasıyla kullanımı artmaktadır[179].

Yapay zekâ uygulamaları, büyük veri kümeleri üzerinden sembolik akıl yürütme algoritmalarını kullanarak problem çözme odaklı geliştirilmektedir. Yapay zekâ uygulamaları insan uzmanlığı gerektiren karar verme ve problem çözmek için belirli kurallar çerçevesinde kodlamayı içeren kural tabanlı sistemlerden oluşmaktadır[180]. Yapay zekâ çalışmaları, belirli disiplinlerde profesyonel insan yeteneklerinin karar verme sürecini taklit etmek için tasarlanmış ve teknolojik gelişmeler ile insan fonksiyonları daha geri planda kalmıştır.

Günümüzde yapay zekâ uygulamaları, insanlar gibi düşünmek ve hareket etmek için algoritmalar ile programlanmış makinelerde insan zekasının simülasyonunu olarak ifade edilmektedir. Geliştirme sürecinde, deneyimden öğrenme,

---

[178] Vikram Mahidhar ve Thomas H. Davenport, "Yapay Zekaya Geçmek İçin Beklemeyi Tercih Eden Şirketler Treni Neden Yakalayamayabilir?", **Harvard Business Review Press Artificial Inteligence** , Ed. Utku Umut Bulsun, Çev. Levent Göktem, 1.Baskı, Optimist Yayın Grubu, 2020, ss.91-106.

[179] Emma Martinho-Truswell, "Teknik Ekipten Olmayan Çalışanların Yapay Zeka Hakkında Yanıtlayabilmesi Gereken 3 Soru", **Harvard Business Review Press Artificial Inteligence** , Ed. Utku Umut Bulsun, Çev. Levent Göktem, 1.Baskı, Optimist Yayın Grubu, 2020, ss.107-118.

[180] Mahidhar ve Davenport, **a.g.e**., ss.91-106.

kalıpları tanıma, karar verme ve günlük yaşamın her disiplininde bilgi ve iletişim teknolojilerini içermekte ve yapay zekanın ana omurgasını oluşturmaktadır[181].

Yapay zekâ uygulamaları, sağlık, finans, ulaşım, eğlence ve gündelik yaşamın verimli ve şeffaf çerçevede eğitim ve üretim modelleri üzerindeki çalışmalar ile daha basit ve daha az insan gücünün kullanıldığı ve gün geçtikçe kendini yenileyen teknolojileri kapsamı içerisinde yer almaktadır.

Yapay zekâ uygulamalarına örnek olarak deneyimleri kişiselleştirmek için bir insanın tercihleri, davranışı ve geçmiş yaşamı hakkında verileri analiz ederek bir e-ticaret sitesinde kişiselleştirilmiş önerileri, geçmiş alışveriş verilerini, araştırma tercihlerine dayalı ürünleri ön plana çıkartmaktadır[182]. Aynı şekilde kişisel sağlık verilerinin mobil cihazlar ve aplikasyonlar aracılığıyla analiz ederek, doktorların erken teşhis ve tanı koymalarına yanı sıra pratik tedavi imkanları sunabilme yeteneği, insan yaşamını kolaylaştıran ve yardımcı unsurlar arasında yapay zekâ uygulamaları yer almaktadır[183].

Yapay zekâ, deneyimlerin kişiselleştirilmesi, sağlığın gelişimi ve takibi, müşteri hizmetlerinin ve iş süreçlerinin geliştirilmesini doğrudan desteklemektedir[184]. Yapay zekâ uygulamaları ile hayatımızın birçok alanında yeniliklere ve farklı disiplinlerde kritik öneme sahip yenilikler sağlama potansiyeli bulunan uygulamaları içermektedir. Günlük hayatta konuşmaları tanımak, görüntüleri yorumlamak ve karar verme gibi insan zekâsı gerektiren görevleri yerine getirebilen algoritma ve sistemler

---

[181] Ng Andrew, "İlk Yapay Zekâ Projenizi Nasıl Seçmelisiniz?", **Harvard Business Review Press Artificial Inteligence** , Ed. Utku Umut Bulsun, Çev. Levent Göktem, 1.Baskı, Optimist Yayın Grubu, 2020, ss.127-140.

[182] H.James Wilson ve Paul Daugherty, "İşbirliğine Dayalı Zekâ: İnsan Ve Yapay Zekâ Güçlerini Birleştiriyor", **Harvard Business Review Press Artificial Inteligence** , Ed. Utku Umut Bulsun, Çev. Levent Göktem, 1.Baskı, Optimist Yayın Grubu, 2020, ss.169-206.

[183] Wilson ve Daugherty, a.g.e., ss.169-206.

[184] H.James Wilson, Paul Daugherty ve Chase Davenport "Yapay Zekanın Geleceğinde Verinin Yeri Daha Fazla Değil Daha Az Olacak", **Harvard Business Review Press Artificial Inteligence** , Ed. Utku Umut Bulsun, Çev. Levent Göktem, 1.Baskı, Optimist Yayın Grubu, 2020, ss.229-242.

geliştirmeye odaklanan yapay zekâ uygulamaları bilgi ve iletişim teknolojileri disiplini olarak nitelendirilmektedir[185].

2.6. Veri Madenciliği ve Veri Komisyonculuğu

Veri madenciliğinin temelleri büyük veri kümelerinin istatistiksel yöntemler ile gerçekleştirilen uygulamaları içermektedir. Bilgi ve iletişim teknolojilerinin yeni ortaya çıktığı 1950'li yıllardan önce veri madenciliği istatistikçiler ve matematikçiler tarafından gerçekleştirilen geleneksel yöntemleri ile veri analizinin yapılmasına dayanmaktadır[186].

1970'li yıllardan sonra teknolojik gelişmelerin hızlanması ile geliştirilen algoritmalar ve bilgi ve iletişim teknolojilerinin kullanımı veri madenciliği kavramının ortaya çıkmasına sebep olmuştur[187]. 20. Yüzyılın ikinci yarısındaki teknolojik gelişmeler veri madenciliğinin ile ilgili birçok yöntemin ortaya çıkmasına, karar ağaçları, kümeleme ve ilişkilendirme gibi teknikler kullanılarak veri toplama ve analiz işlemleri gerçekleştirilmektedir. 1990'lı yıllarda bilgisayar ağ teknolojilerindeki gelişmeler ve internet kavramının ortaya çıkması ile büyük veri kümelerinin kontrolü tamamen bilgisayarlar ve sunucular üzerinde depolanmasına olanak tanımıştır[188]. Bilgisayar ve internet kullanımdaki hızlı artış, veri tabanlarında büyük veri kümelerinin depolanması ve işlenmesi, veri madenciliğini finans, pazarlama ve kamusal faaliyetlerdeki uygulamaların ortaya çıkmasına olanak tanımaktadır[189]. Büyük veri kümelerinin çoğalması ile bulut bilişim teknolojilerinin kullanabilir olması özel şirketler ve kamu yönetimlerinde değerli verilere erişme çabaları veri

---

[185] Wilson, Daugherty ve Davenport, **a.g.e**., ss.229-242.

[186] Joseph M. Woodside, "Bemo: A Parsimonious Big Data Mining Methodology", **Online Academic Journal of Infortmation Technology**, Cilt.7, Sayı.24, 2016, ss.114-123.

[187] Frans Coenen, "Data Mining: Past,Present and Future", **The Knowledge Engineering Review,** Cilt.26, Sayı.1, 2011, ss.25-29.

[188] Coenen, **a.g.e.,** ss.25-29.

[189] Serkan Savaş, Nurettin Topaloğlu ve Mithat Yılmaz, "Veri Madenciliği ve Türkiye'deki Uygulama Örnekleri", **İstanbul Ticaret Üniversitesi Fen Bilimleri Dergisi**, Cilt.11, Sayı.21, 2012, ss.1-23.

madenciliğinin gelişmesine katkı sağlamıştır[190]. Genel olarak veri madenciliği büyük ve karmaşık veri kümelerinin tespit ve analiz etme süreçlerini kapsamaktadır.

Veri madenciliği, çeşitli hesaplama tekniklerini kullanarak, büyük veri kümelerinde yer alan kalıpları ve öngörüleri keşfetme sürecini ifade etmektedir. Veri madenciliğinin amacı, ham verilerden faydalı verileri ayıklamak ve anlamlı bir bütüncül ifadenin oluşturulmasına imkân sunmaktır[191]. Veri madenciliği ile analiz sonucunu birden fazla boyutta keşif yaparak tek bir perspektifte anlam ifade etmeyen veri kümelerini anlaşılabilir bir bilgi oluşturulmasına yardımcı olmaktadır. Veri madenciliği, tespit ve analiz için büyük ve karmaşık veri kümelerinin dönüştürülmesi ve hazırlanmasını sağlamaktadır. Büyük veri kümelerinde yer alan verilerin ilgili konulara göre seçilmesi, gürültülü ve karmaşık verilerin temizlenmesi, eksik verilerin tamamlanması ve büyük veri kümelerinden anlaşılabilir bilgi hazırlanması sürecindeki tüm veri işleme tekniklerini kapsamaktadır[192].

Veri madenciliği uygulamaları, iş dünyasında ve kamu yönetimlerinde karar verme süreçlerinin desteklenmesi için öngörüler sunabilmektedir. Özel işletmeler ve kamu yönetimlerinde yöneticilere ve kullanıcılara direkt olarak katkı sağlayabilmektedir[193]. Veri madenciliği uygulamaları, genel insan davranışındaki kalıpları tespit etmek ve sahtekarlığın ortaya çıkmasına yardımcı olarak yönetim süreçlerini optimize etmek ve veri odaklı kararlar alınması ve politikalar oluşturulmasında kritik öneme sahip bir süreci ifade etmektedir[194].

---

[190] Savaş, Topaloğlu ve Yılmaz, **a.g.e**., ss.1-23.

[191] Dönüş Şengür ve Songül Karabatak, "Data Mining Techniques Based Students Achievements Analysis", **Turkish Journal of Science & Technology**, Cilt.13, Sayı.2, 2018, ss.53-59.

[192] Cenk Akkaya ve Ceren Uzar, "Data Mining and Application Of It To Capital Markets", **International Journal Of Economics and Finance Studies**, Cilt.3., Sayı.2, 2011, ss.58-67.

[193] Ahmed Ragab, Soumaya Yacout ve Mohamed-Salah Ouali, "Intelligent Data Mining for Automatic Face Recognition", The Online Journal of Science and Technology, Cilt.3, Sayı.2, 2013,ss.97-101.

[194] Abdullahi Sidow Osman, "Data Mining Techniques:Review", **International Journal of Data Science Research**, Cilt.2, Sayı.1, 2019, ss.1-4.

Veri madenciliği kavramı ile birlikte veri komisyonculuğu (data broker) kavramı da ortaya çıkmaktadır. Veri komisyonculuğu, sosyoloji analizi için toplumsal verilerin toplanılması, ticari çıkarlar doğrultusunda toplanan verilerin pazarlanması anlamını ifade etmektedir[195]. Veri komisyoncuları bireylerin ve toplulukların sosyal medya platformlarında yer alan kullanıcı profillerinden, açık kaynak veri tabanlarından ve çevrimiçi her türlü kaynaklardan kişisel ve kurumsal verileri toplamaktadır. Elde edilen bilgilerin reklam ve pazarlama stratejilerinin oluşturulmasında, toplanan verilerin işletme hedeflerini gerçekleştirmek ve ticari kazanç sağlamak için kullanıldığı bilinmektedir[196]. Veri komisyonculuğu, bilgi ve iletişim teknolojilerindeki hızlı gelişmeler neticesinde sosyal medya ve internet sunucularından verilerin toplanılması ve analiz sürecini hızlandırmakta ve bilgiye erişim imkanlarını kolaylaştırmaktadır. Veri brokerleri gizlilik ve şeffaflık konusunda endişelerin ortaya çıkmasına neden olup güven konusunda toplumda tedirginliğe neden olmaktadır[197]. Toplumlarda birçok insan, hakkında toplanılan verilerin farkında değildir ve bu verilerin nasıl ve hangi amaçlar doğrultusunda kullanıldığı konusunda çok az bilgiye sahiptirler.

Veri komisyonculuğu uygulamaları, sağlık kayıtları, finansal bilgiler, kişisel verileri ve kamusal verilere erişebilirliği mümkün kılmaktadır[198]. Kişisel verilerin, kişilerin bilgisi ve rızası olmadan pazarlama amaçlı reklam şirketlerine satılmasına olanak tanıyan veri komisyonculuğu endişelerin artmasına sebep olmaktadır[199]. Veri komisyoncularının dezenformasyonun yayılmasına katkı sağladığı düşünülmekte, yanlış ve yanıltıcı bilgilerin topluma yayılması ve algı yönetimine olanak sunmaktadır[200]. Özetle veri madenciliği ve veri komisyonculuğu, kişisel verilerin

---

[195] Hyeontaek Oh ve diğerleri, "Personal Data Trading Scheme for Data Brokers in IOT Data Marketplaces", **IEEE Access Open Access Journal**, Cilt.7, Şubat 2019, ss.40120-40132.

[196] Zeynep Küçükkıralı ve Kerim Eser Afşar, "Dijital Verinin Finansallaşması ve Platform Kapitalizmi", **Marmara Üniversitesi Öneri Dergisi**, Cilt.17, Sayı.58, 2022, ss.665-690.

[197] Justin Sherman, "Data Brokers and Sensitive Data on U.S. Individuals", https://techpolicy.sanford.duke.edu/wp-content/uploads/sites/4/2021/08/Data-Brokers-and-Sensitive-Data-on-US-Individuals-Sherman-2021.pdf , (Erişim Tarihi: 27.03.2023).

[198] Küçükkıralı ve Afşar, **a.g.e**, ss. 665-690.

[199] Küçükkıralı ve Afşar, **a.g.e**, ss. 665-690.

[200] Sherman, **a.g.k.**

toplanılması ve analiz edilerek toplanan veriler üzerinden ticari kazanç ve menfaat sağlamayı ifade etmektedir. Veri madenciliği ve veri komisyonculuğu kavramlarından anlaşılacağı gibi bilgi güvenliği ve elektronik harbin önemi yanı sıra elektronik harp çatısı altında kişisel verilerin korunmasının önemi ve elektronik harp konusunda çalışmalara ihtiyaç duyulmaktadır.

2.7. Blok Zinciri (Blockchain)

Blok zinciri, merkezi bulunmayan dijital bir defter olarak bilgilerin depolanması, bilgiyi paylaşmak ve işlemek maksadıyla bilgisayar ağları aracılığıyla veri tabanlarında bilginin yer alma süreci olarak nitelendirilmektedir[201]. Elde edilen ve işlenen verilerin, her bloğun bir listeye göre içeriklerinin bulunduğu bir dizi bloklardan meydana gelmektedir. Blokların tümü birbiriyle ilişkili ancak sonraki bütün blokları değiştirmeden önceki blokların değiştirilmesine olanak tanımayan sisteme blok zinciri denilmektedir[202]. Blok zinciri merkezi olmayan bir sistem olmasından dolayı güvenirliği sorgulanan fakat internet ağında gerçekleşen bütün işlemlerin değiştirilemez olması ve tehditlere karşın güçlü bir güvenlik kaydı yapılmaktadır[203].

Blok zinciri bütünlüğünün korunması, bankalar veya hükümetler gibi merkezi bir otoriteye güvenilmesi yerine, blok zinciri uygulamalarını kapsayan bir teknoloji ağı tarafından güvenlik endişelerini ortadan kaldırmaktadır[204]. Bütünlüğün sağlanması ve korunması işlemi, blok zincirinde bulunan verilerin manipüle edilmesini güçlendirmekte, sistem içerisindeki verilerin manipüle edilebilmesi için, internet ağındaki bilgi işlem gücünün büyük bir kısmını kontrol edilmesi gerekiyor fakat blok

---

[201] Marcon Iansiti ve Karim R. Lakhani, "Blok Zinciri Hakkındaki Gerçekler", **Harvard Business Review Press Blockchain** , Ed. Çiğdem Zeynep Aydın, Çev. Taner Gezer, 1.Baskı, Optimist Yayın Grubu, 2019, ss.19-52.

[202] Iansiti ve Lakhani, **a.g.e.,** ss.19-52.

[203] Vinay Gupta, "Blok Zincirinin Kısa Tarihi", **Harvard Business Review Press Blockchain** , Ed. Çiğdem Zeynep Aydın, Çev. Taner Gezer, 1.Baskı, Optimist Yayın Grubu, 2019, ss.53-60.

[204] Catherine Tucker, "Blok Zinciri ve Veri Bütünlüğü Devrimi", **Harvard Business Review Press Blockchain** , Ed. Çiğdem Zeynep Aydın, Çev. Taner Gezer, 1.Baskı, Optimist Yayın Grubu, 2019, ss.9-18.

zinciri sisteminde böyle bir durum neredeyse imkânsız olduğu değerlendirilmektedir[205].

Blok zincirinde bir işlem sisteme kaydedildikten sonra değiştirilmesi veya silinmesi mümkün olmamakla birlikte, bu durumun sebebi ise zincirdeki her bloğun blok kapsamının parmak izi olan benzersiz ve çözülmesi güç bir algoritma ile şifrelenmesidir[206]. Blok zinciri sistemi içerisinde bütün güvenlik önlemlerine karşın bir bilgi değiştirilir ise sistem içindeki algoritmanın farklı olmasından dolayı blok zinciri geçerliliğini kaybetmesine yönelik bir sistem oluşturulmaktadır. Geçerliliğini kaybeden blok veya bloklar zincirin tamamının geçersiz olmasına olanak tanıyarak yüksek güvenlik sağlanmaktadır[207].

Blok zinciri, merkezi olmayan, güvenli ve şeffaf olmasından kaynaklı finansal işlemler, tedarik zinciri yönetimi, kimlik doğrulama, akıllı kentler ve sistemler gibi farklı sektör uygulamaları ile ideal bir çözüm haline gelmektedir[208]. Dünya üzerinde öncelikle kripto paraların temelini oluşturan blok zinciri birçok akıllı kent uygulamalarının başrolünde yer almaktadır.

Günümüzde devletlerin ve finans dünyasının büyük veri yığınları içerisinde bilgi harbinin yaşanması orijinal ham verileri gerek devlet yönetimlerinde gerekse iş dünyasında menfaatler doğrultusunda kullanılmak istenilmektedir[209]. Şeffaf ve güvenilir bir şekilde blok zinciri sistemi içerisinde yer alan büyük veri kümeleri, blok zinciri sistemi içerisinde topluma ve paydaşlara açık olarak güvenilir şekilde kalıcı olması sağlanmaktadır.

---

[205] Allison Berke, "Blok Zincirleri Ne Kadar Güvenli", **Harvard Business Review Press Blockchain** , Ed. Çiğdem Zeynep Aydın, Çev. Taner Gezer, 1.Baskı, Optimist Yayın Grubu, 2019, ss.83-94.

[206] Berke, **a.g.e**., ss.83-94.

[207] Berke, **a.g.e**., ss.83-94.

[208] Brian Forde, "Blok Zincirinin Kamusal Verilerin Kamuya Açılması Amacıyla Kullanılması", **Harvard Business Review Press Blockchain** , Ed. Çiğdem Zeynep Aydın, Çev. Taner Gezer, 1.Baskı, Optimist Yayın Grubu, 2019, ss.189-200.

[209] Forde, **a.g.e.**, ss.189-200.

Blok zinciri sistemi içerisine kaydedilen verilerin künyelerini toplum paydaşları rahatlıkla ulaşabilir ve dezenformasyonun önüne geçilmesine katkı vermektedir[210]. Kamu yönetimlerinde ve iş dünyasında blok zincirinin kullanılması kişisel ve kurumsal verilerin korunmasına ilişkin endişelerin ortadan kalkmasına, gelişen bilgi ve iletişim teknolojileri sayesinde verilerin etkin olarak kullanılmasına olanak tanımaktadır. Devletlerin kamu yönetimlerinde ve uluslararası ilişkiler politikalarının belirlenmesinde ve bu politikaların kalıcı olarak bir sistem içerisinde saklanılması ve erişime açık olması şeffaf bir yönetim sistemini blok zinciri ile sağlamak mümkündür.

2.8. Akıllı Sistemler

Teknoloji çağının sonuçları arasında yer alan akıllı sistemler günlük yaşamı kolaylaştırarak uzaktan komuta ve kontrol işlemlerinin gerçekleşmesine olanak tanımaktadır[211]. Akıllı sistemler, kentlerimiz, evlerimiz ve iş yerlerimize kadar günlük yaşamımızda daha çok yer almaya başlamaktadır.

Akıllı ev sistemleri, basit gündelik yaşam formlarının otomatikleşerek konut ortamında kolaylıklar sağlamaktadır. Akıllı ev sistemlerinde, aydınlanma ve elektrik kontrolü, ısı ve havalandırma kontrolü ve güvenlik tedbirleri birbiri ile ilişkili olan elektronik ve mobil cihazlar ile gerçekleştirilmektedir[212]. Akıllı aydınlanma sistemleri bir mobil cihaz uygulaması aracılığıyla sesli komut veya manuel olarak evinizde bulunan aydınlatma ve elektrik sistemlerini kontrol edilmesine olanak tanımaktadır[213]. Akıllı ev sistemleri ile doğrudan açma veya kapama yanı sıra zaman ayarlı komutlar

---

[210] Michael Mainelli "Blok Zinciri Dijital Dünyada Kimliğimizi Kanıtlamamıza Yardımcı Olacak", **Harvard Business Review Press Blockchain** , Ed. Çiğdem Zeynep Aydın, Çev. Taner Gezer, 1.Baskı, Optimist Yayın Grubu, 2019, ss.201-212.

[211] Afad Hyder Chohan, ve diğerleri, "Development of Smart Application for House Condition Survey", **Ain Shams Engineering Journal**, Cilt.13, Sayı.3,2022, ss.1-9

[212] Muammer Akçay, Mehmet Canbaz ve Muhemmet Ömer Diş, "Akıllı Konut Uygulaması", **Estudam Bilişim Dergisi,** Cilt.3, Sayı.1, 2022, ss.1-5

[213] Dmitriy Andreev, "The "Smart City" Consept and it's Implementation Prospects", Ural Environmental Science Forum "Sustainable Development of Industrial Region", 31.May 2023,

M. K. Ammosov North-Eastern Federal University, Department of Technosphere Safety, Yakutie Russia ,2023, ss.1-6

ile gerçekleştirilmesi mümkün olmaktadır. Akıllı ev sistemlerinde ısı ve havalandırma kontrolü için elektronik sensörler ve termostat aracılığıyla uzaktan komuta ve kontrol yazılımları ile evin ısısı ve havalandırılması gerçekleştirilmektedir[214]. Aynı zamanda güvenlik problemlerini ortadan kaldırmak için güvenlik kamera ve alarm sistemleri sayesinde evlerin izlenilmesi ve her türlü tehdide karşın erken ikaz sistemlerini mobil cihazlar ile gerçek zamanlı kontrol edilmektedir[215].

Teknoloji çağında geliştirilen akıllı sistemler, şehirler arası ve şehir içi ulaşımda verimliliği arttırmak ve konforlu seyahat edebilmek için akıllı ulaşım sistemleri yaşamımızı kolaylaştırmaktadır. Şehirler arası ve şehir içi ulaşımda akıllı sistemlerin gerçek zamanlı bilgi ve trafik akışını iyileştirmek maksadıyla küresel konumlama sistemi (GPS) ve gelişmiş teknolojilere yer vermektedir[216]. Akıllı ulaşım sistemleri, gerçek zamanlı trafik kontrolünü optimize etmek ve vatandaşların trafikte güvenli bir şekilde seyahat etmelerini sağlamak için küresel konumlama sistemleri, elektronik sensörler ve kameraların birbirleri ile bağlantılı ve senkronize olacak şekilde müşterek bir uygulamada kullanılmasına olanak tanımaktadır[217]. Şehirleri arası ve şehir içi seyahatlerde yol koşulları, hava durumu ve trafik yoğunluğu hakkında gerçek zamanlı bilgi akışı akıllı ulaşım sistemleri ile kullanıcılara sunulmaktadır. Günümüzde artan nüfus yoğunluğu ve araç sayısındaki yükselişler kentlerde otopark sorunu ortaya çıkartmakta olup, müsait park yerlerinin tespiti ve ulaşılmak istenilen hedef konumundaki park durumu hakkında bilgi sağlayarak, otopark ödemelerinin internet bankacılığı ile gerçekleştirilmesine ve insanların zamandan tasarruf etmeleri akıllı ulaşım sistemleri ile imkân verilmektedir[218].

---

[214] Melek Tomaş ve Neslihan Dostoğlu, "Yapay Zekaya Sahip Akıllı Evler", **Avrupa Bilim ve Teknoloji Dergisi**, Cilt.1, Sayı.18, 2020, ss.486-493

[215] İsa Avcı, "Akıllı Evlerde IoT Teknolojileri ve Siber Güvenlik", **Avrupa Bilim ve Teknoloji Dergisi**, Özel Sayı.34, 2022, ss.226-233

[216] Razaman Şengül ve Hande Yüksel Altınbaş, "Akıllı Kentin Bir Bileşeni Olarak Akıllı Ulaşım Uygulamalarının İncelenmesi: Kocaeli Büyükşehir Belediyesi Örneği", **Uluslararası Kültürel ve Sosyal Araştırmalar Dergisi,** Cilt.6, Sayı.2, 2020, ss.487-502

[217] Şengül ve Yüksel Altınbaş, **a.g.e.**, ss.487-502

[218] Zekeriya Bilici ve Veysel Babahanoğlu, "Akıllı Kent Uygulamaları ve Konya Örneği", **Akademik Yaklaşımlar Dergisi**, Cilt.9, Sayı.2,2018, ss.124-139

21. yüzyılda gerçekleştirilen teknoloji devrimleri ile sağlık sistemlerinin bilgi ve iletişim teknolojileri kullanarak sağlık hizmetleri sonuçlarını ve hasta tecrübelerini iyileştirmek ve geri bildirimler ile şeffaf bir sağlık yönetimi sağlanmaktadır. İnsan hayatının erken teşhis ve zamanın kritik önemi ile akıllı sağlık uygulamaları, kişisel sağlık kontrolü ve kaliteli hizmetler sunulabilmesi için elektronik sağlık uygulamalarına daha çok yer verilmektedir[219]. Kişisel sağlık verileri cep telefonları ve akıllı saat gibi elektronik cihazlar ile giyilebilir bilgi ve iletişim teknolojileri fiziksel aktiviteleri, kalp atış hızı, uyku düzeni ve hareket verilerini kayıt altına alarak bireysel sağlık kontrolüne fayda sağlamaktadır[220].

Bilgi ve iletişim teknolojileri birçok endüstrilerde kullanılmakta olup günlük hayatımızın bir parçası olan otomobillerde artık elektronik sensörler ve teknolojiler ile donatılmaktadır[221]. Akıllı otomobil ve ticari amaçlı kullanılan kara araçlarının güvenlik ve kişiselleştirilmiş performansı bilgi ve iletişim teknolojileri, elektronik sensörler ve elektronik komuta ve kontrol panelleri ile hız sabitleme, otoyol şerit çizgisi takip kontrol sistemleri, acil ve otomatik frenleme, seyir halinde kör noktaların takibi, yağmur ve park sensörleri gibi birçok teknoloji senkronize bir şekilde çalışmaktadır[222]. Akıllı otomobiller gelişmiş güvenlik paketleri, yapay zekâ uygulamaları ve sesli komutlar ile kontrol edilerek, performans ve yakıt tüketiminde verimliliği ön plana çıkması gibi özelliklerinden dolayı tercih edilmesi gün geçtikçe artmaktadır.

Akıllı kentler, ulaşım, enerji, iletişim ve yönetim faaliyetler gibi çeşitli hizmetleri bilgi ve iletişim teknolojilerini kullanarak hayatımızda yer alan akıllı sistemlerden bir diğeridir[223]. Akıllı kentler, kent sakinlerinin yaşam kalitesini ve refahını arttıran teknoloji çağı şehirleşme ve yerel yönetimler konseptidir. Akıllı

---

[219] Arzu Yıldırım, "Kamu Yönetiminde Sağlık Politikalarındaki Dönüşüm: E-Sağlık Uygulamaları", **Kuram ve Uygulamada Sosyal Bilimler Dergisi**, Cilt.6, Sayı.2, 2022, ss.125-140

[220] Yıldırım, **a.g.e.**, ss.125-140

[221] Hayrettin Gökozan ve Mehmet Taştan, "Akıllı Taşıtlar ve Kontrol Sistemleri", **Mesleki Bilimler Dergisi**, Cilt.7, Sayı.2, 2018, ss.58-62

[222] Gökozan ve Taştan, **a.g.e**., ss.58-62

[223] Tomaş ve Dostoğlu, **a.g.e**., ss.486-493

şehirler, yenilenebilir enerji, sürdürülebilir akıllı ulaşım sistemleri ve toplumsal refahın en iyi seviyelerde yer almasına odaklanarak çevre dostu uygulamalara yer vermektedir[224].

Akıllı kentler, katılımcı bir yönetim anlayışı ile bilgi ve iletişim teknolojilerinden faydalanmaktadır. Örnek olarak vatandaşların hükümet yetkilileri ve diğer yöneticiler ile bağlantı kurmak için sosyal medya veya diğer çevrimiçi iletişim uygulamalarına yer vermektedir. Akıllı kentler vatandaşlarına yerel yönetimlerinde katılımcı olma ve iletişim fonksiyonlarının aktif olarak kullanılması için fırsat sağlayarak daha güvenilir bir toplum ve refah seviyesi yüksek kaliteli bir yaşam imkânı tanımaktadır[225].

Sonuç olarak akıllı sistemler gündelik yaşamda yaygınlaşarak, yaşama, çalışma hayatı ve iletişim kurma becerilerimizi değiştirmektedir. Akıllı kentlerden akıllı otomobillere kadar tüm akıllı sistemler kolaylık, enerji verimliliği ve tasarruf, güvenlik, üretkenlik ve eğlence gibi sosyo-kültürel hayatımıza doğrudan etki etmektedir. Teknoloji çağında yaygınlaşan akıllı sistemleri toplumların gelişmesine ve refah bir toplum oluşturmak için fırsatlar sunmaktadır. Bilgi ve iletişim teknolojilerini sosyal bilimlerde etkin olarak kullanılması toplumların gelişmesine, bireysel gelişimin topluma sunduğu avantajları kullanarak daha yaşanılabilir dünya inşa edilmesi mümkün hale gelmektedir[226]. Teknolojinin hızlı gelişimi elektroniğe bağımlı bir yaşamın artması geleneksel yönetim anlayışının toplumları çağın gerisinde kalması kaçınılmaz kılmaktadır. İnsansız orduların gün geçtikçe geliştirilmesi, insansız kara, hava ve deniz araçlarındaki gelişmeler dünyanın otonom silahlar ile donatıldığı günümüzde mühendislik bilimleri ile sosyal bilimlerin entegre bir şekilde müşterek olarak bilimsel çalışmalara yer verilmesi gerekmektedir[227].

---

[224] Bilici ve Babahanoğlu, **a.g.e.**, ss. 124-139

[225] Tomaş ve Dostoğlu, **a.g.e**., ss. 486-493

[226] Bilici ve Babahanoğlu, **a.g.e.**, ss. 124-139

[227] Sinem Akkaya ve Harun Özbay, "Otonom Araçların Akıllı Ulaşım Politikaları Üzerindeki Etkileri", **Akıllı Ulaşım Sistemleri ve Uygulamaları Dergisi,** Cilt.5, Sayı.2, 2022, ss. 200-210

2.9. İnsansız Ordular

İnsansız ordular, taktik ve stratejik savaşmanın konvansiyonel savaşların doğasını değiştirebilecek teknolojileri kapsamaktadır. Robotik, yapay zekâ, insansız hava, kara ve deniz araçlarındaki teknolojik gelişmeler insansız ordular düşüncesinin gerçekleşmesine olanak tanımaktadır[228]. İnsansız orduların geliştirilmesi ile cephelerin temelini oluşturan askerlerin yer almayacağı, insan zayiatı ve yaralanmaların ortadan kalkacağı ve potansiyel olarak askeri birlikleri destekleyici teknolojilere sahip olma, bilimsel çalışmalara ve teknolojiye hâkim olma ön plana çıktığı bilinmektedir[229].

İnsansız orduların, insan için tehlike veya yaşanması zor coğrafi şartlarda teknolojik teçhizatlar ile sonuç almayı hedeflemektedir. İnsansız savaş sistemleri ile keşif faaliyetleri, mayın tarlalarının kurulması ve temizlenmesi, patlayıcıları etkisiz hale getirmek için günümüzde kullanılan örnek çalışmalar arasında yer almaktadır[230]. İnsansız orduların maliyet tasarrufu gibi finansal olarak ciddi katkılar sağlamaktadır. Barınma, yiyecek, tıbbi bakım ve hizmet destek birliklerine olan ihtiyacın azalması ile askeri teçhizatları daha düşük maliyet ile elde edilmesine olanak vermektedir.

İnsansız orduların kurulması ve desteklenmesi için, politika yapıcıların ve askeri kadroların insansız orduların sonuçlarını kritik değerlendirmeler ile uygun düzenlemeler, etik yasalar geliştirmesi gerekmektedir[231]. İnsansız ordular düşüncesi, askeri teknolojilerde muhtemel dönüştürücü gelişmeleri temsil edeceği düşünülmektedir. Devletlerin silahlı kuvvetlerine esneklik, çeviklik ve insan hayatına yönelik daha az risk sunarak, savaşları ve çatışmaları yönetebilme ve harekât şekillerinde yeni gelişmelere ve teknolojilere sahip olma isteğini güncel tutmaktadır[232].

---

[228] Paul Scharre, "**İnsansız Ordular Katil Robotlar, Otonom Silahlar ve Makine Savaşları**", Ed. Can Uyar, Çev. Kutsi Aybars Çetinalp, 2.Baskı, Kronik Kitap, İstanbul, 2021, s. 27

[229] Scharre, **a.g.e**., s. 29

[230] **a.g.e**., s. 137

[231] Küzeci, **a.g.e.,** s. 89

[232] **a.g.e**., s. 91

Otonom silahların insan gözetimi olmadan karar verebilme potansiyeli hakkında endişeler meydana gelmiş olsa da mevcut otonom silahların operatörlerinin insan olması komuta ve kontrolün insan eliyle gerçekleşmesi karar verme yetkisi makinelere bırakılmayıp savaş suçu kaygılarını azaltmaktadır[233]. Ancak günümüzde kendi başına karar verebilen otonom silah sistemlerinin gelişimine ilginin fazla olduğu bilinmektedir.

İnsansız savaş sistemlerinin barışta kötü amaçlı taraflarca ele geçirilmesi veya bu sistemlere elektronik harp saldırılarının gerçekleşmesi potansiyeli bulunmaktadır. İnsansız otonom bir silahın yetkisiz kullanıcılar tarafından ele geçirilmesi askeri ve sivil hedeflere yönelik saldırıların gerçekleşmesi ve savaş suçu işlenmesine olanak tanıyarak stratejik üstünlük sağlamak maksadıyla uluslararası savaş hukukuna hasarlar vermesi öngörülmektedir[234]. İnsansız orduların kritik önemi elektronik harp unsurlarının güçlü olması gerekliliğini doğurmaktadır. Elektronik harp unsurlarına ve politikalarına gün geçtikçe daha çok ihtiyaç duyulmaktadır.

İnsansız silah sistemleri, yapay zekâ, makine endüstrisindeki gelişmeler ve elektronik sensörler ile yüksek teknolojin müşterek kombinasyonu ile gerçekleştirilmektedir. Savunma sanayilerinde yüksek teknolojik gelişmeler ile hedeflerin tespit edilmesi, takip edilmesi, hedeflere yönelik saldırıların gerçekleştirilip gerçekleştirilmeyeceğine karar sürecini destekleyip taraflara analiz imkânı sunmaktadır[235]. İnsansız orduların temelinde elektronik sensörler, kameralar, radar sistemleri, bir teknolojiyi oluşturan yazılımların komuta kontrol teknolojilerini kapsamaktadır.

İnsansız silahların kullanımı ile ilgili uluslararası hukuk ve savaş hukukunda doğrudan çalışmalara yer verilmediği bilinmektedir. 1949 yılında ortaya çıkmış olan Cenevre Sözleşmesi savaş hukukuna ilişkin kuralları kapsamakta, otonom silahların

---

[233] Scharre, **a.g.e**., s. 222

[234] Marc Goodman, "**Geleceğin Suçları Dijital Dünyanın Karanlık Yüzü**", Ed. Yavuz Türk ve Kadir Güven, 3.Baskı, Timaş Yayınları, İstanbul, 2020, ss. 454-499

[235] Bülent Yazıcı, "Otonom Silah Sistemlerinin Uluslararası Silah Hukuku ve Politiği Açısından Sorunsal Meseleleri", **Bilecik Şeyh Edebali Üniversitesi Sosyal Bilimler Enstitüsü Dergisi**, Cilt.4, Sayı.1, 2019, ss. 280-292

kullanımı hususuna özel olarak değinilmemektedir. Ancak Birleşmiş Milletler 2013'ten itibaren otonom silahların kullanımını düzenleyen yeni çalışmalara yer vermeye başlamıştır[236]. Otonom silahların uluslararası hukuk kapsamında anlaşmaların ve kuralların geliştirilmesi süreci zamana yayılarak güncellenen teknolojik gelişmelere göre yavaş ilerlemektedir. İnsansız silahların kullanılması insansız hava, kara ve deniz araçları dahil olmak üzere keşif ve gözetleme, taarruz ve savunma ihtiyaçlarının karşılanması gibi çeşitli askeri maksatlar ile kullanılmaktadır.

21. yüzyılda hızla artan teknolojik gelişmeler ile drone olarak bilinen insansız hava araçları dünya gündemini meşgul etmekte ve insansız hava araçları (İHA) gözetleme, keşif, lojistik, saldırı gibi farklı görevleri elektronik sensörler, kameralar ve radar sistemleri ile görev icrası gerçekleştirmektedir[237]. İnsansız hava araçları, pilotlar için tehlikeli veya erişilmesi mümkün olmayan ortamlarda ve şartlarda görev ifa edebilmektedir. İnsan hayatını riske atmadan keşif ve gözetleme faaliyetleri bilinen en yaygın görevleri arasında yer almaktadır. Geliştirilen bu hava araçları keşif ve gözetleme amacı dışında silah sistemleri ile donatılarak bir savaş uçağının gerçekleştirebileceği görevleri yerine getirebilmektedir[238].

İnsansız hava araçları küresel konumlama sistemleri, elektronik harp donanımları ve yüksek çözünürlüklü kameralar ile donatılmaktadır. Günümüzde silahlı insansız hava araçları askeri operasyonların kritik öneme sahip teçhizatı olarak uzaktan komuta ve kontrol sistemleri ile donatılan insansız hava araçları yerden operatörler tarafından kontrol edilmektedir[239].

İnsansız hava araçları askeri amaçlar dışında sivil hayatta da kullanılmaktadır. İnsansız hava araçları ile erişilmesi zor veya insan hayatını tehlikeli hale getirebilecek coğrafi şartlarda hava fotoğrafçılığı, bilimsel araştırmalar ve gündelik yaşamda, doğal

---

[236] Yazıcı, **a.g.e.**, ss. 280-292

[237] Scharre, **a.g.e**., ss. 93-115

[238] **a.g.e**., ss. 93-115

[239] Berkant Akkuş, "Devletlerin Pozitif İnsan Hakları Yükümlülüğü ve Kolluk Operasyonları Sırasında Otonom Silah Sistemlerinin Kullanımı", **Mehmet Akif Ersoy Üniversitesi Sosyal Bilimler Enstitüsü Dergisi**, Cilt. 1, Sayı.36, 2022, ss. 76-94

afetlerde hasar tespit ve bilgi toplama amaçlı olarak yine insansız hava araçları görev yapabilmektedir[240]. İnsansız hava araçları lojistik hizmetlerinde malzemelerin uzak ve erişilmesi insanı hayatı açısından zor yerlerde sıklıkla tercih edilmektedir. Lojistik sektöründe müşterilerine hızlı ve verimli bir şekilde teslimatın gerçekleştirilmesi için gelişmelerin takip edildiği ve bu teknolojilerin araştırma geliştirme çalışmalarına yer verilmektedir.

Netice itibari ile insansız hava araçları hem askeri hem de sivil hayatta çok yönlü uygulamaları bulunan teknolojilerdir. İnsansız hava araçlarının toplumlar için birçok avantajı bulunsa da dikkatle değerlendirilmesi gereken hukuki ve politik alt yapıların hazırlanması, topluma entegre edilebilecek uygun düzenlemeler ve denetimleri ile insansız hava araçları askeri sistemlerde ve sivil endüstrilerde devrim yaratacak ve insanlık için verimli sonuçlar elde edilmesi potansiyeline sahip teknolojiler ile donatılmaktadır[241].

İnsansız kara araçları (İKA), keşif ve gözetleme yanı sıra taktik muharebe harekatlarında operatörler aracılığı ile uzaktan komuta ile çalışan, yüksek elektronik ve mekanik teknolojiler ile donatılmış vasıtaları içermektedir[242]. İnsansız kara araçları, el tipi modeller, ağır silahlar ile donatılmış büyük araçlar gibi çeşitli şekil ve boyutlarda üretilerek, askeri sahada mayınların temizlenmek, el yapımı patlayıcıların imha edilmesi ve sabit konumlarda silahlandırılmış güvenlik araçları günümüzde kullanılmaktadır[243]. İnsan hayatını tehlikeye atacak geleneksel taktik muharebe sahasında ve tehlikeli görevlerde insansız kara araçlarından faydalanılmaktadır.

İnsansız kara araçları keşif ve gözetleme, taarruz ve savunma harekatlarında etkin olarak kullanılmaktadır. İnsansız kara araçları, makineli tüfekler ve hava savunma silahları gibi teçhizatlar ile donatılarak insan hayatını daha az bir risk ile cari harekatlarda, kritik keşif ve gözetleme faaliyetleri ile harekât merkezlerine değerli

---

[240] Akkuş, **a.g.e**., ss. 76-94

[241] Akkuş, **a.g.e**., ss. 76-94

[242] Köksal Gündoğdu ve Ali Çalhan, "İnsansız Askeri Kara Aracı Tasarımı", **İleri Teknoloji Bilimleri Dergisi**, Cilt.2, Sayı.1, 2013, ss. 36-45

[243] Gündoğdu ve Çalhan, **a.g.e.**, ss. 36-45

istihbarat verileri toplayabilme kabiliyetleri bulunmaktadır[244]. Lojistik ve ikmal gibi kritik öneme sahip muharebe destek unsurlarının faaliyetlerinde insansız kara araçları tercih edilmektedir.

Askeri kullanım dışında sivil hayatında bir parçası haline gelmekte olan insansız teknolojiler geliştirilmektedir. Birçok endüstri de üretime doğrudan katkı sağlayarak elektronik ve mekanik teknolojiler ile gerçekleştirildiği bilinmektedir. Ağır sanayi ve her türlü üretim endüstrisinde operatörler aracılığı ile yük taşıma, imalat, tarım ve günlük yaşamda akıllı otomobil ve ticari kara araçları insan kontrolünde çalışsa da daha az enerji ve efor sarf ederek insan sağlığına doğrundan destek olmaktadır[245].

İnsansız deniz araçları (İDA), su üzerinde insan faktörü olmadan çalışabilen keşif ve gözetleme yanı sıra çeşitli askeri görevleri yerine getirebilen teknolojiler ile donatılan deniz araçların içermektedir. Diğer insansız araçlar gibi yapay zekâ, elektronik sensörler, yüksek çözünürlüklü kameralar ve radar sistemleri insansız deniz araçlarında teknolojik ana unsurları, küçük gemiciklerden büyük su altı ve su üstü deniz araçları gibi çeşitli boyutlarda bulunmaktadır. İnsansız deniz araçları diğer insansız kara ve hava araçları gibi keşif gözetleme, su altı ve su üstü askeri harekatlarında uzaktan komuta ile kullanılmaktadır[246]. İnsan hayatını riske atmadan düşman donanma gemileri ve deniz harekatları hakkında gerçek zamanlı istihbarat toplama kaynaklarından bir tanesidir.

İnsansız deniz araçları torpido veya gelişmiş silahlar ile donatılarak insan hayatını tehlikelerden uzak tutarak savunma ve taarruz harekatlarında gelecek yıllarda daha fazla kullanılacağı, ikmal ve istirahate ihtiyaç duymadan uzun süre görev ifa

---

[244] **a.g.e.**, ss. 36-45

[245] Salih Vardin, Pınar Demircioğlu ve İsmail Böğrekci "Arazi Uygulamaları İçin İnsansız Yer Aracı Geliştirilmesi", **Uluborlu Mesleki Bilimler Dergisi,** Cilt.5, Sayı.1, 2022, ss. 1-13

[246] Murat Yorulmaz ve Kaan Karabulut, "Deniz Taşımacılığında Akıllı Gemiler: Gemi Kaptanlarının Bakış Açısı", **Ekonomi, İşletme ve Maliye Araştırmaları Dergisi**, Cilt.3, Sayı.1, 2021, ss.40-54

edebilmektedir[247]. Söz konusu araçların insan hayatını tehlikeye atmadan düşman sularında keşif görevleri gibi uzun menzilli görevler için tercih edilebilirliğini arttırdığı, çeşitli coğrafi ve hava koşullarında insan hayatını tehlikeye atılmasının önüne geçilmesi insansız deniz araçları ile amaçlanmaktadır[248].

Genel olarak insansız hava, kara ve deniz araçları, insan hayatının tehlikeye atılmasının önüne geçebilecek teknolojileri kapsamaktadır. Ancak temel güvenlik sorunlarının ortadan kalkması için tüm bu araçların güçlü elektronik harp teknolojileri ile donatılması kaçınılmaz bir gerçektir.

2.10. E-Yönetişim

Bilişim ve iletişim teknolojileri aracılığıyla gerçekleştirilen yönetişim modeli, elektronik yönetişim, pratik yönetim örnekleri yönetim aşamaları, yönetimini kolaylaştırılması, yönetim süreçlerinin güncellenmesi ve bütün yönetim süreçlerini kapsamaktadır[249]. Yazılım, mobil yazılım ve web sunucularının desteğiyle, devlet kurumları ile sivil kurumların halka, bilişim ve iletişim teknolojileri vasıtasıyla sundukları hizmetlerin tümü e-yönetişim kapsamındadır. E-yönetişim yalnızca kamu sektöründe kullanılmamakta, aynı zamanda özel sektör ile kamu sektörleri arasında köprü vazifesindedir. "*E-yönetişim, bilişim ve iletişim teknolojileri ve ağ yöneticileri vasıtasıyla, devlet, halk, özel sektör ve sivil toplum kuruluşları arasındaki etkileşimlere yön veren, basitleştiren ve yeni imkanlar sunan yeni bir yönetişim evresidir*"[250].

E-yönetişim, e-devlet, e-demokrasi ve e-iş fonksiyonlarından oluşmaktadır. E-devlet fonksiyonu; devlet kamu yönetimleri ve halk arasındaki etkileşimin elektronik ortam ile bilişim ve iletişim teknolojileriyle birlikte, bilgi toplama ve bilgi işleme

---

[247] Fevzi Fırat Gözüyeşil, "Denizde Çatışmanın Önlenmesine Dair Uluslararası Kurallar Bağlamında İnsansız ve Otonom Gemilerde İyi Gemicilik İlkesi ve Gözcülük Görevi", **Adalet Dergisi**, Cilt.1, Sayı.66, 2021, ss.193-225

[248] Yorulmaz ve Karabulut, **a.g.e.**, ss. 40-54

[249] Ramazan Şengül ve Özlem Balıkçı, "Yerel Yönetimlerde E-Yönetişim Üzerine Bir Araştırma", **Ordu Üniversitesi Sosyal Bilimler Araştırmaları Dergisi**, Cilt.11, Sayı.2, 2021, ss. 417-436

[250] Bekir Parlak ve Kadir Caner Doğan, "**E-Yönetişim Kavramsal/Kuramsal Çerçeve, Ülke İncelemeleri ve Türkiye'ye Yansımaları**", 1.Baskı, Beta Yayımcılık, İstanbul, 2019, s.39

evrelerinin gerçekleştirilmesi olarak tanımlanmaktadır[251]. E-demokrasi fonksiyonu; elektronik ortamlar ile etkileşim sağlayarak, vatandaşların politik sistemin devam ettirilebilmesi için bilişim ve iletişim teknolojileri vasıtasıyla demokratik süreçlerin yönlendirilmesi e-demokrasi, kamu ve özel sektörlerin web sunuları üzerinden, etkileşim sürecini kapsamaktadır[252].

E-yönetişim etkin bir şekilde vatandaşların hizmetine sunulduğun da pozitif sonuçlar almak mümkündür. Halkın bilgiye kolay erişmesi ve kullanması, kamu hizmetlerinin kalitesinde pozitif etkiler görülmektedir. Vatandaşların bilişim ve iletişim teknolojilerini kullanarak, ekonomik şartların iyileştirilmesi ve bilgi teknolojilerine dayalı istihdam imkanları sunmaktadır. Düşük maliyet ile hizmet ve ürünlerin kullanıcılara erişiminde hem ekonomik hem de zamandan tasarruf sağlamaktadır[253]. Veri tabanları oluşturarak sunulan ürün ve hizmetlerin, birçok alanda olduğu gibi hukuk alanında da bilgiye erişimi kolaylaştırması gibi e-yönetişimin birçok alanda faydalarından söz etmek mümkündür. Toplumların kendilerini geliştirmeleri için, zamanın doğru kullanılmasına ve zaman tasarrufuna dikkat etmeleri gerekmektedir. Kamu yönetimlerinin, bilişim ve iletişim teknolojilerini vatandaşlarına sunulan hizmetlerin kalitesini arttırmak için ve zamanı en iyi şekilde kullanarak elektronik yönetişim desteğiyle toplumsal gelişmeleri görmek mümkündür[254].

E-yönetişim, devletin bilişim ve iletişim teknolojileriyle bireylerin yaşam standartlarını artırmasına, zamanı etkili bir biçimde kullanarak, devlet ile vatandaş arasındaki etkileşimi maksimize ederek hem devletlerin kamu yönetimindeki başarısını hem de vatandaşların bireysel kazanımlarını arttırmaktadır. Kamu yönetimlerinin aktif etkileşimli bir iletişim ortamı sağlamak maksadıyla kablolu ve kablosuz internet erişim altyapılarını en iyi şekilde vatandaşlarına sunmaları

---

[251] Turan Şener ve Nezihe Ülkü Eren, "E-Devlet'in Yönetişim Bağlamında Değerlendirilmesi", **Karadeniz Araştırmaları Dergisi**, Cilt.18, Sayı.72, 2021, ss.863-873

[252] Murat Çelik ve Mehmet Emin Yardımcı, "Dijital Devlet ve İyi Yönetişimin Kökleri", **Siyasal Ekonomik ve Entelektüel Boyutlarıyla İyi Yönetişim**, Ed. Mehmet Karakaş, Selin Karatepe ve Fatma Benli, 1.Baskı, Beta Yayıncılık, İstanbul, 2018, ss.409-430

[253] Şener ve Eren, **a.g.e.**, ss. 863-873

[254] Çelik ve Yardımcı, **a.g.e.**, s.425.

gerekmektedir. Devlet olarak bir bilişim ve iletişim teknolojilerinin en iyi şekilde faydalanıp aynı altyapı hizmetleri bireylere sağlanmadığı taktirde tek yönlü bir teknoloji kullanımında hiçbir fayda görmeyecektir[255]. Bilişim ve iletişim teknolojileri alt yapısı, devlet, bireyler ve özel sektör işletmelerine tüm kullanıcılara maksimum erişim imkânı tanımalıdır[256].

Kamu yönetimi disiplinine göre, iyi bir e-yönetişim, kamu personelinin, bireylere en iyi ürün ve hizmetleri, yaşam standartlarını geliştirme ve eşitlik doğrultusunda gerçekleştirmek mümkündür. Bilişim ve iletişim teknolojilerinin kullanımını arttırarak, verimli bir şekilde vatandaşlara hizmet sunumları gerçekleştirilmelidir[257].

Elektronik yönetişim, vatandaşların katılımlarıyla ve kamu yönetimlerine fayda sağlayarak bilişim ve iletişim teknolojilerin katılımcılara ulaşabileceği her türlü ortam hazırlamalı ve desteklenmelidir. Ülkelerin demokratikleşme süreçlerinde güncel yönetim politikalarını yakından takip ederek kamu politikalarındaki reformlar vasıtasıyla gerçekleştirilmelidir Elektronik yönetişim, yabancı kaynaklara ulaşmak için ve şeffaf kamu politikaları belirlenmesi noktasında, erişimi ve politika belirleme süreçlerini kolaylaştırmıştır[258]. Vatandaşların bilişim ve iletişim teknolojilerini kullanmak için gerekli görülen eğitim veya yardımcı uygulamaların kamu alanında, istihdam ve kaliteli hizmet sunmamaları ülkelerin gelişmelerine önemli katkılar yapmaktadır. Sosyal olarak toplumların meslek, eğitim ve teknolojik olarak kaliteli bir yaşam standartlarına ulaşması mümkündür. Elektronik yönetişim ile yüz yüze gerçekleştirilen işlemlerden meydana gelen zaman kaybının yanı sıra sağlıklı bir iletişim ve kamu görevlisi ile vatandaşlar arasında problemsiz bir iş yapabilme imkânı

---

[255] Yıldız Atmaca ve Faysal Karaçay, "Türkiye'deki Kamu Yönetimi Reformlarında Dijitalleşme ve E-Yönetişim", **Internationl Journal of Management and Administration**, Cilt.4, Sayı.8, 2020, ss. 260-280

[256] Qi Zou ve diğerleri, "Vision and Reality of E-Government for Governence Improvement: Evidence From Global Cross-Country Panel Data", **Technological Forecasting & Social Change an Internatıonal Journal**, Cilt.1, Sayı.194, 2023, ss. 1-17

[257] Atmaca ve Karaçay, **a.g.e.**, ss. 260-280

[258] Parlak ve Doğan, **a.g.e**., s.99.

tanımaktadır. İnternetin sağlamış olduğu imkanlar ile en önemli değer olan zamanı etkili bir şekilde kullanılmasını olanak sağlamaktadır[259].

Vatandaşların temel hak ve özgürlüklerini kendi hür iradeleri ile yöneticilerini belirlemeli, yöneticiler bilişim ve iletişim teknolojileri aracılığıyla etkin bir şekilde iletişimde kalarak yönetime aktif katılım sağlamalıdır. Elektronik yönetişim yalnızca yönetim uygulamalarının da yer almamaktadır. Siyaset alanı içinde de elektronik yönetişim uygulamalarının görmek ve yönetici olarak siyasi karar alıcılara sunduğu imkanlar görülmektedir.

Kamu yönetimleri, verilerin elektronik ortamlara aktarılması sürecinden, bireylerin siyasi faaliyetlere direkt olarak elektronik yönetişim kapsamı içinde yer alan elektronik demokrasiyle gerçekleşmektedir[260]. Elektronik yönetişim, siyasi faaliyetlerin yürütülmesinde elektronik yönetişimin sağlamış olduğu, elektronik yönetim uygulamaları, vatandaşların aktif olarak etkileşimli ve toplumun elektronik bilgi iletişim teknolojileri imkanlarıyla siyasi faaliyetlerine kolaylık sağlamaktadır[261].

Kamu politikalarının geliştirilmesinde, ulusal birliklerin elektronik yönetişim stratejik politikalarının içerisinde yer almaktadır. Bilişim ve iletişim teknolojilerine yönetimsel olarak geçiş sürecinde vatandaşların sürece uyumu konusu, geri planda bırakılmayarak önemli bir faktör olduğu vurgulanmıştır. Bilgiye erişim aşamasında, vatandaşlara karşı yöneticilerin şeffaf ve net bir yol izlemeleri, vatandaşların iyi ve güvenilir bir şekilde bilgiye ulaşmalarına imkân tanımaktadır. Elektronik yönetişim, bireylerin istek ve şikayetlerini bilişim ve iletişim teknolojileri ile çevrimiçi uygulamalarla yer verilmektedir[262]. Yöneticiler, elektronik yönetişim sayesinde

---

[259] Özgür Uçkan, **E-devlet, E-demokrasi ve Türkiye**, 1.Baskı, Literatür Yayınları, İstanbul, 2003, s. 70.

[260] Zou vd., **a.g.e.**, ss. 1-17

[261] Aman Singh, "E-Governance: Moving Towards Digital Governance", **Peer-Reviewed, Multidisciplinary & Multilingual Journal**, Cilt.2, Sayı.1, 2023, ss. 204-215

[262] Atmaca ve Karaçay, **a.g.e.**, ss. 260-280

vatandaşlarından geri beslemeler alarak, yönetim sürecini iyileştirmelerine elektronik yönetişim aracılığıyla imkân tanımışlardır[263].

2.11. E-Devlet

Vatandaşlara devlet tarafından sunulan hizmetlerin, elektronik ortamda bu hizmetler devam ettirmesi olarak tanımlanabilir. Bütün kamu hizmetlerinin elektronik ortamda hizmet sağlanması devlet ile vatandaşlar arasındaki elektronik portal uygulamalarıdır[264].

Kamu yönetimlerinin, iletişim ve bilişim teknolojisi imkanlarıyla daha verimli olması için imkanlar tanımaktadır. Kamu hizmetlerinin, vatandaşlara direkt olarak ulaştırılması ve erişim imkanlarıyla daha hızlı gerçekleştirilmesini sağlamaktadır. E-devlet uygulamalarında vatandaşların kamu hizmetlerine doğrudan katkı sağlaması, kamu yönetimlerinde ve pratikte meydana gelen tıkanıklıkların ortadan kaldırılması için, vatandaşların etkin bir şekilde erişebilecekleri e-devlet uygulamaları yeni bir model olarak ortaya çıkmaktadır[265]. "*Devletin sunduğu hizmetlerin, vatandaşların herhangi bir zamanda diledikleri yerden ulaşabilecekleri ve devlet içi örgütlerin güvenli olarak bilgi paylaşabilecekleri şekilde çevrimiçi hale getirilmesi*" olarak tanımlanmıştır[266].

E – devletin kamu yönetimlerdeki tıkanıkların giderilmesi konusunda kesin bir çözüm olmamakla beraber, kamu yöneticilerinin ve kamu çalışanlarının, vatandaşlar ile yüz yüze gelmeden hizmetlerin yerine getirilmesine imkân tanımaktadır. Devlet, bilişim ve iletişim teknolojilerine erişimi aynı zamanda pratikteki kullanıcıların,

---

[263] Uçkan, **a.g.e,** s.361.

[264] Luis Alex Valenzuela Fernandez ve diğerleri, "E-Goverment and Its Development in The Region: Challenges", **International Journal of Professional Business Review**, Cilt.8, Sayı.1, 2023, ss. 1-15

[265] Uçkan, **a.g.e.**, s.43

[266] Noureddine Boudriga ve Benebdallah Salah**, Laying out the Foundation for a Digital Government Model Case Study: Technology, Human Factors, and Policy**, Kluwer Academic Publishers, Boston, 2002, s.292'den akt. Ali Şahin ve Erhan Örselli, **Teoriden Uygulamaya E-Devlet**, 2. Baskı, Atlas Akademi, Konya, 2016, s.10

bilişim ve iletişim teknolojilerine erişiminde bir problemle karşılaşmaması için ihtiyaç duyulan teknolojik alt yapıyı hazırlamalıdır[267]. Devlet, ulaştıramayacağı hizmetlerde e-devlet uygulamalarında problem yaşamaması, bilişim ve iletişim teknolojilerini tüm ülkeye sunmalı ve teknoloji alt yapılarının olmadığı yerlerdeki vatandaşlarına e-devlet hizmetini ulaştırmak için kamu hizmetlerinin elektronik ortamlarda gerçekleştiği e-devlet uygulamalarında her bir vatandaşın erişimine imkân tanıyacak alt yapıyı oluşturulmalıdır[268]. Elektronik ortamda sunulan hizmetlerin, vatandaşların işlerini daha hızlı ve kolay erişim sağlamasına imkân tanımaktadır. E – devlet üzerinden sunulan kamu hizmetlerinin, geleneksel devlet işleyişine kıyasla, vatandaşların avantajı olacak birçok faktör bulunmakta, kamu hizmetlerinin ve kamu yönetimlerinin, kalitesi artmış olacak ve yöneticilere, kamu çalışanlarına kolaylıklar sağlayacaktır[269].

Kamu yönetimi anlayışına hâkim olan hiyerarşik, katı bürokrasi kamu yönetimi, bilişim ve iletişim teknolojilerinin gelişimiyle kamu yönetimleri daha esnek olmaya başlamıştır. Teknolojik gelişmeler devlet ile vatandaş arasında yeni bir iletişim ağı oluşturmaktadır. Kamu hizmetlerinin doğrudan vatandaşlara sunulması, klasik kamu yönetimi anlayışı yerini yeni olan elektronik devlet ve elektronik yönetişime bırakmaktadır[270]. E-devlet uygulamalarının, kamu hizmetlerinin verimliliği ve başarısını arttırması söz konusudur. Devlet, vatandaşlarla kamu kurumları arasındaki iletişimi, veri aktarım kolaylıklarını internet ve bilişim ve iletişim teknolojilerini kullanarak, kullanıcılara erişim kolaylığı ve kamu hizmetlerinde tasarruflara imkân vermektedir[271].

---

[267] Mehmet Aktel, Süleyman Öğrekçi ve Bedrettin Özmen, "E-Devlet ve Yönetim İlişkileri", **Gazi Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi**, Cilt.19, Sayı.3, 2017, ss.765-787

[268] Alpay Karasoy, "E-Devlet Uygulamalarının Hizmet Kalitesine Etkileri", **Selçuk Üniversitesi Sosyal Bilimler Meslek Yüksek Okulu Dergisi,** Cilt.12, Sayı.1-2, ss.279-294

[269] Karasoy, **a.g.e.**, ss. 279-294

[270] Handan Ertaş, "Yönetişim – E-Devlet Bağlamında Kamu Yönetiminin Dönüşümü", **Teoriden Uygulamaya E-Devlet**, Ed. Ali Şahin ve Erhan Örselli 2. Baskı, Atlas Akademi, Konya, 2016, s.40.

[271] Erhan Örselli ve Yasin Taşpınar, " E-Devlet: Fırsatlar ve Tehditler Bağlamında Bir Analiz", **Teoriden Uygulamaya E-Devlet**, Ed. Ali Şahin ve Erhan Örselli 2. Baskı, Atlas Akademi, Konya, 2016, s.13

Yönetim performanslarının daha iyi bir seviyeyi gelmesi için, kamu yönetimlerinin pratik uygulamalardaki erişime daha hızlı ve çözüm odaklı olmasına yardımcı olmaktadır. E-devlet, vatandaşların hizmetlere ulaşması esnasındaki problemlerin azalmasına ve kamu yönetimi açısından ortaya çıkabilecek beşerî sorunlara karşı çözüm olarak, vatandaşların teknolojiyi kullanma imkanları oranında e-devlet uygulamalarının yaygınlaşması beklenmektedir[272]. Aynı şekilde kamu yönetimlerinin veri erişimi için paylaşımlarının kısıtlı olması e-devlet uygulamalarının kamu yönetimleri üzerindeki negatif etkilerden birisidir. Kamu kurumlarının kapalı devre veri kullanımı ve internet üzerinden vatandaşlara kısıtlı veri paylaşımı ve web sunucularının maksimum performansı ile kamuya tam olarak hizmet veremediği, zaman zaman yaşanan sunucu kilitlenmeleri ve kısa süreli e-devlet hizmetinin kesintiye uğraması hizmetlerin tam performans ile çalışmadığını göstermektedir[273].

Vatandaşların yaşanan bu problemlerden dolayı işlerini klasik yönetim aracılığıyla gerçekleştirmesi ve e-devlet uygulamalarına olan güvensizliği ortaya çıkarmaktadır. E -devlet uygulamaları, pratikte kamu yönetiminde görev yapan personel için yeni bir olgudur. Kamu görevlilerinin elektronik ortam kullanıcısı olabilmeleri, yetki ve gerekli elektronik erişim izinleri yanı sıra teknoloji kullanımına yatkın kamu çalışanlarına ihtiyaç duyulmaktadır[274]. Geleneksel yönetim ile e-devlet arasındaki temel farklılıklar; geleneksel yönetim anlayışında pasif vatandaş, iletişim aracı olarak kâğıt, hiyerarşik bir yapısal yönetim, yöneticilerin veri paylaşımı, personel yardımı, denetim mekanizmasının tümü bireyler üzerinde olması ve tek yönlü iletişim olması gibi dezavantaj olabilecek etkenler bulunmaktadır[275]. E-devlet kapsamında ise, aktif vatandaş, elektronik iletişim, koordineli ağ yapısı, vatandaşların veri girişi ve paylaşımında bulunması, yanıt merkezinin otomatik veya sesli iletişim merkezleriyle gerçekleşmesi, uzman yardımı denetim mekanizması veri güncellemeleri ile gerçekleşen ve iletişimin daha çok bilişim ve iletişim teknolojileri vasıtasıyla

---

[272] Akın Efendioğlu ve Emre Sezgin, "E-Devlet Uygulamalarında Bilgi ve Paylaşım Güvenliği", **Çukurova Üniversitesi Sosyal Bilimler Enstitüsü Dergisi**, Cilt.16, Sayı.2, 2007, ss. 219-236

[273] Karasoy, **ag.e.,** ss.279-294

[274] Örselli, **a.g.e.,** s.24

[275] Uçkan, a**.g.e.,** s.47

gerçekleştiği görülmekte, e-devlet uygulamalarının geleneksel yönetim anlayışına göre kamu yönetimlerine avantaj sağlamaktadır[276]. "*E-devlet modeli, özellikle düşük maliyet kaliteli hizmet performansı üzerinde temellenen ve toplam kalite yönetimi ile müşteri memnuniyeti ölçütlerine göre yapılandırılmış, verimlilik yönetimi sistemiyle somut ifadesini elektronik ticarette bulan elektronik iş modelinden doğrudan etkilenmiştir*"[277].

Kamu yönetimi uygulamalarında, vatandaşlara verilen hizmetlerin yine vatandaşlara veya kamu kurumları ve özel kuruluşlara veri akışı e-devlet ile sağlanmaktadır. Tek yönlü olarak gerçekleştirilen veri aktarımı, e-devlet uygulamaları için herhangi bir yarar sağlamamaktadır. Verilerin elektronik ortama aktarılması ve sunucularda depolandığı bu süreçte kapalı devre etkileşimsiz bir hizmet ortamı bulunmaktadır[278]. Vatandaşlar ile kurumlar arasında iletişimi aktif olarak gerçekleştiği zaman, kullanıcılardan yöneticiler veya kurumlara elektronik posta kanalıyla vatandaşların veri paylaşımı, veri araştırması, kişisel veya kurumsal uygulamaların içinde sorgulama yapabilme, ihtiyaç duyulduğunda verileri veya belgeleri tek yönlü indirebilme ve çevrimiçi yardım olanakları gibi bu işlemleri e-devlet erişimi ile gerçekleştirilebilmektedir[279].

Elektronik devlet uygulamalarının, merkezi yönetim ve yerel yönetimlerin dahil olduğu tek bir web ara yüzü üzerinden oluşturulan portal da bireysel işlemler ve kamu alanındaki hizmetlerin birbirleriyle entegre olduğu zaman e-devlet uygulamaları tam olarak aktif olacaktır[280]. Kullanıcılara kesintisiz olarak erişim imkânı verilmesi veya kurum ve kuruluşların işlemlerinin tümünü gerçekleştirmesinde interneti verimli, etkin olarak tam performansla kullanılması e-devlet uygulamalarının gelişimine katkı

[276] Fernandez ve diğerler, **a.g.e.**, ss. 1-15

[277] Uçkan, **a.g.e.,** ss,46-47

[278] **a.g.e.,** s.,49.

[279] **a.g.e.,** s.,49.

[280] Ertaş, **a.g.e.,** s. 43

sağlaması, bu süreçte kamu hizmetlerinin elektronik olarak katılımcılara web ara yüzleri aracılığıyla, kullanıcı katılımlı bir ortam oluşacaktır[281].

Vatandaşların kamu hizmetlerine ulaşmak için, aktif bir katılım sağladığı, bireysel ve kamusal verilere erişmek için bilişim ve iletişim teknolojileri aracılığıyla kullanılması elektronik devlet kapsamı içindedir. Kamu yönetiminde, kullanıcı olarak yer alan vatandaşlara, etkileşim içinde adaletli ve hızlı bir şekilde katılım sağlamak amacıyla devletin almış olduğu politik kararlar ve uygulamaların tümü elektronik devlet politikalarıyla gerçekleşmektedir[282].

Bilişim teknolojileriyle kullanıcılara ulaştırılan hizmetlerin bir araya gelmesiyle, kamu yönetiminde ve kurumların yapısal işlerindeki reformlara yer verilmekte iken, kullanıcılar ile hizmet sektörü arasındaki ikili iletişimin doğuracağı problemleri ortadan kaldırmaktadır[283]. Nitekim internet üzerinden gerçekleştirilen etkileşimlerin, daha az personel ve maliyetle karşılanmaktadır. Devletlerin veri depolama ve paylaşma aşamasında ülke nüfusları dikkate alınırsa, verilerin oluşturulması, saklanması, ihtiyaç duyulan kişilere ve kurumlara aktarılması sürecindeki yer, zaman ve veri depolama hususunda elektronik devlet uygulamaları önemli bir kazanç sağlamaktadır[284].

Bilgi ve iletişim teknolojilerinin alt yapı problemleri e-devlet uygulamalarına erişimi sınırlayabilir ve devlet hizmetlerinden faydalanılmasının önüne geçilmesi dezavantajları arasında yer almaktadır. E-devlet uygulamaları, pratikte siber güvenlik problemlerinin ve tehditlerinin var olması devlet faaliyetlerinin dijitalleşmesi siber saldırılara karşı savunmasız kalınması vatandaşların hizmetlere erişimi engellenebilir. Siber saldırılar ile kritik devlet verilerini ve vatandaşların kişisel verilerine erişilmesi yöneticilerin güvensizliğine devlet politikalarının elde edilmesine olanak tanıması

---

[281] Aktel ve Öğrekçi, **a.g.e.**, ss.765-787

[282] Serhat Baştan ve Ramazan Gökbunar, "Kamu Hizmetlerinin Sunumunda E-Devletle İlgili Yeni Gelişmeler: Tümleşik E-Devlet Sistemlerine Doğru", https://acikerisim.deu.edu.tr/ (Erişim Tarihi:25.04.2023).

[283] Karasoy, **a.g.e.**, ss.279-294

[284] Efendioğlu ve Sezgin, **a.g.e.**, ss. 219-236

mümkün hale gelebilir[285]. E-devlet uygulamalarının bütünlüğünü ve güvenliğinin sağlanabilmesi için elektronik harp çalışmalarına ve politikalarına yatırımlara yer verilmesi gerekmektedir.

E-devlet uygulamaları, siyasal iletişimi ve kamusal hizmetlerin dijital çağda e-yönetişimin önemli bir yönünü vurgulamaktadır. Şeffaflık ve hesap verilebilirlik, devlet hizmetlerinde dijital sunumlara yer verilmesi, katılımcı vatandaş kitlesinin artışının olması ve maliyetlerde ciddi tasarrufların önünün açılması e-devlet uygulamalarının en büyük avantajları arasında yer almaktadır[286]. E-devlet, web hizmetlerinde temel bilgilerin sağlanmasından, çevrim içi hizmet dağıtım sistemlerinin uygulanmasına kadar bir dizi gelişmeleri kapsamaktadır. E-devlet uygulamalarının amacı, şeffaflığı, hesap verilebilirliği ve katılımcı vatandaş portföyünün oluşturulmasına teşvik ederken aynı zamanda devlet operasyonlarının verimliliğini ve etkinliğinin arttırmaktır[287].

Sosyal bilimlerde ve siyasal iletişimin dijital dönüşümünde, vatandaşların demokratik süreçlere katılımını arttırmak için bilgi ve iletişim teknolojilerinden faydalanılmasını ifade etmektedir. Vatandaşları kamusal tartışmalara dahil etmek, bilgiye erişim imkânı tanımak ve hükümetlerin karar alma süreçlerinde internet, sosyal medya ve diğer dijital platformların kullanılmasına teşvik edilmesi daha refah bir toplum anlayışının ortaya çıkmasına yardımcı olmaktadır[288]. Siyasal iletişimin dönüşümü gün geçtikçe çevrim içi oylama, sosyal medya uygulamaları ile katılımcı ve bilgi akışının gerçekleştirildiği ortamların oluşturulması ve dijital toplantı ortamları dahil olmak üzere birçok farklı bilgi ve iletişim teknolojileri ile gerçekleştirilmektedir[289].

---

[285] Efendioğlu ve Sezgin, **a.g.e.**, ss. 219-236

[286] Başak Solmaz, "**Siyasal İletişimin Dijital Dönüşümü**", 1.Baskı, Literatürk Academia, Konya, 2019, ss. 9-35

[287] Baştan ve Gökpınar, **a.g.k.**

[288] Fernandez ve diğerler, **a.g.e.**, ss. 1-15

[289] Solmaz, **a.g.e.**, ss. 9-35

Toplumların dijital dönüşüme entegre edilmesi, vatandaşların demokratikleşme süreçlerinde katılımı artmasını sağlamak, şeffaflığa teşvik etmek ve karar alma da kaliteli ve destekleyici yönetim süreçlerinin olgunlaşmasını sağlamaktadır. Modern demokrasinin önemli bir yönü olan yenilikleri takip ederek, bilgi ve iletişim teknolojileri ile birlikte e-yönetişim, e-devlet ve benzeri elektronik kavramları ortaya çıkartmaktadır[290]. Katılımcı bir yönetim anlayışının vatandaşlara ulaşma ve vatandaşların hizmetlere erişiminin, zaman olarak topluma kazanç sağlaması devlet yönetiminin karar alma süreçlerine doğrudan veya dolaylı olarak katkısı bulunmaktadır[291].

21. yüzyılda gerçekleşen teknolojik gelişmeler ile toplumların ve devlet yönetimlerinde ciddi bir elektronik yeniliklerin dijital bir dünyaya dönüşümü, akıllı yaşam sistemleri, insansız ordular ve dijitalleşen yönetişim ve devlet organlarının elektronik devlet, elektronik ticaret ve benzeri uygulamalar hakkında gerçekleştirilen birçok bilimsel çalışmalar bulunmaktadır[292]. Elektronik harp çalışmalarına daha çok askeri ve mühendislik disiplinlerinde ağırlık verilmekte olup, sosyal bilimlerde elektronik harp politikaları ve bilimsel çalışmalara yer verilmemekte, elektronik harp askeri ve mühendislik literatürlerde dinleme, konum tespiti ve karıştırma olarak ifade edilmektedir[293]. Teknoloji çağında toplumların elektronik eşyaları daha çok kullanması ve sosyal yaşamın bir parçası haline gelen elektronik cihazların önümüzdeki yıllarda devletlerin milli güvenlik sorunları arasında yer alacağı değerlendirilmektedir. Sosyal ve siyaset bilimlerinde elektronik harp kavramının araştırılması ve devlet politikalarında elektronik harp çalışmalarına daha çok yer verilmesi gerekmektedir.

---

[290] Şener ve Eren, **a.g.e.**, ss.863-873

[291] Erhan Eroğlu, "Siyasal İletişimde Kültürün Dijital Dönüşümü", **Siyasal İletişimin Dijital Dönüşümü**, Ed. Başak Solmaz, 1.Baskı, Literatürk Academia, Konya, 2019, ss. 334-359

[292] Emrah Aydemir, "Siyasal İletişimde Dijital Diplomasi", **Siyasal İletişimin Dijital Dönüşümü**, Ed. Başak Solmaz, 1.Baskı, Literatürk Academia, Konya, 2019, ss. 315-333

[293] Aydemir, **a.g.e.**, ss. 315-333

ÜÇÜNCÜ BÖLÜM

ELEKTRONİK HARP

3.1. Elektronik Harbin Tarihsel Gelişimi

17. yüzyılda Baltimore ile Washington arasında gerçekleşen haberleşme dünya tarihinde kullanılan ilk elektriksel telgraf haberleşmesidir[294]. İngiliz alfabesinin kısa çizgi ve nokta şekilleri ile anlamlı bir kelime oluşturan semboller yardımıyla ilk elektriksel haberleşme gerçekleştirilmiştir. Tarihsel süreçte teknolojinin gelişimi ile 17. Yüzyıl sonlarında telefon cihazının ortaya çıkışı, 20. Yüzyıl başlarında ise genlik modülasyonu (A.M.) radyo yayınları kullanılmaya başlanılmıştır[295].

Genlik modülasyonun da gönderici ve alıcılarda bulunan modülatör ve demodülatör kullanılmakta olup, modülasyon, yüksek frekanslı sinyallerin iletimi için sinyallere yüklenen bilgilerin değiştirilerek alıcıya transfer sürecini içermektedir[296]. Alıcılarda bulunan demodülasyon ile yüksek frekanslı bilgi sinyalinin genlik değişimi ile bilgi sinyaline dönüştürülmesi, yüksek frekanslı bilgi sinyali ile ses ve görüntü sinyali olarak alıcı ve verici arasında bilgi transferi gerçekleştirilmektedir[297]. Teknik olarak sinüs ve kosinüs ve benzeri sinyallerinin karşılıklı olarak modülasyonlar aracılığı ile çözümünü ifade etmektedir.

II. dünya savaşı öncesinde frekans modülasyonu yayınlar keşfedilmiş olup, frekans modülasyonu haberleşme sistemlerinin kullanımının yaygınlaşması II. Dünya savaşı sonrasında görülmektedir[298]. Frekans modülasyonu (F.M.) genlik modülasyonuna (A.M.) göre daha geniş bir kapsam ile kaliteli yayın ve haberleşme

---

[294] Sait Yılmaz, "**21. Yüzyılda Güvenlik ve İstihbarat**", 1.Baskı, Alfa Yayınları, İstanbul, 2006, ss.607-611

[295] Yılmaz, **a.g.e.,** ss. 607-611

[296] Gümüş, Bozkurt ve Erdoğdu, **a.g.e**., ss.95-125.

[297] **a.g.e**., ss.95-125.

[298] Oya Tokgöz, "Siyasal Toplumsallaşmada Kitle Haberleşme Araçlarının Rolü Ve Önemi", **Nevşehir Hacı Bektaş Veli Üniversitesi Sosyal Bilimler Enstitüsü Dergisi**, Cilt.33, Sayı.3, 1978, ss. 80-92

gerçekleştirildiği için haberleşme sistemlerinde tercih edildiği bilinmektedir[299]. Frekans modülasyonunda aktarımı gerçekleştirilen bilgi sinyali sinüs sinyallerinden meydana gelmekte, taşıyıcı sinyalin sinüs sinyali olmasından dolayı alıcılarda sinüs sinyali çözümü ile frekans değişikliklerinden sinüs sinyali bilgi sinyaline dönüştürülmektedir[300]. Gönderici devrelerinde gerçekleştirilen modülasyon ile bilgi sinyali alıcı devrelerine eriştiğinde demodülasyon devreleri ile ses ve görüntü olarak bilgiye çevrilmektedir.

Yukarıda bahsi geçen haberleşme sistemleri analog haberleşme sistemleri, "*bir insan konuştuğunda bir ses dalgası yayar. Bu ses dalgası bir mikrofon vasıtası ile elektriksel dalgaya dönüştürüldüğünde, elde edilen işaret zamanın fonksiyonudur ve bu işarete analog işaret, işaretin bu hali ile yapılan haberleşmeye de analog haberleşme denir*"[301].

Analog haberleşme, teknolojik gelişmeler ile televizyon yayıncılığına başlanılmıştır. Televizyon yayıncılığı 1936 yılında haberleşme vasıtası olarak bilgi aktarımı ve teknik olarak sinyallerin insanlar aracılığıyla kodlanması ve kod çözücüler ile bilgi-haber alışverişi gerçekleştirilmiştir. Günümüzde kullanılan MODEM kavramı, modülasyon ve demodülasyon kelimelerinin birlikte kullanımı ile ortaya çıkmıştır[302]. Genlik modülasyonu ve frekans modülasyonun temelinde yer alan teknik detaylar 20. Yüzyılın ikinci çeyreğinden itibaren yeniliklere ve gelişmelere yer verildiği bilinmektedir.

Elektronik harp tarihi boyunca askeri alanlarda kullanılmıştır. Elektronik harbin tarihsel sürecini incelediğimizde, 1. Dünya Savaşı'nda ilk kez kullanılmış,

---

[299] Akkaya ve diğerleri, **a.g.e.,** ss.272-315

[300] Caner Arabacı, "Bir Radyo Alıcısının Serencamı", **Selçuk İletişim Dergisi**, Cilt.1, Sayı.1, 1999, ss.133-139

[301] Yılmaz, **a.g.e.,** ss. 607-611

[302] Ali Efe İralı, "Uyumlu Tasarıma Geçişte Kitle İletişim Araçlarının Gelişimi", **Selçuk İletişim Dergisi**, Cilt.14, Sayı.2, 2021, ss. 982-1004

ikinci Dünya Savaşı'na kadar geliştirilerek ikinci dünya savaşında da elektronik harpten faydalanılmıştır[303].

Elektronik araç ve gereçlerinin artan kullanımı ile insanlar farkında olarak veya olmayarak kişisel verilerini paylaşımlara açmaktadırlar. 1. Dünya Savaşında, elektromanyetik spektrumlar üzerinden haberleşme cihazları olan telsizlerin konumunun belirlenmesi, gerçekleştirilen telsiz konuşmalarında iletişimin kesilmesi, frekans karıştırması gibi faaliyetler gerçekleştirilmiştir[304].

Örnek olarak, Avusturya – Macaristan Krallığı, Bosna- Hersek'te yaşanan siyasal ve askeri problemleri, İtalyanların kullanmış olduğu telsizlere karşı dinleme faaliyeti yaparak bilgi toplamışlardır. İngilizlerin geliştirmiş olduğu, konum bilgisinin öğrenilmesi, ilk kez Almanya gemilerinin konumlarının tespitinde kullanılmıştır. [305]

2. dünya savaşına kadar gelişimini sürdüren elektronik harp teknolojileri ile radar sistemleri kullanılmaya başlanmıştır. Sinyal istihbaratı olarak uçakların ve gemilerin yerlerinin tespit edilmesi, telsiz cihazlarındaki muhaberelerin dinlenilmesi ve konum bilgilerinin tespit edilmesi II. Dünya Savaş'ında kullanılan elektronik harp teknolojileri ile gerçekleştirilmiştir[306]. II. dünya savaşında hava araçlarının kullanılmaya başlanmasıyla birlikte, elektromanyetik spektrum ile seyrüsefer sistemlerine yer verilmiştir. Uçak seyrüsefer sistemlerinin elektronik harp ile aldatma yapılarak hedefler ve rotalarının farklı olması sağlanmıştır[307].

Radar sistemlerinin kullanılmaya başlanılması ile uçak ve gemilerde bu teknolojilere yer verilmiştir. Ancak elektronik harp teknikleri ve elektronik harp

---

[303] Ahmet Naci Ünal, "**Siber Güvenlik ve Elektronik Bileşenleri**", 1.Baskı, Nobel Akademik Yayıncılık, Ankara, 2015, ss. 8-10

[304] **a.g.e**. , ss. 8-10

[305] Ünal, **a.g.e**. , ss. 8-10

[306] M. Özgür Seçim, "Radyonun Bir Haber Alma Aracı Olarak Kullanılması: Adnan Menderes Üniversitesi Öğrencilerine Yönelik Bir Araştırma", **Karabük Üniversitesi Sosyal Bilimler Enstitüsü Dergisi**, Cilt.7, Sayı.1, 2017, ss. 302-317

[307] Yılmaz, **a.g.e.**, ss. 263-276

karıştırma uygulamaları da aktif olarak kullanılmaya başlanılmıştır[308]. Aynı zamanda elektronik harp unsurları orduların harekât planlarında da uygulanmaya başlayarak dahil olmuştur. Elektronik harp II. Dünya savaşı sonrasında kurulan Kuzey Atlantik Antlaşması Örgütü (NATO) ve Varşova paktları ile birçok ülke elektronik harp unsurlarını kullanmaya başlamıştır.

Elektronik harbin teknolojik gelişimi, körfez savaşına kadar devam etmiş ve körfez savaşına yön veren teknolojiler olarak anılmıştır. Son olarak 21. Yüzyıl da elektronik harp teknolojilerinin kullanımı Azerbaycan ve Ermenistan arasında, Karabağ savaşında aktif olarak kullanılmış ve etkili sonuçlar Azerbaycan tarafından alınmıştır. Elektronik harbin önemi ve tarihsel süreçteki gelişimiyle günümüzden kullanılan bütün elektronik haberleşme araç ve gereçlerine elektronik harp uygulamalarının kullanılmasının mümkün olduğu anlaşılmaktadır[309].

Elektronik harp, ülkelerin birbirine üstünlük sağlamak maksadıyla, ülkelerin kullanmış olduğu tüm teknolojileri, askeri, ekonomik ve devlet politikalarına ilişkin bilgi toplamak maksadıyla gerçekleştirdiği istihbarat faaliyetleri olarak tanımlanmaktadır.

Elektronik harp (EH), askeri alanda kullanılan elektromanyetik spektrumlar üzerinde gerçekleştiren askeri organizasyonlardır. "*Daha geniş anlamda elektronik harp, tehdit kuvvetlerinin elektronik sistemlerin varlıklarının ve yerleşim yerlerinin tespiti, tehdit sistemlerinin yok edilmesi veya etkinliklerinin azaltılması dost kuvvetlerin elektronik sistemlerinin tehdit tarafından tespitine veya etkisizleştirilmesine engel olunması maksadıyla elektronik sistem ve tekniklerinin kullanılması olarak ifade edilmektedir*"[310].

---

[308] Ünal, **a.g.e**., s.12

[309] Marc Jones, "Hacking, Bots and İnformation Wars in The Qatar Spat", https://d1wqtxts1xzle7.cloudfront.net/56335866/POMEPS_GCC_Qatar-Crisis.pdf?1523917784 , (Erişim Tarihi: 19.05.2023).

[310] Sargun Göktun, ve diğerleri, "Elektronik Harp", https://www.milsoft.com.tr/wp-content/uploads/2020/12/Elektronik-Harp_MilSOFT.pdf , (19.05.2023).

Bilgi ve iletişim teknolojilerinin hızlı gelişimi ile birlikte, insanların ve toplumların gündelik hayatta kullandıkları kitle iletişim ve araç gereçleri vasıtası ile psiko-sosyal etkiler görülmektedir. Elektronik cihaz kullanımı, bireysel olarak artması bilgi güvenliği, siber tehditler ve saldırılar da artmaktadır. Teknolojik gelişmeleri kötü niyetli kullanıcılar tarafından bireylerin ve kamu bilgilerinin, elektronik ortamlarda güvenli bir şekilde kullanmaları ve işlemeleri aynı zamanda korumaları gerekmektedir[311]. Bilginin doğru ve etkin kullanımı, bilgi ve iletişim teknolojilerinin kullanımıyla doğru orantılı olarak güvenli bir şekilde olması gerekmektedir.

3.2. Elektronik Harp (EH)

Elektronik harp (EH), elektromanyetik spektrum ile gerçekleştirilen her türlü iletişim, haberleşme ve elektronik cihazların kullananların kendi çıkarları doğrultusunda üstünlük sağlamak maksadıyla kullanılmasıdır[312]. Elektromanyetik spektrumu (EMS) kontrol etmek ya da düşmana taarruzda bulunmak amacıyla elektromanyetik ve yönlendirilmiş enerjinin kullanılmasını içeren her türlü askeri ve istihbarat faaliyetlerini içermektedir[313].

Elektromanyetik spektrum, elektrik yüklü parçacıkların birbiri ile geçişlerini kapsayan temel doğa kuvvetlerinin etkileşim halinde kalmasıyla, durağan pozisyondaki elektrik yüklerinin etkileşimi ile ortaya çıkan manyetik alanlar ve teknik olarak haberleşmeyi sağlayan elektromanyetik dalgaların çeşitliği elektromanyetik spektrumu ifade etmektedir[314]. Evrendeki ışık davranışları elektrik motorlarının çalışma prensiplerini, güneş ışınlarının ve yıldızlardaki plazmaların hareketleri ve doğa olayları elektromanyetik spektrum ile gerçekleştiği bilinmekte olup fizik ve

---

[311] Ünal, **a.g.e**. s. 4

[312] D. Curtis Schleher, "**Bilgi Çağında Elektronik Harp**", Çev. Berna Kara 1.Baskı, Doruk Yayımcılık, Ankara, 2004, s. 19

[313] Schleher, **a.g.e.**, s. 20

[314] Kadir Erdin, "Elektromanyetik Dalgaların Oluşumu ve Uzaktan Algılama", **İstanbul Üniversitesi Orman Fakültesi Dergisi**, Cilt.28, Sayı.2, 1978, ss. 158-167

teknik disiplinlerin esas çalışma alanı içerisinde yer almaktadır[315]. Elektromanyetik spektruma ışık dalgaları, radyo sinyal dalgaları, x ışınları ve gama ışınlarını örnek olarak verilebilir. Günümüzde birçok haberleşme sistemi elektromanyetik spektrum aracılılığı ile çalışmaktadır. Radyo ve görüntü sinyallerinin alıcı-verici devreler ile gökyüzünde titreşim ile iletilerek ses ve görsel bilgiye dönüştürülmesi ile insanlar gündelik yaşamda kullanmaktadır[316].

Elektronik harp çalışmaları daha küçük bir kapsama alanı içerisinde küresel gerilimlerin askeri ve askeri olmayan istihbarat ve politika dengeleri üzerinde odağı bulunmaktadır. Elektronik harp, uluslararası ilişkiler ve uluslararası çatışmalara yöntemsel olarak destek veren bir kavramdır. Söz konusu elektronik harp faaliyetleri doğrudan devlet yöneticileri ilgilendiren problemleri belirmek maksadıyla ortaya çıkmamış daha çok askeri konjonktürde kullanılan elektronik harp tarihsel süreçte ulusal güvenlik politikalarındaki etkisi dikkat çekici boyutta olmuştur[317]. Uluslararası ilişkiler ve istihbarat çalışmaları arasında elektronik harbin teorik boşluklarına ve konunun geri planda kalmasına sebep olduğu bilinmektedir[318].

Elektronik harp toplumların, ulusların ve uluslararası ilişkiler sentezlerinin gerçekleştirilmesi için bilgi ve iletişim teknolojilerinin doğru anlaşılması, sosyoloji çalışmalarının ve bilginin elde edilmesinde başrolde yer almaktadır. Toplum bilimi yalnızca siyaset, finansal argümanlar ve askeri ilişkiler ile sınırlı kalmamakta toplum için gerçekleştirilecek araştırmaların kültürel ve teknoloji çalışmalarının kapsamı içerisinde elektronik harp çalışmalarının gerekliliği ortaya çıkmaktadır[319]. Uluslararası iletişimin sosyo-kültürel ve beşerî boyutları, siyaset ve ekonomik enstrümanların gerisinde kaldığı düşünülmektedir. Bilgi ve iletişim teknolojilerindeki gelişmeler

---

[315] Erdin, **a.g.e.**, ss.158-167

[316] Han Zhang ve diğerleri, "Big Data Analysis and Prediction of Electromagnetic Spectrum Resources: A Graph Approach", **Mdpi Journal Sustainability**, Cilt.15, Sayı.1, 2022, ss. 2-17

[317] Ali Burak Darıcılı, "**Siber Uzay ve Siber Güvenlik Nedir**?", 1.Baskı, Dora Basım-Yayın, Bursa, 2017, ss. 14-46

[318] Yılmaz, **a.g.e.,** s.21

[319] Darıcılı, **a.g.e.**, ss. 14-46

devlet yöneticilerinin, bireylerin ve iş dünyasının küresel boyutta bütün toplumları ve insan hayatını doğrudan etkilemektedir[320].

Uluslararası ilişkiler, ulusların kendi bünyelerinde ya da devlet destekli kurumların bilgi ve iletişim teknolojileri araç ve gereçlerinin kullanımında tekelleşmeden uzaklaşarak, ulusal kurum ve kuruluşların global bir etki altında ilerlediği siyasal ve istihbarat faaliyetleri ortaya çıkmaktadır[321]. Bilgi ve iletişim teknolojilerindeki gelişmeler ve küresel anlamda devletler arası ilişkilerin önemi, barış durumunda iken bilgi toplama ve analiz edilmesi ile elektronik harp faaliyetleri üstünlük sağlamak maksadıyla etkin olarak kullanılmaktadır.

Elektronik harp, bilgi ve eylemin gerçek zamanlı olarak senkron bir şekilde gerçekleştirilmesi, ulusların dış politikalarında karar vericilerin gizli ve örtülü eylemler ve tekniklerin kullanılması, algı yönetimi ve psikolojik üstünlük sağlamak maksadıyla düşman veya hedefin ikna edilebilirliğini ya da karşı istihbarat ve politikalarının imha edilmesi veya etkisiz kılınması sürecini kapsayan faaliyetleri içermektedir[322]. Ulusal güvenlik politikaları, bilgi güvenliği ve devlet faaliyetlerinin korunması ve devlet yönetimini kapsayan unsurların güvenliğinin sağlanması için elektronik korunma ile desteklenmelidir[323]. Stratejik bilgi ve politikaların, devlet başkanı ve yöneticilerin yönetişim faaliyetlerinde kendi siyasi politikalarına ve devlet politikalarının diğer ulusların saldırı ve tehditlerine karşın stratejik üstünlük avantajı vermemek maksadıyla en iyi şekilde korunması ve bilgi güvenliğinin en üst seviyede olması gerekmektedir[324]. Elektronik harp faaliyetlerinin hedefi, her türlü bilgi edinme ve analizlerin gerçekleştirilmesi ile stratejik bilgi ve faaliyet üstünlüğünün sağlanması ulusal güvenlik politikalarının oluşturulmasında bilginin gücünü etkin şekilde kullanmaktır.

---

[320] Yılmaz, **a.g.e.,** s.81

[321] Ümit Özdağ, "**İstihbarat Teorisi**", 15.Baskı, Kripto Basım, Ankara, 2021, s.112

[322] Özdağ, **a.g.e.**, s.113

[323] Yılmaz, **a.g.e.,** s.135

[324] Özdağ, **a.g.e.**, s.110

Elektronik harp teknolojilerinin asli görevi, uluslararası politikaları meydana getiren stratejik bilginin elde edilmesi ve toplanan verilerin ulusların çıkarları doğrultusunda işlenmesidir. 21. Yüzyıl teknoloji çağında bilgi ve iletişim teknolojilerinin sürekli gelişimi uluslararası rekabet ortamında güven problemlerini ve bir devletin diğer bir devletin iç işlerine karışılmasına olanak tanıyan uygulamalara imkân vermektedir[325]. Elektronik harp faaliyetlerinin özünde stratejik üstünlük, güven duygusu ve karar alıcılara mevcut bilgi gücü ile destek vererek gerçek zamanlı doğru kararlar alınmasına yardımcı olmak yer almaktadır. Elektronik harp, stratejik olarak bilgi ve iletişim teknolojileri ile istihbarat faaliyetlerini küresel gelişmeleri yakından takip etmek, devletlerin sınır komşuları hakkında bilgi toplamak ve her türlü istihbarat faaliyetlerini tespit ve imha etme ana fikri ile gerçekleştirilmektedir[326]. Günümüzdeki teknolojik gelişmelerin hız kesmeden devam etmesi ve gün aşırı yeni bir teknolojilerin ortaya çıkması, merkeziyeti olmayan internet uygulamaları ve sanal kuruluşların ortaya çıkması, bireysel ve toplumsal meydana gelebilecek her türlü tehdidin ortadan kaldırılması elektronik harp politikalarını oluşturmuş devletlere büyük bir avantaj sağladığı düşünülmektedir[327].

Elektromanyetik spektrumun kontrolü ve yönlendirilmesi ile gerçekleştirilen elektronik harp, tarihsel süreçte ordular tarafından kullanıp askeri operasyonların kilit unsuru olarak bilgi desteği ve gerekli elektronik destek, taarruz ve korunma faaliyetlerini icra etmektedir. Elektronik harbi oluşturan unsurlar ise elektronik destek (ED), elektronik taarruz (ET) ve elektronik korunmadır (EK)[328].

3.2.1. Elektronik Destek (ED)

Düşmanın elektromanyetik spektrumunun kullanımını imha etmek veya engellemek için elektronik harp unsuru olarak elektronik destek faaliyetlerinden yararlanılmaktadır. Elektronik destek, elektronik harp faaliyetleri içerisinde,

---

[325] Yılmaz, **a.g.e.,** s.613

[326] Schleher, **a.g.e.**, s. 23

[327] Yılmaz, **a.g.e.,** s.140

[328]Muharrem Arık, "Next-Generation Radar and Electronic Warfare Systems", https://libdigitalcollections.ku.edu.tr/digital/collection/TEZ/id/28127 ,(Erişim Tarihi: 19.05.2023).

elektromanyetik sinyallerin tespiti, konumunun belirlenmesi ve karşıt kuvvetlere dair kullanılan teknolojilerin tanımını yapma faaliyetlerini kapsamaktadır[329]. Elektromanyetik spektrum, mikro dalgalar, radyo dalgaları, kızıl ötesi iletişimi, x ve gama ışınlarını da içerisine alan frekans aralığını kapsamaktadır[330].

Elektronik destek, düşman varlığını ortaya koyabilecek elektronik sinyallerin tespit edilmesi, tanımlanması, düşman iletişimi ve iletişim teknikleri hakkında istihbarat toplamak müttefik veya kendi birliklerinin elektronik tehditlerden korunmasını sağlamak maksadıyla gerçekleştirilen elektronik harp fonksiyonudur[331]. Düşmanın elektronik teçhizatını ve muhaberesini bozarak aynı esnada dost birliklerin muharebe sahasında gerçekleştirilen elektronik harp faaliyetlerinden zarar görmemesini ve iletişim sürekliliğinin sağlanmasına olmasına olanak tanımaktadır. Cari harekatta elektronik destek kritik öneme sahip olan sonuçlarından bir tanesi gerçek zamanlı durumsal farkındalığın yüksek olmasıdır.

Elektronik destek faaliyetleri ile düşman elektronik teçhizatının tespit edilmesi, radar sistemlerinin ve haberleşme sistemlerinden yayım yapan sinyaller hakkında bilgi toplama, kestirme (konum tespiti) ve sinyal taraması ile haberleşme frekanslarının tespit edilmesine olanak tanımaktadır[332]. Düşman imkân ve kabiliyetlerinin değerlendirilmesi ve karşı istihbarat faaliyetlerinin önlenmesi elektronik destek faaliyetleri ile mümkün olmaktadır. Genel olarak elektronik destek, elektromanyetik spektrum içinde yer alan sinyallerin tespit ve analiz edilmesi ile gerçekleştirilen istihbarat faaliyetleri olarak tanımlanmaktadır. Elektronik harp komuta kontrol merkezlerinde elektronik harp operatörleri tarafında gerçekleştirilen bu faaliyetler

---

[329] Veysel Dinç, "Elektronik Harp Teknikleri", **Yüksek Lisans Tezi**, Gazi Üniversitesi, Ankara, 2010, s. 8

[330] Manish Gupta, Hareesh G. ve Arvind Kumar Mahla, "Electronic Warfare: Issues and Challenges for Emiter Classification", **Defence Science Journal**, Cilt. 61, Sayı.3, 2011, ss. 228-234

[331] Schleher, **a.g.e.**, s. 437

[332] Schleher, **a.g.e.**, s. 440

müşterek birliklere elektronik harp komuta merkezleri tarafından bilgi paylaşımı ile cari harekatta gerçek zamanlı bilgi alışverişine olanak tanımaktadır[333].

3.2.2. Elektronik Taarruz (ET)

Elektronik taarruz, elektromanyetik spektrumun kontrolü, tarama faaliyetleri ile tespitinde kullanılan, teknolojik imkanların kısıtlanması veya engellenmesi, elektronik harp sistemleri ile elektromanyetik spektrum sinyalleri ile taarruz edilerek sinyal karıştırması yapılarak ve dost kuvvetlerin bu olaylardan zarar görmemesi için gerçekleştirilen faaliyetlerdir[334]. Elektronik harbin diğer unsuru olan elektronik taarruz, düşmanın iletişim becerilerini, istihbarat faaliyetleri ve karar mekanizmasını doğrudan etkilediği için geçmişte ve günümüzde kritik bir öneme sahip olmaktadır[335].

Elektronik taarruz faaliyetlerinden elektronik karıştırma elektromanyetik spektrumda bulunan radyo sinyallerini karıştırmak, aldatma faaliyetleri gerçekleştirmek veya elektronik teçhizatın fiziksel olarak zarar vermek için yüksek güç yönlendirilmiş enerji kullanarak gerçekleştirilmektedir[336]. Elektronik taarruzun maksadı, düşman haberleşmesini azaltmak, komuta kontrol ve karar sistemlerinin etkinliğini yok etmek, tespit edilen tehdit unsuru elektronik faaliyetlerin engellenmesi ve elektronik silah ve elektronik ile donatılmış olan tüm silah sistemlerinin kabiliyetlerinin gerçekleştirilmesine engel olarak harekatta stratejik üstünlük sağlamaktır[337]. Elektronik taarruz karıştırma, aldatma, kimlik sahtekarlığı gibi faaliyetler ile gerçekleştirilmektedir.

Karıştırma, düşman iletişimi sekteye uğratmak veya haberleşmeye engel olmak maksadıyla yüksek güç yönlendirilmiş enerji ile tüm elektronik sistemlerin devre dışı

---

[333] **a.g.e.**, s. 490

[334] Özgür Aydın, "Elektronik Harp ile Toplanan Verilerin Veri Madenciliği Yöntemleri ile Analiz Edilmesi", **Yüksek Lisans Tezi**, Bahçeşehir Üniversitesi, İstanbul, 2017, s. 10

[335] Schleher, **a.g.e.**, s. 60

[336] Schleher, **a.g.e.**, s. 58

[337] **a.g.e.**, s. 53

kalması için gerçekleştirilmektedir[338]. Yüksek teknoloji elektronik harp teçhizatları ile üretilen yüksek frekanslı enerji üretiminin yönlendirilmiş antenler vasıtasıyla lokal ve büyük bölgelerin elektronik faaliyetlerinin engellenmesi elektronik karıştırma olarak ifade edilmektedir.

Aldatma, düşmanı yanıltmak için yanlış hedefler ve sinyaller oluşturarak gerçekleştirilen elektronik harp tekniğidir. Düşman haberleşme frekanslarını tespit edilerek, haberleşmeyi manipüle etmek için aynı frekanslardan yayınlar yapılması ve haberleşme içinde yanlış hedef ve komutlar ile düşmanı aldatmaya yönelik bütün elektronik harp faaliyetlerini kapsamaktadır[339]. Aldatma, harekât esnasında harekatın tümüyle şekillenmesine ve sonuçları değiştirici etkisi bulunmaktadır. Aldatma faaliyetlerinden birisi olan kimlik sahtekarlığı, düşmanın karar mekanizmasında yer alan elektronik cihazların ve haberleşme sistemlerine sızarak, düşman komuta kontrol merkezini ele geçirmek suretiyle düşman birliklerine kendi lehlerine komutlar verilmesini ifade etmektedir[340].

Elektronik korunma ise dost kuvvetler olarak bilinen personel, teknolojik haberleşme ve elektronik araçların, fiziki binaların saldırı ve tehditlerine elektronik harp unsurlarına karşı korunmasını ifade etmektedir[341].

3.2.3. Elektronik Korunma (EK)

Elektronik korunma, elektronik teçhizatın düşman elektronik harp sistemleri tarafından bozulmasına, ele geçirilmesine karşın kullanılan önlemler ve teknik uygulamalardır. Elektronik korunma yöntemlerinden sinyal şifreleme, frekans atlama ve kripto anahtarları gibi önlemler ile gerçekleştirilmektedir[342]. Düşman elektronik

---

[338] **a.g.e.**, s. 211

[339] **a.g.e.**, s. 233

[340], Schleher, **a.g.e.**, s. 235

[341] **a.g.e.**, s. 20

[342] Çağatayhan Çolakoğlu, "Tactical Command and Control System and Network Centric Warfare", **Journal of Military and Information Science**, Cilt.2, Sayı.3, 2014, ss. 70-76

harp müdahalelerini en aza indirgenmesi için yönlendirilmiş anten, frekans atlamalı ve kriptolu haberleşme araçlarının kullanılması ile düşman elektronik harp sistemlerinden korunarak karşı elektronik harp taarruz teknikleri birlikte icra edilmektedir[343].

Elektronik korunma, elektronik harp unsurlarının tümü gibi kritik öneme sahiptir. Dost kuvvetleri her türlü elektronik saldırı, müdahale ve karıştırma faaliyetlerinden elektronik korunma uygulamaları ile bertaraf edilmektedir. Elektronik harp unsurlarından elektronik destek, elektronik taarruz ve elektronik korunma faaliyetlerinin içerisinde yer alan frekans atlama, karıştırma teknikleri, yönlendirilmiş frekans ve enerji yanı sıra pasif olarak dinleme faaliyetlerine yer verilmektedir[344].

Frekans atlama; bir iletişim sinyalinin frekansını mikro zaman dilimi içinde değiştirilerek, düşmanın radyo frekans sinyallerini bozmasını ve sinyalin engellenmesini zorlaştıran teknikleri kapsamaktadır[345].

Yayılı spektrum; haberleşme sinyallerinin daha kapsamlı bir band aralığında frekansın yayılmasını ve düşman unsurlarına karşı elektronik harp korunma tekniği olarak bilinmektedir[346].

Yön bulma ve yer tespiti; düşmanın karıştırma faaliyetlerini kaynağına ulaşmak ve düşman muhabere vasıtalarının konum bilgisini bulmak için kullanılan elektronik harp tekniğidir. Yer tespitinde yüksek doğrulama oranlarına ulaşmak için en az üç elektronik harp sisteminin aynı anda çalışarak kestirme yapılarak alınan farklı yönlerden sinyallerin birleştirilmesi ile konumun güçlü bir kesinlik içermesi mümkün hale gelmektedir[347].

Sinyal Karıştırma; düşmanın haberleşme sistemlerini çalışmaz hale getirme veya haberleşmenin engellenmesi için kullanılan güçlü sinyalleri yönlendirerek

---

[343] Schleher, **a.g.e.**, s. 172

[344] **a.g.e.**, s. 557

[345] Schleher, **a.g.e.**, s. 259

[346] **a.g.e.**, s. 623

[347] **a.g.e.**, s. 493

düşman iletişimini sekteye uğratılması, aynı zamanda uygulanan sinyal karıştırma faaliyetlerinden dost haberleşme sistemlerinin etkilenmemesi için gerçekleştirilen elektronik harp tekniğidir[348]. Yönlendirilmiş enerjiler ile haberleşme frekanslarını belirli bir yönde iletilmesine müsaade edilmesi ile düşman haberleşmesinin kısıtlanmasına, dost elektromanyetik spektrumunun korunarak aktif haberleşmenin sağlanabilmesi için uygulanan önemli bir elektronik harp unsurudur[349].

Dinleme; düşman elektromanyetik spektrumunun tespit edilmesi, tespit edilen radyo frekansları aracılığı ile düşman hakkında istihbarat toplamak maksadıyla icra edilen elektronik harp tekniğidir[350]. Dinleme, elektronik harp hakkında bilinen en aktif istihbarat toplama kaynağıdır. Dinleme faaliyetleri ile elde edilen bilgilerin düşman üzerinde stratejik üstünlük sağlanması bağlamında en önemli elektronik harp tekniğidir.

3.3. Elektronik Harp ile Gerçekleştirilen İstihbarat Faaliyetleri

Elektronik harp ile gerçekleştirilen istihbarat faaliyetlerinin çoğu teknik istihbarat ile elektronik harp bileşenlerinin yardımı ile teknik istihbarat (techint), elektronik istihbarat(elint), sinyal istihbaratı(sigint), muhabere istihbaratı(comint), siber istihbarat, görüntü istihbaratı(imint), ve sosyal medya istihbaratı(socmint) gerçekleştirilmektedir.

3.3.1. Teknik İstihbarat (TECHINT)

Düşmanın muhtemel tehdit unsurlarının, teknoloji birimlerini ve kabiliyetleri hakkında bilgi toplanılmasının ve teknoloji uygulamalarını kapsayan geniş bir istihbarat alanıdır[351]. Teknik istihbarat, teknoloji araç ve gereçlerinin yanı sıra teknoloji bilimindeki araştırma ve geliştirme faaliyetlerinin, milli güvenlik, askeri ve

---

[348] **a.g.e.**, s. 233

[349] **a.g.e.**, s. 615

[350] **a.g.e.**, s. 81

[351] Ali Burak Darıcılı, "**İstahbarat 101**", 1.Baskı, Dora Basım-Yayın, Bursa, 2023, s. 190

istihbarat operasyonları ile devlet yöneticilerinin karar alma sürecini doğrudan etkileyen ve önemli destekler sağlayan bir kavramdır[352].

Devletlerin barış durumunda ve seferberlik durumunda, diğer devletlerin kabiliyetlerini ve niyetlerini, potansiyel tehdit unsurlarını, güvenlik açıklıklarının tespit ve analizi teknik istihbarat ile gerçekleştirilmektedir[353]. Bilimsel çalışmaların takibini sağlamak, diplomatik ve uluslararası anlaşmalar için stratejik üstünlük sağlamak maksadıyla teknik istihbarat faaliyetleri, bir devletin stratejik duruşu ve karar alma süreçlerinin planlanması veya kaynaklar ayrılmasında teknik istihbarat ciddi bir öneme sahip olmaktadır[354]. Teknik istihbarat yukarıda yer alan istihbarat faaliyetlerinin tümünü kapsamaktadır.

Teknik istihbarat, teknolojik gelişmelerin takibi ve yeniliklere hızla cevap verebilme, teknoloji çağının dezavantajlarından birisi olan bilgi kirliliği istihbarat uzmanlarının ve analistlerin istihbarat faaliyetlerini zorlaştıran etmenlerdendir[355]. Aynı zamanda karşı istihbarat faaliyetleri aldatma, teknik istihbarat icraatlarının boşa çıkartılması, bilgi ve haber dezenformasyonu ve gizlilik gibi birçok güçlükleri de içermektedir.

İstihbarat faaliyetleri yasal ve etik olarak ulusal ve uluslararası hukuk kapsamında gerçekleştirilmektedir. Teknik istihbaratın dolaylı veya doğrudan hedefi düşman veya müttefik devletlerin, bilgi ve iletişim teknolojileri kabiliyetlerine ve muhtemel tehditlere karşın öngörülü bir fikir ortaya koymak için çalışmalara yer vermektir[356]. Milli güvenlik politikalarının ve devletlerin uluslararası ilişkilerde stratejik üstünlük sağlanmasında kritik bir öneme sahip olmasından dolayı teknik istihbarat uzmanlarının karşılaşmış olduğu zorluklara rağmen, elektronik harp

---

[352] Özdağ, **a.g.e.**, s. 121

[353] Emre Çıtak, "**Güvenlik ve İstihbarat**", 1.Baskı, Yeniyüzyıl Yayınları, İstanbul, 2017, s. 175

[354] Aziz Yakın, "**İstihbarat Casusluk ve Casuslukla Mücadele**", 1.Baskı, Dışişleri Akademisi Yayınları, Ankara, 1969, s. 36

[355] Darıcılı, **a.g.e**, 2023, s. 195

[356] M. Hayati Taban ve Emre Aydilek, "Dijital Çağda İstihbarat Analizi", **İstihbarat Çalışmaları ve Araştırmaları Dergisi**, Cilt.2, Sayı.1, 2023, ss. 39-67

faaliyetlerinin bilgi ve iletişim teknolojilerindeki gelişmeleri yakından takip ve farklı kaynaklardan fayda sağlama kabiliyeti, uluslararası ilişkiler ve güvenlik politikalarının sürdürülebilirliğini sağlamaktadır[357].

3.3.2. Elektronik İstihbarat (ELINT)

Elektronik istihbarat, elektronik haberleşme cihazları ve kitle iletişim araçları üzerinden elektronik sinyaller vasıtasıyla bilgi toplama ve elde edilen bilgi üzerinden gerçekleştirilen analiz işlemlerini ifade etmektedir[358]. Elektronik istihbarat faaliyetleri, dünya devletlerinin istihbarat toplama ve askeri operasyonlarının yönetiminde, bütün devletlerin birbiri hakkında bilgi toplamak maksadıyla gerçekleştirilen önemli bir bilgi kaynağını ifade etmektedir[359].

Elektronik istihbarat, elektronik teçhizatın konum bilgisi, teçhizatın türü ve işlevlerinin ne olduğunun tespit edilmesi için radyo sinyalleri ve radar sistemlerinin elektromanyetik spektrum içerisinde yer alan sinyallerinin engellenmesi, düşman tarafından kullanılan elektronik cihazların tanımlanması ve bütün toplanan verilerin analiz edilerek işlenme sürecini kapsamaktadır[360]. Elektronik istihbarat ile stratejik üstünlüğün sağlanması, askeri operasyonlar ve elektronik istihbarat faaliyetlerinin, istihbarat birimlerine avantaj ve karar vericilere bilgi akışı sağlanmaktadır.

Elektronik istihbarat, elektronik sinyallerini analiz etmek ve radyo sinyallerini engellemek için bir takım özel elektronik ekipmanlar ve yazılımlar kullanılarak gerçekleştirilmektedir. Görüntü istihbaratı ve sinyal istihbaratı ile birlikte bilgi toplama faaliyetleri, anlamlı bir bilgi elde edilmesi ve teyit edilmesi gibi tespit ve analiz işlemleri elektronik istihbarat kapsamında bir bütün olarak kullanılmaktadır. Elektronik istihbaratın önemi, düşman hakkında kritik bilgi ve kullanılan elektronik

---

[357] Çıtak, **a.g.e.**, 2017, s. 348

[358] Kazım Mehmet Erol, "**Açık Kaynak İstihbaratı ve Askeri İstihbarat Haşdi Şabi Örgütü Üzerinde Uygulama**", 1. Baskı, Nobel Bilimsel, Ankara, 2022, s. 25

[359] Özdağ **a.g.e.**, s. 128

[360] Schleher, **a.g.e.**, s. 35

cihazların tanımlanmasının yanı sıra düşman elektromanyetik spektrumu hakkında bilgi akışını sağlamakta ortaya çıkmaktadır[361]. Elektronik istihbarat ile elektronik posta ve mesajlaşma uygulamaları gibi elektronik haberleşmelerin analiz edilerek, diğer devlet yöneticilerinin programları, karar mekanizmasında yer alan düşünceleri ve niyetleri hakkında önemli bilgilerin elde edilmesi mümkün hale gelmektedir[362].

Elektronik istihbarat, askeri birimlerde radar, seyrüsefer sistemleri ve diğer elektronik teçhizatlar tarafından haberleşme sinyallerinin tespit ve analiz edilmesini kapsamaktadır[363]. Elektronik istihbarat bahse konu radar, seyrüsefer sistemleri yanı sıra güdümlü füzelerin ve silahların etkili ve tesirli menzillerinin doğruluk yüzdelerini ve çalışma şekli hakkında bilgi akışı sağlamaktadır[364].

21. yüzyılda gelişen bilgi ve iletişim teknolojileri hızlı ve sürekli olarak güncellenerek yeni bir teknolojinin ortaya çıkması elektronik istihbaratın inovasyonlara açık hale gelme zorunluluğu ortaya çıkmaktadır. Teknik bilimler ile birlikte sosyal bilimlerin entegre edilerek, teknoloji çağında bütün yenilikleri yakından takip ederek bilimsel çalışmalara yer verilmesi gerekmektedir. Elektronik teknolojileri gelişmeye devam ettiği sürece devlet yöneticileri ve istihbarat örgütleri elektronik istihbaratın yetenekleri etkili ve güncelliğinin korunması için akademik çalışmalara ve araştırma geliştirme yatırımlarına ağırlık verilmesi gerekmektedir.

3.3.3. Sinyal İstihbaratı (SIGINT)

Sinyal istihbaratı, bilgi ve iletişim teknolojileri ile elektronik cihazlar aracılığıyla gönderilen veya alınan sinyaller hakkında bilginin toplanılması ve analizinden meydana gelmektedir[365]. Sinyal istihbaratı devletlerin milli güvenlik

---

[361] **a.g.e.**, s. 467

[362] Darıcılı, **a.g.e.**, 2023, s. 182

[363] Erkan Sezgin, "**İstihbarat Üzerine**", 1.Baskı, Cinius Yayınları, İstanbul, 2022, s. 89

[364] Sezgin, **a.g.e.**, s. 90

[365] Emre Çıtak, "Çağımızın Gerekliliği Olarak Sinyal İstihbaratı", **Hitit Üniversitesi Sosyal Bilimler Enstitüsü Dergisi**, Cilt.8, Sayı.2, 2015, ss. 751-770

politikaları bakımından kritik bir öneme sahiptir. Elektronik harp unsurları aracılığı ile gerçekleştirilen sinyal istihbaratı askeri ve istihbarat operasyonlarında her zaman kullanılmakta ve çağın gereklilikleri doğrultusunda geliştirilmektedir. Sinyal istihbaratı elektronik harbin temelini oluşturmakta ve birçok elektronik harp faaliyetleri sinyal istihbaratı altında açıklanmaktadır[366].

Muhabere istihbaratı, elektronik istihbarat, sinyal istihbaratı, görüntü istihbaratı, teknik istihbarat, açık kaynak istihbarat ve sosyal medya istihbaratı bilgi toplama ve analiz faaliyetlerinin temelinde elektronik harp bileşenleri yer almaktadır[367]. Dinleme, kestirme ve sinyal karıştırma faaliyetlerinin sinyal istihbaratı birimlerince analiz edilerek istihbarat raporları ve cari hareket planlamaları hazırlanmaktadır[368]. Sigint hücre olarak bilinen sinyal istihbaratı birimleri teknik istihbarat, elektronik istihbarat, muhabere istihbaratı ve elektronik harp faaliyetleri bu hücre tarafından analiz edilerek karar süreçlerinin şekillenmesine yardımcı olmaktadır. Radyo ve telsiz sinyalleri, mobil telefon aramaları, internet sağlayıcıları ve internet trafiği gibi elektronik haberleşmelerin tespit ve analiz edilmesi, düşman veya diğer devletlerin bilgi ve iletişim teknolojileri kabiliyetleri hakkında kozmik verilerin ortaya çıkartılması sinyal istihbaratı tarafından gerçekleştirilebilmektedir[369].

3.3.4. Muhabere İstihbaratı (COMINT)

Radyo, telefon, telsiz ve bilgisayar gibi iletişim vasıtaları aracılığı ile gönderilen veya alınan bilgi sinyallerinin tespit edilmesi, var ise kripto anahtarlarının çözülmesi ve analizi işlemlerinin bir bütün olarak bilgi toplama faaliyeti olarak ifade edilmektedir[370]. Haberleşme vasıtalarının iletim hattının yani frekans bant aralığının ve doğrudan kullanılan sabit frekanslarının tespit edilerek dinleme faaliyetinin icra

---

[366] Çıtak, **a.g.e.,** 2015, s. 751-770

[367] Semih Sevinç, "Sinyal İstihbaratı Analizi Bağlamında Bir Değerlendirme: Rubicon Operasyonu ve Türkiye", **İstihbarat Çalışmaları ve Araştırmaları Dergisi**, Cilt.2, Sayı.1, 2023, ss. 68-81

[368] Özdağ **a.g.e.**, s. 123

[369] Özdağ **a.g.e.**, s. 124

[370] Schleher, **a.g.e.**, s. 32

edilmesi olarak, dinleme faaliyetleri HF, UHF ve VHF haberleşme antenleri ile gerçekleştirilmektedir[371].

Yüksek Frekans bandı olarak da bilinen HF bandı, tipik olarak iletişim amaçları için tahsis edilen bir dizi radyo frekansını ifade etmektedir. Elektromanyetik spektrumun bir parçası olan ve 3 ile 30 megahertz (MHz) arasında değişen frekansları kapsayıp HF bandına "kısa dalga" bandı olarak da ifade edilmektedir[372]. HF sinyalleri, gökyüzü dalgası yayılımı adı verilen bir katmanı kullanarak uzun mesafeler kat edebilmektedir. Yüksek frekans iyonosfer tarafından kırılır veya yansıtılırlar, bu da iletim kaynağından uzakta bulunan alıcılara ulaşmalarına izin vermekte, HF bandı özellikle ufukta uzun menzilli iletişim için uygun hale getirmektedir[373].

Geniş mesafelerde yayılma yetenekleri nedeniyle, dünya çapında iletişim için HF sinyalleri kullanılmaktadır. Uluslararası yayın, deniz haberleşmesi, askeri haberleşme, amatör radyo ve havacılık gibi çeşitli amaçlarla kullanılabilir. Yüksek frekans (HF) bandı, atmosferik koşullara ve girişime karşı hassas olup, güneş aktivitesi, iyonosfer bozulmaları ve hava koşulları gibi faktörler HF sinyallerinin kalitesini ve aralığını etkilemektedir[374]. HF bandındaki belirli frekans aralıkları, uluslararası anlaşmalarla düzenlenir ve her ülkedeki telekomünikasyon yetkilileri tarafından yönetilir. Bu frekanslar, her biri belirli iletişim hizmetleri için belirlenmiş farklı bölümlere ayrılmıştır. HF iletişimi, tipik olarak HF frekans aralığında sinyalleri iletebilen ve alabilen özel elektronik ekipmanı gerektirmekte, HF iletişimi için kullanılan antenler, genellikle gökyüzü dalgası yayılımının verimliliğini en üst düzeye çıkarmak için tasarlanmıştır[375].

---

[371] **a.g.e.**, s. 60

[372] Ilolighata Tamarapreye Okoko, "A Review On Radiowave Propagation Models For Very High Frequency And Ultra High Frequency Band", **International Journal of Engineering Science and Application**, Cilt.6, Sayı.4, 2022, ss. 103-112

[373] Okoko, **a.g.e.,** ss. 103-112

[374] Okoko, **a.g.e.,** ss. 103-112

[375] **a.g.e.,** ss. 103-112

Yüksek frekans (HF) bandı, uzun menzilli iletişim ve küresel kapsama gibi avantajlar sunarak, diğer iletişim biçimlerinin uygulanabilir olmadığı durumlar için kritik öneme sahiptir. Yüksek frekans aynı zamanda, girişime duyarlılık, değişken yayılma koşulları ve daha yüksek frekans bantlarına kıyasla sınırlı bant genişliği dahil olmak üzere sınırlamaları da vardır. Özetle yüksek frekans (HF) bandı, 3 ile 30 MHz arasındaki radyo frekanslarını kapsar ve uluslararası yayın, deniz ve askeri haberleşme, amatör telsiz ve havacılık gibi uzun menzilli haberleşme için kullanılmaktadır.

VHF veya Çok Yüksek Frekans bandı, UHF bandından daha yüksek ancak HF bandından daha düşük olan bir dizi radyo frekansını ve elektromanyetik spektrumda 30 megahertz (MHz) ila 300 MHz bant aralığını ifade etmektedir[376]. VHF bandı, yayın, havacılık, deniz iletişimi, kamu güvenliği ve iki yönlü telsiz sistemleri dahil olmak üzere çeşitli iletişim amaçları için yaygın olarak kullanılmaktadır[377].

Frekans olarak HF bandından daha yüksek, ancak UHF bandından daha düşüktür. Bu aralık, FM radyo yayıncılığı, televizyon yayıncılığı, hava trafik kontrolü, kara mobil radyosu ve diğer birçok uygulama için kullanılan frekansları ve UHF bandına benzer şekilde, VHF sinyalleri öncelikle görüş hattı iletimi yoluyla yayılır[378]. Düz hatlarda hareket ederler ve verici ve alıcı antenler arasında net bir yol gerekmektedir. Ancak VHF sinyalleri, frekanslarının düşük olması nedeniyle UHF'ye kıyasla biraz daha uzun menzile sahiptir.

VHF bandı, yayın amaçlı yaygın olarak kullanılmaktadır. Örneğin FM radyo yayıncılığı, genellikle VHF bandındaki frekansları kullanır. Televizyon yayıncılığında, özellikle analog karasal televizyon sistemlerinde VHF frekansları da kullanılmaktadır[379]. Ek olarak, VHF frekansları havacılık iletişimi, deniz iletişimi, kamu güvenliği telsiz sistemleri ve diğer profesyonel iletişim uygulamaları için

---

[376] Annie Liza Capili Pintor ,ve diğerleri, "Spectrum Survey Of VHF And UHF Bands İn The Philippines ", https://www.researchgate.net/publication/286850875_ , (Erişim Tarihi:12.04.2023).

[377] Thaisa Jawhly ve Ramesh Chandra Tiwari, "Simple VHF and UHF Loss Model**", Journal of Latex Class Files,** Cilt. 14, Sayı. 8, 2015, 1-4

[378] Pintor, ve diğerler, **a.g.k.**

[379] Jawhly ve Tiwari, **a.g.e.**, ss. 1-4

kullanılır. VHF sinyalleri, düşük frekansları nedeniyle genellikle UHF sinyallerinden daha uzun bir menzile sahiptir. UHF sinyallerine kıyasla nispeten daha uzun mesafelerde, özellikle minimum engel bulunan açık alanlarda kullanılmakta, ancak menzil, arazi, binalar ve atmosferik koşullar gibi faktörlerden etkilenerek yayın kalitesi düşebilmektedir[380].

VHF bandında çalışan haberleşme sistemleri, VHF frekansları için tasarlanmış özel antenler ve elektronik ekipmanlar ile sinyalleri iletmek ve almak için VHF antenlerinin yanı sıra VHF frekans aralığına ayarlanmış alıcı-vericiler ve alıcıları içermektedir. Diğer frekans bantlarına benzer şekilde, VHF bandı da aynı aralıkta çalışan diğer cihazlardan potansiyel parazite tabidir. Girişimi önlemek ve verimli spektrum kullanımını sağlamak için, kanal tahsisi ve koordinasyonu düzenleyici kurumlar tarafından gerçekleştirilir[381]. VHF bandı, kamu güvenliği kuruluşları, acil durum hizmetleri ve ilk müdahale ekipleri tarafından yaygın olarak kullanılmaktadır. Polis departmanları, itfaiye ve diğer acil servisler, acil durumlarda ve kritik durumlarda etkili iletişim için genellikle VHF iletişim sistemlerini kullanmaktadır[382].

UHF veya Ultra Yüksek Frekans bandı, frekansı HF bandından daha yüksek olan bir dizi radyo frekansını ifade etmektedir. Elektromanyetik spektrumun 300 megahertz (MHz) ile 3 gigahertz (GHz) arasında değişen bir bölümünden oluşmaktadır[383]. UHF sinyalleri, HF sinyallerine göre daha kısa dalga boyuna sahiptir ve yaygın olarak çeşitli iletişim ve yayın amaçları için kullanılır. UHF bandı, televizyon yayıncılığı, mobil iletişim, kablosuz ağlar (Wi-Fi), telsiz telefonlar, telsizler, uydu iletişimi ve diğer birçok uygulama için kullanılan frekansları içeren 300 MHz ile 3 GHz arasındaki frekansları kapsamaktadır[384]. UHF sinyalleri öncelikle görüş hattı iletimi yoluyla yayılmaktadır. Düz hatlarda hareket ederler ve verici ve alıcı antenler arasında net bir yol gerekmektedir. Binalar ve arazi gibi engeller, UHF sinyal

---

[380] Pintor, ve diğerleri, **a.g.k.**

[381] Zhaleh Sadreddini, "Bilişsel Radyo Ağlarında Çok Ölçütlü Karar Verme Yöntemlerine Dayalı Yeni Bir Spektrum Modeli", **Doktora Tezi**, Karadeniz Teknik Üniversitesi, Trabzon, 2018, ss.1-33

[382] Jawhly ve Tiwari, **a.g.e.**, ss. 1-4

[383] Sadreddini, **a.g.e.**, ss.1-33

[384] **a.g.e.**, ss.1-33

yayılımını etkileyerek sinyal blokajına veya bozulmasına yol açarak işlevini olumsuz etkilemektedir[385].

HF gibi daha düşük frekans bantlarıyla karşılaştırıldığında, UHF sinyalleri, daha yüksek frekans ve görüş hattı yayılma özelliklerinden dolayı daha kısa bir menzile sahiptir. Menzil, tekrarlayıcılar veya sinyal güçlendiriciler kullanılarak genişletilebilmesine rağmen, tipik olarak nispeten daha kısa mesafelerde iletişim için kullanılmaktadır[386]. UHF bantları, HF'ye kıyasla daha geniş bant genişliği sunarak daha yüksek veri iletim hızlarına olanak tanır. Bu, UHF'yi dijital televizyon yayıncılığı, kablosuz geniş bant ve yüksek hızlı veri iletişimi gibi uygulamalar için uygun hale getirmektedir. UHF bandı içindeki belirli frekanslar, ulusal ve uluslararası düzenleyici kurumlar tarafından tahsis edilir ve düzenlenir[387]. UHF bandındaki farklı frekans aralıkları, paraziti önlemek ve verimli spektrum kullanımını sağlamak için belirli uygulamalar için belirlenmiştir.

UHF iletişimi, UHF frekans aralığında çalışacak şekilde tasarlanmış özel alıcı-vericiler, antenler ve alıcılar gerekmektedir. Bu cihazlar yaygın olarak telekomünikasyon, yayıncılık, kamu güvenliği ve kablosuz iletişim sistemleri gibi çeşitli sektörlerde kullanılmaktadır. UHF bandı, aynı frekans aralığında çalışan diğer cihazlardan kaynaklanan potansiyel girişime tabidir. Paraziti azaltmak için, UHF iletişim sistemleri genellikle frekans bölmeli çoklu erişim (FDMA), zaman bölmeli çoklu erişim (TDMA) veya kod bölmeli çoklu erişim (CDMA) gibi kanal teknikleri kullanılmaktadır[388]. UHF bandı, televizyon yayıncılığı, kablosuz iletişim ve kamu güvenliği ağları dahil olmak üzere modern iletişim sistemlerinde çok önemli bir rol oynamaktadır.

Günümüzde kullanılan cep telefonları ve mobil iletişim araçları da yukarıda açıklanan bant aralıklarında haberleşme gerçekleştirmektedir. Global mobil iletişim

---

[385] Pintor, ve diğerleri, **a.g.k.**

[386] Jawhly ve Tiwari, **a.g.e.**, ss. 1-4

[387] Sadreddini, **a.g.e.**, ss.1-33

[388] Sadreddini, **a.g.e.**, ss. 46-59

sistemi (GSM) ikinci nesil (2G); 900 MHz bant, GSM 2G ağının bir parçası olarak kullanılmaktadır. Daha yaygın olan GSM 2G bandı radyo telsiz haberleşmesine göre frekans bant aralığı nedeniyle daha iyi güvenli haberleşme imkanı sağlamaktadır. Mobil haberleşme sistemlerinde 1800 MHz bant da GSM 2G ağının bir parçasıdır, ancak daha çok şehir merkezleri tercih edilir[389]. UMTS/WCDMA (3G), 900 MHz ve 2100 MHz bant, karasal radyo erişim ağı "UMTS" (Universal Mobile Telecommunications System) ve yüksek hızlı iletişim protokolü olan "WCDMA" (Wideband Code Division Multiple Access) 3G teknolojileri için kullanılmakta, daha düşük frekanslı boyutlar geniş kapsama alanı ve daha iyi haberleşme ve erişim sağlamakta hem ses hem de veri iletişim için kullanılmaktadır. Uzun süreli gelişim "LTE" (Long-Term Evolution) dördüncü (4G) ve beşinci nesil (5G), 1850 MHz ve 3800 MHz bant aralığında, 4G ve 5G teknolojileri için, düşük frekans nedeniyle geniş kapsama alanı sağlar ve hem ses hem de veri iletişim için kullanılmaktadır[390].

Muhabere istihbaratı, bilgi sinyalini gönderen ve alanın kimlik tespitinin yapılmasını, bilginin içeriği ve iletişim zamanı hakkında kritik öneme sahip bilgilerin erişimine imkân tanımaktadır[391]. Bilgi toplamak maksadıyla haberleşme sinyallerinin tespit edilmesi, kaynaklarının belirlenmesi ve analiz işlemlerine muhabere istihbaratı denilmektedir. Geçmişte olduğu gibi günümüzde de etkin olarak istihbaratta bilgi toplama yöntemidir. Dünya üzerinde birçok devlet, istihbarat örgütleri ve askeri kurumlar tarafından bilgi toplamak maksadıyla muhabere istihbaratı yöntemini kullanmaktadır[392].

Geleneksel telsiz ve radyo haberleşme sistemleri, uydu haberleşmesi ve dijital hücresel veri ağları gibi yeni nesil haberleşme sistemleri, muhabere istihbaratı uzmanları tarafından tespit edilerek dinleme ve konum bilgilerinin bulunması faaliyetlerini gerçekleştirmektedir. Muhabere istihbaratı 21. Yüzyıl'da istihbarat toplamak için ve kıymetli bilgilere erişimde sıklıkla kullanılan bir elektronik harp

---

[389] Okoko, **a.g.e.,** ss. 103-112

[390] **a.g.e.,** ss. 103-112

[391] Özdağ, **a.g.e.,** s. 106

[392] Özdağ, **a.g.e.,** s. 107

tekniğidir. Özellikle kişisel verilerin korunmasına ilişkin yasaların gündemde olduğu günümüzde muhabere istihbaratı icra edilirken etik ve yasal problemler ortaya çıkmaktadır. Özel hayatın gizliliği, mahremiyet gibi sivil hayatta kişisel verilerin korunması ile doğrudan ilgisi olan faaliyetler, istihbarat pratiklerini zorlaştırsa da istihbarat örgütleri ve hükümetler tarafından yasal zemin oluşturularak icra edilmektedir[393].

Modern hayatın bir parçası haline gelen mobil cihazlar, bilgisayarlar, elektronik postalar, mobil telefon görüşmeleri ve özel mesajlaşma uygulamaları bireyler ve gruplar hakkında elektronik harp muhabere istihbaratı ile aktif bilgi toplama ve analizler sonucunda kıymetli bilgilere ulaşılmaktadır[394]. Muhabere istihbaratı, sinyal trafik analizi, sinyal analizi ve dil analizi gibi aşamalardan meydana gelmektedir. Sinyal trafik analizi, haberleşme esnasında çağrı süresi ve yoğunluğu, haberleşme bilgisinin veri hacmi gibi işlemlerin sentezlenmesinden meydana gelmektedir. Sinyal analizi, bir takım teknik veriler olan modülasyon çeşidi, frekans bant genişliği, iletişim frekansı, var ise kripto kodlarının tespit edilmesi ve analiz edilme süreci olarak tanımlanmaktadır[395]. Dil analizi ise, kriptolu içeriklerin kod çözücüler veya dil uzmanları tarafından çözümlenmesi, dil farklılıklarından doğan muhtemel tehdit unsuru içeriklerindeki anahtar kelime ve kelime gruplarının incelenmesi, tercüme ve aktarma işlemlerinin gerçekleştirilmesini ifade etmektedir. Özetle muhabere istihbaratı, istihbarat örgütleri, askeri kurumlar, devlet yöneticileri tarafından uluslar, kişiler ve gruplar hakkında bilgi toplamak maksadıyla gerçekleştirilen teknik bir elektronik harp yöntemidir.

---

[393] **a.g.e.,** s. 110

[394] Darıcılı, **a.g.e.**, 2023, s. 189

[395] Sezgin, **a.g.e.**, s. 89

3.3.5. Görüntü İstihbaratı (IMINT)

Görüntü istihbaratı, yararlı bilgilerin elde edilmesi için görsel medya araçları olan fotoğraf ve video içeriklerinin veya görsel verilerin analizlerinin gerçekleştirildiği istihbarat tekniğidir[396]. Görüntü istihbaratı, devletlerin istihbarat örgütleri ve askeri kurumları vasıtasıyla diğer devlet kurumları ve vatandaşları hakkında bilgi toplamak amacıyla gerçekleştirilen bir faaliyettir[397].

Görüntü istihbaratı insansız hava araçları, uydular ve elektronik teçhizat aracılığı ile farklı kaynaklardan görsel verilerin toplanması ve analizleri ile meydana gelmektedir[398]. Devletlerin diğer devletler üzerinde her türlü stratejik üstünlük sağlamak amacıyla milli güvenlik unsurları tarafından analiz edilerek karar alıcılara rapor şeklinde sunulmaktadır. Devletlerin üstünlük sağlamak maksadıyla vatandaşların ve kurumların medya araçlarının takip edilerek görüntü istihbaratı sağlanmaktadır. Bilgi ve teknoloji çağında kullanımı yaygınlaşan elektronik cihazların mobil telefon ve kurumsal siteler veya uygulamalar aracılığıyla gerçekleştirilen paylaşımlardan toplanan verileri içermektedir[399]. Elektronik harp teçhizatları ile görsel verilerin analizi, bilgisayar yazılımları, özel donanımlar ve geleneksel kitle iletişim araçları ile görüntü istihbaratı elde edilmektedir.

Görüntü istihbaratı ile binalar, harp araçları, askeri tesisler ve stratejik öneme sahip tesislerin faaliyetlerini ve sahip olunan nesneler ve teçhizat hakkında gerçekleştirilen analizlerin tümünü kapsamaktadır[400]. Askeri operasyonları yönetime ve istihbarat faaliyetlerini desteklemek amacıyla ülke yöneticilerine kritik ve önemli bilgilerin sunulmasında dikkat çekici bir elektronik harp faaliyetidir.

Görüntü istihbaratı çevre faktörlerinin detaylı bir şekilde analiz edilmesi ve ülke yöneticilerine bilinçli ve kapsamlı kararlar alabilmeleri için yardımcı olmaktadır.

---

[396] Özdağ, **a.g.e.,** s. 125

[397] **a.g.e.,** s. 126

[398] **a.g.e.,** s. 126

[399] Darıcılı, **a.g.e.**, 2023, s. 244

[400] **a.g.e.,** s. 242

Geleneksel fotoğrafçılık ve sinema, görsel dijital içerik platformlarına elektronik harp tabanlı yazılımlar ile bilgi toplama ve analiz süreçlerini kapsamaktadır. Görüntü istihbaratı kritik askeri sahaların, nükleer tesislerin, stratejik endüstri sahalarının tespitinde ve doğal afetlerde hasar durumunun anlaşılması için de aktif olarak kullanılmaktadır[401].

Görüntü istihbaratı, nesne algılama algoritmaları bir görsel içindeki nesnelerin tanımlanması ve tespit edilmesi için, günümüzde yaygın olarak kullanılan insansız hava araçları ve uydular anlık görüntü verisi toplamak maksadıyla elektronik teknolojiler ile güçlendirilmektedir. Bilgi toplama faaliyetleri açık kaynak verilerden, sosyal medya uygulamaları ile görüntü istihbaratı ve analizleri gerçekleştirilmektedir.

Elektronik harp faaliyetlerinden bir tanesi olan görüntü istihbaratı, devletlerin ve toplumların bilgi ve iletişim teknolojilerin kullanımının yaygınlaşması ile yapay zekâ ve teknoloji alanındaki çalışmaları ve bilim üretilen her disiplinde hem bireysel hem de profesyonel iş hayatında kritik öneme sahip olduğu değerlendirilmektedir[402]. Dijital dönüşüm çağında elektronik harp, yaygınlaşan teknoloji kullanımı devletlerin milli güvenlik sorunlarının engellenmesi ve bertaraf edilmesinde kritik öneme sahip olmaktadır.

3.3.6. Sosyal Medya İstihbaratı (SOCMINT)

Sosyal medya istihbaratı, sosyal medya kullanıcı davranışları, işletme ve ticari amaçlı reklam içeriklerinin eğilimlerini, toplulukları ve müşteri merkezli bireysel kullanıcı ve işletme hesaplarının sosyal medya uygulamaları ile elde edinilen bilgilerin analiz edilme süreçlerini kapsamaktadır[403]. Ticari işletmeler ve kamu yönetimlerinin, kamuoyunun düşüncelerini, mantıklı karar alma sürecinde sosyal medya uygulamaları aracılığıyla stratejik hamleler yapılmasına olanak tanımaktadır.

---

[401] Sezgin, **a.g.e.**, s. 91

[402] Erol, **a.g.e.**, s. 28

[403] Erol Başaran Bural, "**Açık Kaynak İstihbaratında Yeni Bir Boyut Sosyal Medya İstihbaratı**", 1.Baskı, Yeditepe Akademi, İstanbul, 2021, s. 101

Sosyal medya istihbaratı, mobil aplikasyonlar, haber siteleri, forumlar ve web tarayıcıları gibi farklı kaynaklardan görsel, yazılı ve ses içeriklerinin tespit ve analiz edilmesi ile gerçekleştirilmektedir[404]. Elde edilen veriler bireysel, ticari ve kamu yararına ön görülü karar alma süreçlerini belirlemek, stratejik hedefler doğrultusunda kitleleri kontrol ve ihtiyaçlarına cevap verebilmek için aynı zamanda rakiplerinden önde olma avantajı sağlayarak, işletmeler ve kurumlar analiz edilen veriler sonucunda marka, ürün ve hizmetlerin nasıl karşılık bulduğunu öğrenir, alınan geri beslemeler ile kuruluşların araştırma ve geliştirme faaliyetlerine yön vermektedirler[405]. Sosyal medya istihbaratı ticari işletmelere ve kamu kurumlarına ürün ve hizmet stratejileri hakkında bilgi sahibi olunmasına, toplanan ve analiz edilen bilgiler aracılığıyla projeksiyon olarak fayda sağlamaktadır. Aynı zamanda müşteri ihtiyaçları ve rekabet edilen firmalar hakkında güncel veri akışının sağlanmasına, siyasi partilerin vatandaşlar hakkında gerçek zamanlı istek ve vaatlerinin öğrenilmesinde rekabet avantajı sağlamaktadır.

Sosyal medya istihbaratı ile insan davranışı, duyarlılığı ve toplumların demografik yapısı hakkında veri analitiğinin gerçekleştirilmesine imkân vermekte, sosyal medya uygulamaları ile bir takım yazılım ve algoritmaların kullanılması basit bir kullanıcının bilgi sahibi olması ve analiz yapması mümkün olmaktadır[406].

21. yüzyılın ilk çeyreğinin bitmesine yakın süreç olan günümüzde, insanların birbirleriyle iletişim ve etkileşim halinde bulunmaları geleneksel yöntemlerin dışında sosyal medya aracılığı ile gerçekleşmektedir. Bilgi ve iletişim teknolojilerinin gelişimi ile yaygın olarak kullanılan sosyal medya uygulamaları bilgi kirliliğinin artmasının yanı sıra birçok haber alma ve bilgiye erişim imkânı vererek popülerliğini arttırmaktadır[407]. Sosyal medyanın milyonlarca insan tarafından aktif olarak kullanılması neticesinde sosyal medya istihbaratı kavramı ortaya çıkmıştır.

---

[404] Bural, **a.g.e.**, s. 85

[405] Levent Eraslan, "**Sosyal Medya ve Algı Yönetimi Sosyal Medya İstihbaratına Giriş**", 2.Baskı, Anı Yayıncılık, Ankara, 2020, s. 112

[406] Eraslan, **a.g.e.**, 113

[407] Eraslan, **a.g.e.**, ss. 12-44

Dünya genelinde milyarlarca insanın kullandığı sosyal medya araçları ile bilgi ve iletişim teknolojilerinin her ulustan insanın birbiri ile etkileşim ve bilgi alışverişi içerisinde yaşamlarını sürdürebilme ve küresel çapta haberleri gerçek zamanlı öğrenmesi mümkün hale gelmektedir[408]. Modern iş dünyasında, iş stratejilerinin belirlenmesi ve uygulanmasında sosyal medya istihbaratı önemli argümanlar ve avantajlar sağlamaktadır. Müşteri duyarlılığını anlamak, rakiplerini yakından takip etmek, kriz yönetiminde etkin rol oynamak ve pratik çözüm önerilerinin sunulması, inovasyona açık bir işletme düşüncesi ve fırsatları yakalamak için sosyal medyadan elde edilen bilgiler kullanıcılarına öngörü imkânı vermektedir[409].

3.3.7. Kamu Yönetiminde ve Siyasal İletişimde Sosyal Medya İstihbaratı

Kamuoyu hakkında halk üzerindeki hassasiyet ve davranış okumaları için sosyal medya verileri yöneticilere öngörü sunmakta, sosyal medya istihbaratının önemi kamu yönetimi ve siyasal iletişimde ön plana çıkmaktadır. Kamu yönetiminde ve siyasal iletişimde hemen hemen her konu da gerçek zamanlı bilgi ve kamuoyu görüşlerinin analiz edilmesine yardımcı etken sosyal medya platformlarıdır. Sosyal medya verileri, acil ilgi gerektirebilecek interaktif etkileşimin sağlanması siyasi paydaşların farklı konulardaki kamu duyarlılığına doğrudan etki ve sonuç alınmasına olanak tanımaktadır[410]. Kriz yönetiminde kamu yetkililerinin hızlı bir şekilde cevap verme ve harekete geçebilme yeteneği sosyal medya uygulamaları ile gerçekleştirilmektedir.

Sosyal medya uygulamaları üzerinden toplanan verilerin ile kriz anında krizin kapsamını ve gerekliliklerini yerine getirmek için kamuoyu duyarlılığının kontrol edilmesine günümüz teknoloji çağında yardımcı unsurların en başında yer almaktadır[411]. Belirli grup ve farklı bakış açılarına sahip toplumlar da toplumun ilgi

---

[408] **a.g.e.**, ss. 121-131

[409] **a.g.e.**, s. 224

[410] Stefon Aust ve Thomas Ammann, "**Dijital Diktatörlük- Kitlesel Gözetim, Verilerin Kötüye Kullanımı, Siber Savaş**", Çev. Erdinç Yücel ve Hasan Yılmaz, Ed. Hayriye Ünal 3.Baskı, Hece Araştırma, Ankara, 2019, ss. 145-174

[411] Darıcılı, **a.g.e.**, 2023, s. 229

alanlarının tespit edilmesi ve topluma faydalı içeriklerin üretilmesi, kamu yöneticileri tarafından zamandan tasarruf sağlayarak analiz edilmesi sosyal medya istihbaratı faaliyetleri ile mümkün hale gelmektedir. Kamu yöneticilerinin politika kararları alınması süreçlerinde gerçek zamanlı güçlü bilgi akışı ve toplum davranışlarının kıymetli öngörüler ile paydaşlara sunulması ve politika stratejilerinin belirlenmesine yardımcı argüman olarak kullanılmaktadır[412].

Kamu yöneticileri ve siyasi otoriteler sosyal medya içeriklerini takip ederek, vatandaşların güvenliğini ve demokratikleşme sürecinde kritik sonuçları ortaya çıkaracak yanlış bilgi akışı ve sahte haberlerin tespit edilmesi ve bu ve benzeri olaylara karşın tedbirlerin alınmasını, sosyal medya istihbaratı uygulamalarını kullanarak engellenebilmesi söz konusudur[413]. Sosyal medya verileri politika oluşturma ve stratejik avantajların değerlendirilmesi için bir ölçme değerlendirme olanağı tanımaktadır. Sosyal medya istihbaratı, kamu yöneticilerin ve siyasi paydaşların toplum ile açık diyalog halinde olması, vatandaşların hükümetlere olan güvenini artması ve kapsayıcı bir karar alma sürecini doğrudan vatandaşların katılımcı bir yönetim anlayışına sahip olunmasına, toplumların güçlü bir demokrasi ile yönetilmesine katkı sağlamaktadır[414].

Özetle sosyal medya istihbaratı, politika değerlendirme ve geri bildirimi, kriz ve afet yönetimi, demokrasinin güçlendirilmesi, kamuoyunu izleme, kampanya stratejileri, yanlış bilgilendirme ve dezenformasyonun tespit edilmesi, katılımcı bir toplum oluşturma ve hükümet performans değerlendirmelerinin etkin bir şekilde gerçekleştirilmesine imkân tanımaktadır[415]. Sosyal medya istihbaratı daha doğru kararlar vermeyi kolaylaştırdığı ve demokratik süreci güçlendirdiği görüşünden dolayı kamu yönetimlerinde ve siyasal iletişimde kritik öneme sahip olmaktadır.

---

[412] Şahin Ciner, "**Dijital Demokrasi**", 1.Baskı, Sokak Kitapları Yayıncılık, İstanbul, 2017, s. 45

[413] Ciner, **a.g.e.,** s. 58

[414] **a.g.e.,** ss. 76-78

[415] Özdağ, **a.g.e.,** s. 84

Küresel çerçevede teknoloji çağının bir sonucu olarak ortaya çıkan sosyal medya uygulamaları gündelik yaşamın, iş ve endüstri dünyasında, akademik çalışmalar ve politika çalışmalarının kritik bir argümanı haline gelmektedir. Bireylerin sosyal ihtiyaçlarının, eğlenme, arkadaşlık, eğitim ve benzeri tüm sosyal hayatın bileşenleri bilgi ve iletişim teknolojileri araçları ile sosyal medya uygulamaları ile gerçekleştirilmektedir[416].

Sosyal medya istihbaratı herhangi bir amaç doğrultusunda gerçekleştirilebilirken, evrensel hukuk ve kişisel verilerin korunmasına ilişkin yasalara uygun olmak zorundadır. Sosyal medya paydaşlarının uygulamaların ve verilerin doğru kullanımı için eğitimlere yer verilmeli, aynı zamanda kişisel verilere erişim konusunda bilgilendirilmesi, verileri düzeltme ve silme haklarının başkalarının hayatına müdahale ve hakaret içermemesi konusunda bilgilendirilmesi gerekmektedir[417]. Hukuki anlamda sosyal medya içeriklerinin delil olarak kabul edilmesi, kişisel mahremiyet ve etik kurallar çerçevesinde kanunlara ve nizamlara uygun olma zorunluluğu ve yasal çerçevede devletlerin istihbarat örgütleri ve güvenlik birimleri tarafından gerçekleştirilen faaliyetler, kanunlara ve etik değerlere tabii olacak politikalara ve çalışmalara yer verilmelidir[418].

3.3.8. Siber İstihbarat

Güvenlik Türk dil kurumu sözlüğünde, "*toplum yaşamında yasal düzenin aksamadan yürütülmesi, kişilerin korkusuzca yaşayabilmesi durumu, emniyet*" şeklinde tanım yapılmaktadır[419]. Toplum hayatında insanlar, temel yaşam ihtiyaçlarından hemen sonra güvenlik ihtiyacının karşılanmasını istemektedirler.

Genel anlamda insanların, bireysel güvenlik ve güvende olma hisleri için, kanun koyucuların belirlemiş oldukları güvenlik yasalarına ihtiyaç duyulmaktadır.

---

[416] Aust ve Ammann, **a.g.e.,** ss. 261-290

[417] Ciner, **a.g.e.,** ss. 84-87

[418] **a.g.e.,** ss. 88-100

[419] Türk Dil Kurumu Sözlüğü, "Güvenlik Kelime Anlamı" https://sozluk.gov.tr , (Erişim Tarihi: 09.04.2023).

Toplumun refahı ve güven içinde yaşamasını devletlerin temel görevleri arasında yer almaktadır[420].

Bilgi ve iletişim teknolojilerinin, kişisel verilerin korunması, tehdit unsuru içeren her türlü saldırılara karşı ortamın korunmasıyla siber güvenlik kavramı ortaya çıkmaktadır[421]. Siber güvenlik kavramının amacı, bilginin korunması ve saklanmasını ifade etmektedir. Bilgi güvenliği kavramı açıklarken değindiğimiz, "*erişebilirlik, bütünlük, gizlilik, kimlik doğrulama, inkâr edilemezlik*" gibi etkenler siber güvenliği ortaya çıkaran temel unsur arasında yer almaktadır[422].

Bilgi güvenliği kavramıyla veya birden çok verilerin bir araya gelerek oluşturdukları anlamlı veri topluluğu olan verilere bilgi denilmektedir. Bilgi güvenliği ise işlenen ve bir araya gelen verilerin güvenli bir şekilde korunması, saklanması ve gerektiği hallerde iletimi sürecini kapsamaktadır. Bilgi güvenliğini sağlamak maksadıyla bilgisayar güvenliği yani bilgi ve iletişim teknolojileri araçlarının güvenliği de söz konusu olmaktadır. Bilgi güvenliği genel olarak, kişisel verilerin ve örgüt ve organizasyonlara ait verilerin güvenliğini, bilgisayar güvenliği ise bu verilerin işlendiği, saklandığı ve paylaşım araç gereçlerini kapsamaktadır[423].Siber güvenlik, bilgi güvenliği ve bilgisayar güvenliğinin tüm bileşenlerini kapsayan, kişileri ve kurumların doğrudan müdahil olduğu kavramdır.

Bilgi ve iletişim teknolojilerinin kullanımının artmasıyla fiziki güvenlik unsurları yani konvansiyonel güvenlik unsurları yerini yazılım kodlarına ve elektronik programlara bırakmıştır[424].

---

[420] Hakan Hekim ve Oğuzhan Başıbüyük, "Siber Suçlar ve Türkiye'nin Siber Güvenlik Politikaları", https://www.researchgate.net/publication/348241799 , (09.04.2023).

[421] Ahmet Naci Ünal, "**Siber Güvenlik ve Elektronik Bileşenleri**", 1.Baskı, Nobel Akademik Yayıncılık, Ankara, 2015, s. 111

[422] Ünal, **a.g.e.,** s. 112

[423] Mehmet Eren, "**Avrupa Birliği'nin Siber Güvenlik Politikası**", 1.Baskı, Beta Basım Yayım Dağıtım, İstanbul, 2017, s. 23

[424] Eren, **a.g.e**., s.25

Teknoloji çağında, devletlerin ve kurumların bilgisayarlar üzerinden gerçekleştirdiği işlem sayısı artış göstermektedir. Bilgisayar ve sunucular üzerine kaydedilen, depolanan verilerin korunması öncelikle bilgisayar güvenliği ile ilişkilendirilmemektedir[425]. Siber güvenliği meydana getiren bilgi güvenliği ve bilgisayar güvenliğine karşı, uygulanan saldırılar ve tehditler kişisel verilerin ve kurumsal güvenlik açıklarından faydalanmaktadır.

Devletlerin siber güvenlik anlamında, uluslararası etkileşimleri ve devletler arasındaki anlaşmalara, güvenlik açıklarına ortadan kaldırmaya yönelik müşterek çalışmalara yer verilmesi gerekmektedir. Aynı zamanda uluslararası alanda devletlerin güç ve gövde gösterileri, realist teorileri ortaya çıkartmaktadır[426].

Devletin stratejik planları, ekonomi ve güncel hayata dair verilerin, elektronik arşiv ortamlarında depolanması ve saklanması neticesinde siber saldırılar ile gizlilik içinde saklanan verilere erişim engelleme maksadı taşımaktadır. Siber saldırılar, bilgisayar virüsleri, işletim sistemi virüsleri, makro virüsler, betik virüsler ve truva atları gibi tehdit ve saldırı içeren kötü amaçlı yazılımlardan oluşmaktadır[427].Kişisel ve kurumsal verilerin korunmasına yönelik yapılan tehditler ve saldırıların önlenmesi için, devletlerin belirlemiş oldukları siber güvenlik stratejileri ve politikaları önemli bir güvenlik unsuru olarak değerlendirilmektedir.

Siber güvenlik stratejileri ve siber güvenlik politikaları devletlerin milli güvenlik sorunlarının çözümleri arasında yer alması gerekmektedir. Askeri, siyasi ve ekonomik olarak devlet politikalarının, fiziki realist yaklaşımlar ile korunduğu gibi, bilgi ve iletişim teknolojileri araçlarında saklanan her türlü bilginin siber güvenlik politikalarında yer alması gerekmektedir[428].

---

[425] Şahin Korkmaz, "İzleme ile Güvenliğin Sağlanması" **İşletim Sistemleri Güvenliği**, Ed.Çelebi Uluyol 1.Baskı, Gece Akademi, Ankara, s.54

[426] Gökhan Bayraktar, "**Siber Savaş ve Ulusal Güvenlik Stratejisi**", 1.Baskı, Yeniyüzyıl Yayınları, İstanbul, 2015, s. 45

[427] Korkmaz, **a.g.e**. s.59

[428] Bayraktar, **a.g.e**., ss.125-142

Siber casusluk ve bilgisayar ağlarına izinsiz erişim, bir hedefin teknolojik araştırma geliştirme faaliyetleri, askeri ve istihbarat operasyonlarının teknoloji kullanımı hakkında bilgi toplama faaliyetlerini kapsamaktadır[429]. Günümüzde teknoloji güncellemeleri, çevrimiçi ve çevrimdışı bilgi üretimi ve bilgi alışverişinin hız kesmeden kendini güncellemesi siber güvenlik alanında birçok yeniliğin ortaya çıkmasına olanak tanımaktadır[430]. Gün geçtikçe artan bilgi güvenliği ve siber istihbarat ihtiyaçları, akademik çalışmalara daha çok yer verilmesi konunun önemi vurgulamaktadır.

Siber istihbarat, bilgi ve iletişim teknolojilerinin hızlı gelişmeler neticesinde siber tehditlerin ve bilgi güvenliği bağlamında güvenlik açıklıklarının oluşmasına zemin hazırlamaktadır. Siber saldırılar, güvenlik açıklıklarından faydalanarak bilgi toplama, analiz etme ve bilginin etkin olarak işlenmesi süreci siber istihbarat ortaya çıkartmaktadır[431]. Devletleri yöneten hükümetlere, güvenlik birimlerine ve milli güvenlik unsurlarına yanı sıra ekonomik büyüme ve finansal çevreye aktif bilgi akışının sağlanması, potansiyel tehditlere karşı, siber istihbarat faaliyetleri önlem alınmasına doğrudan katkı sağlamaktadır[432]. Siber istihbarat, kamu kurumları ve özel endüstrilerde potansiyel tehditlerin ve risk analizlerinin gerçekleştirilmesi ile mevcut durumun güvenilir olması ve yöneticilerin karar süreçlerinde kritik öneme sahiptir.

Siber istihbarat, kamu kurumaları yanı sıra vatandaşların gündelik sosyal hayatlarında karşılaşılabilecek siber saldırıların tespit edilmesine ve erken ikaz sistemleri ile ihtiyaç duyulan güvenlik önlemlerinin alınmasını ifade etmektedir[433]. Ulusal güvenlik birimleri ve istihbarat örgütleri, siber güvenlik prosedürlerini uygulama yöntemlerini ve politikaları geliştirerek, erken ikaz ve etkin karşı önlemler

---

[429] Semra Aksaray, "Siber Zorbalık", **Çukurova Üniversitesi Sosyal Bilimler Enstitüsü Dergisi**, Cilt.20, Sayı.2, 2011, ss.405-432

[430] Gönül Cengiz, "Siber Suçlar, Sosyal Medya ve Siber Etik", **İletişim Çalışmaları Dergisi**, Cilt.7, Sayı.3, 2021, ss.407-424

[431] Ercan Nurcan Yılmaz, Halil İbrahim Ulus ve Serkan Gönen, "Bilgi Toplumuna Giriş ve Siber Güvenlik", **Bilişim Teknolojileri Dergisi**, Cilt.8, Sayı.3, 2015, ss.133-146

[432] Yılmaz, Ulus ve Gönen, **a.g.e**., ss.133-146

[433] Aksaray, **a.g.e**., ss.405-432

alınmasına yardımcı asli unsurlardır. Siber istihbarat, devlet yöneticilerine ve toplumu meydana getiren tüm paydaşlarına, bilinçli karar alma süreçleri ve öngörülü fikirler sunmakta, tehdit öngörüsü, gelişmiş güvenlik önlemleri, bilgiye dayalı karar verme süreçleri, hukuka ve sosyal yaşama uyumluluk ve yasal gereksinimlerin karşılanması teknoloji çağında siber istihbarat mümkün hale gelmektedir[434]. Siber istihbaratta güncel olarak büyük veri kümelerinin ortaya çıkması ve bu verilerden doğru bilgi analizi yapmanın güçlüğü ve bilgi ve iletişim teknolojileri vasıtaları ile anonim olarak yayılan bilgi alışverişlerinden kaynaklı tehdit unsuru oluşturabilecek kimliklerin tespiti ve doğrulanması siber istihbaratın dezavantajlarından bir tanesidir[435].

Kamu kurumları ve özel sektör paydaşlarının dijital alt yapısındaki güvenlik açıklıklarının tespit edilmesi güvenlik değerlendirmeleri kapsamında siber güvenlik birimleri tarafından gerçekleştirilmektedir. Güvenlik değerlendirmeleri, elektronik sistem güvenlik açıklıkları, bilgi ve iletişim teknolojileri ağ yapısı, elektronik cihazların ve yazılım uygulamalarının güvenlik taraması ve siber tehdit unsurları tarafından oluşabilecek yanlış uygulamaların tespitinden meydana gelmektedir. Kamu yönetiminde bilişim ağ teknolojileri ve kurumsal ağ yapılarının güvenliğinin sağlanması, kötüm amaçlı yazılımların tespit edilerek, siber suçlar ile ilgili delil toplama, delilin korunması ve analiz edilmesi, tehdidi oluşturan kimliğin doğrulanması siber güvenlik birimlerince gerçekleştirilmektedir[436].

Açık kaynak veri terminalleri, kamusal ve özel veri tabanları ve sosyal medya uygulamaları gibi birçok kaynaktan veri toplama işlemleri siber istihbarat birimlerince gerçekleştirilmektedir. Elde edilen verilerin tehdit ve kötü niyet analizlerinin yapılması, gizli içeriklerin açığa çıkarılması ve kimlik doğrulama için geliştirilen algoritmalar ve elektronik harp bileşenlerinden faydalanarak veri analiz süreci işlemektedir. İstihbarat raporları ve ulusların milli güvenlik kararları ile istihbarat

---

[434] Cengiz, **a.g.e.,** ss.407-424

[435] **a.g.e.,** ss.407-424

[436] Yılmaz, Ulus ve Gönen, **a.g.e**., ss.133-146

havuzundan kolluk kuvvetleri ve kamu kurumları, kamuoyu ise kitle iletişim araçları vasıtasıyla bilgilendirilmektedir.

Elektronik devlet uygulamaları, elektrik, ulaşım ve haberleşme sistemi gibi kritik öneme sahip alt yapı çalışmaları siber saldırı ve terör eylemlerine karşı önlemlerin alınması, siber güvenlik ve erken ikaz sistemleri ile donatılması ulusların milli güvenliğinde kritik öneme sahiptir[437]. Kamu kurumları, özel sektör ve vatandaşların dijital alt yapı ve veri tabanlarını, kişisel ve tüzel kişi verilerinin korunması, fikri mülkiyet haklarının siber tehditlerden korunması için siber istihbarat ve güvenlik birimlerin ihtiyaç duyulmaktadır. Siber istihbarat ve güvenlik birimleri, yazılım korsanlığı, mali dolandırıcılık ve casusluk faaliyetlerinin engellenmesini hedeflemektedir. Ulusal güvenlik birimleri ve uluslararası kuruluşlar, siber suç unsurlarını belirlemek, önlemek veya kovuşturmak amacıyla müşterek hareket etmesi gerekmektedir[438]. Hükümetlerin yanı sıra uluslararası birlikleri meydana getiren bürokratların, etkin siber güvenlik politikaları ve stratejik planlamalar ile güncel bilgileri siber istihbarat ve güvenlik birimlerinden faydalanarak, devletlerin ve uluslararası birliklerin muhtemel siber tehditlere karşı mücadele etmek için müşterek güvenlik politikalarına yer verilmesi gerekmektedir[439].

3.3.9. Siber Güvenlik Stratejileri ve Politikaları

Siber güvenliği meydana getiren araçlar, siber uzay araçları olarak literatürde anılmaktadır. İnternet kullanımı, kapalı devre ağ bileşenleri, mobil araç ve gereçleri, uydu haberleşme sistemleri ve hava araçları siber uzay araçlar arasında yerini almaktadır[440]. Siber uzay araçları, ülkelerin savunma sistemleri ve karşı taarruz araçları ile kendi çıkarları doğrultusunda kullanılmaktadır. Bilişim ağları ve ağ

[437] Aksaray, **a.g.e**., ss.405-432

[438] **a.g.e**., ss.405-432

[439] Yılmaz, Ulus ve Gönen, **a.g.e**., ss.133-146

[440]Ayşegül Güneş, "Küresel Güçlerin Ulusal Siber Güvenlik Stratejileri: ABD Örneği", http://cyberpolitikjournal.org/index.php/main/article/view/18/18 , (Erişim Tarihi: 05.05.2023).

yönetim sistemleri ile devletler, istihbarat faaliyetlerini yerine getirmekte iken karşı istihbarat çalışmalarına yönelik savunma stratejileri geliştirilmektedir[441].

Ülkelerin milli güvenlik stratejilerini belirlerken, bilgi ve iletişim teknolojilerinin yaygınlaşması, teknolojik altyapı çalışmaları, kamu sektörü ve özel sektör reaksiyon göstererek altyapılarını, kurumları ve güvenlik politikalarını güncellemesi zaruri bir ihtiyaç haline gelmektedir[442].

Siber güvenlik stratejileri hazırlanırken, toplumun demokrasi içerisindeki düzeni, insan hakları beyannamesinde yer alan temel hak ve özgürlüklerin korunması, bireysel sınırlandırmalar uygulanırken, bu sınırlandırmaların kişi hak ve özgürlüklerine elverişli olması gerekmektedir. Katılımcı bir yönetim mekanizması, hukuksal olarak ve teknik altyapı destekleyici, birleştirici ve koruyucu yöntemler kullanılarak siber güvenlik stratejileri ortaya çıkartılması gerekmektedir[443].

Saldırı ve tehditlere karşı, kişisel verilerin yanı sıra kurumsal bilgilerin korunması amacıyla, siber güvenlik strateji ve politikaları oluşturulması gerektiği unutulmaması gereken önemli bir unsurdur. Siber güvenlik stratejileri bilgi ve iletişim teknolojilerinin, kurum ve özel sektör sistemlerini korumak, her türlü tehdit ve saldırıya karşı güvenlik politikalarının belirlenmesi ile temel amacına ulaşmasına yardımcı olmaktadır[444]. Her ne kadar kişisel ve kurumsal verilerin korunması maksadıyla güvenlik stratejileri belirlense de gözden kaçırılmaması gereken diğer bir husus altyapı ve fiziki donanımlarında korunması son derece önemlidir.

Siber saldırı ve tehditlere karşı, uluslararası iş birliği yapılarak hukuksal yaptırımlara yer verilmelidir. Öncelikli olarak kişisel verilerin kamu ve özel sektör verilerinin siber güvenlikten daha çok hukuki olarak korunması gerekmektedir. Siber

---

[441] Güneş, **a.g.k.**

[442] Mehmet Ada, "Nato Üyesi Ülkelerin Siber Güvenlik Stratejileri Açısından İncelenmesi", **Yüksek Lisans Tezi,** Gazi Üniversitesi, 2018, ss. 43-49

[443] Ada, **a.g.e**., ss.43-49

[444] Salim Kurnaz ve Mustafa Önen, "Avrupa Birliği'ne Uyum Sürecinde Türkiye'nin Siber Güvenlik Stratejileri", https://dergipark.org.tr/en/pub/ijps/issue/41280/581227 , (Erişim Tarihi: 05.05.2023).

güvenlik stratejilerini belirlerken, hukuk alanında da yaptırımlara ve caydırıcı politikalar bulundurulmalıdır[445].

Siber güvenliğin önemi, askeri ve ekonomik alanlardaki uygulamalar ile ülkeler arasında ve organize siber suçlarla mücadele ile siber savunma politikaları milli güvenliğin temel unsurunu oluşturmaktadır[446]. Siber güvenlik alanında yer alan, siber uygulama alanları, insan faktörü, altyapı ve donanımın unsurlarının öncelik olarak güvenlik politikalarında, eğitimli ve kalifiye personel yetiştirmek olarak belirlenmelidir. Zararlı yazılımlara karşı koruma programları, personelin kişisel ve kurumsal verilerin paylaşımındaki hassasiyeti, alt yapı ve donanım bileşenlerine etkili bir şekilde kullanılması siber güvenliğin ve korumanın temel amaçları arasında bulunmaktadır[447].

Bilgi ve iletişim teknolojilerinin gelişimiyle, internet kullanımı artmakta olup kullanıcıları daha çok uygulama ve araçlarla vakit geçirmektedir. Aynı doğrultuda insanlara ve kurumlara karşı saldırı ve tehditleri artış göstermektedir. Siber güvenlik alanındaki tehditlerin oluşumunu engellemek maksadıyla yapılması gereken, hukuki mevzuat ve politikalarda daima sürdürülebilir ve yenilikleri takipçi olması gerekmektedir[448]. Siber güvenlik stratejilerinin dünya ülkelerinde ki uygulama ve politikalarını inceleyerek siber güvenlik stratejileri ele alınmalıdır. Amerika Birleşik Devletleri'nde siber güvenlik, kamu sektöründe merkeziyetçi bir ağ yapısı ile, kamu sektöründe yer alan bileşenlerin, tehditleri ve saldırıları önceden haber veren erken ikaz uygulamaları ve koruma ilkelerine yer verilmesi düşüncesiyle hareket edilmektedir[449].

---

[445] Ayşegül Nacak, Arif Sarı ve Onurhan Yılmaz, "Küreselleşen Dünyada Siber Güvenliğin Artan Önemi ve Gelişmiş Ülkelerde Siber Güvenlik Stratejileri", https://www.researchgate.net/publication/303945885 , (Erişim Tarihi: 05.05.2023).

[446] Nacak, Sarı ve Yılmaz, **a.g.k.**

[447] Halil İbrahim Mil, Saffet Gülep ve Ahmet Ünal, "Türkiye'nin Siber Güvenlik Stratejileri", https://www.researchgate.net/publication/349052551 , (Erişim Tarihi: 05.05.2023).

[448] Mil, Gülep ve Ünal**, a.g.k.**

[449] Ecir Uğur Küçüksille, Sevda Nur Genç ve Yunus Emre Karabulut, "Dünyada Siber Güvenlik Stratejileri ve Bir Siber Güvenlik Stratejisinin Oluşumu", https://www.researchgate.net/publication/338557611 , (Erişim Tarihi:05.05.2023).

Siber saldırılara karşı veri kaybının sıfıra indirgenmesi için, gerçekleştirilen risk analizleri ve toplumun siber güvenlik hakkında bilinçlendirilmesi çalışmaları da Amerika Birleşik Devletleri'nde uygulanmaktadır.

Almanya'da siber güvenlik stratejileri, kozmik bilgilerin donanımsal olarak korunması, siber güvenliğin kamu ve özel sektörlerde daha fazla yer alması, siber güvenlik alanı için kurumların kendi bünyesinde birim oluşturulması ve eğitimler ile vatandaşlarını ve kamu personeli aydınlatma politikalarını benimsemektedirler[450].

Japonya devleti ise, siber güvenlik politikalarını, siber tehdit ve saldırılara karşı koyma ve saldırının erken ikaz uyarı sistemleri ile önüne geçmeyi planlamaktadır. Bilgi güvenliği ve kişisel verilerin korunmasına ilişkin, halkın bilinçlendirilerek siber güvenlik stratejilerini ve ulusal güvenlik politikaları oluşturulmaktadır[451].

İngiltere'nin siber güvenlik stratejilerine bakışı, her türlü tehdit ve saldırı henüz gerçekleşmeden tespit edilmesi ve önlenmesine yönelik çalışmaları öncelik verilmektedir. Ayrıca siber savunma birimleri oluşturularak, askeri, ekonomik ve siyasi alanlarda siber güvenliğin önemine vurgu yapılmaktadır[452]. Siber güvenlik politikaları uygulanırken, diğer yandan istihbarat faaliyetleri ile tehdit unsuru oluşturabilecek bilgi ve belgelerin toplanarak kamuoyunda farkındalığı arttırmayı hedeflemektedirler.

Genel olarak siber güvenlik stratejileri, ülkelerin ulusal ve uluslararası sahnede milli güvenlik sorunu olarak algılanmakta ve gerekli önlemler için çalışmalar yapılmaktadır. Siber güvenlik, elektronik altyapı ve donanımların korunmasıyla başlamakta, kullanıcılar kişisel verileri ile kurum bilgilerinin saldırılara karşı korunmasını temel amaç olarak değerlendirilmektedir. Siber güvenlik politikaları belirlenirken, teknolojik gelişmelerin sürekli olarak takip edilmesi, gelecek planları ve vizyon belirlenerek hareket edilmesi gerekmektedir. Veri kaybının en aza

---

[450] Küçüksille, Genç ve Karabulut, **a.g.k.**

[451] **a.g.k.**

[452] Küçüksille, Genç ve Karabulut, **a.g.k.**

indirgenmesi için, risk analizleri gerçekleştirilmeli ve risk değerleme raporlarına geniş olarak yer verilmesi öngörülmektedir.

Elektronik harp, ülkenin kritik altyapısını, hükümet sistemlerini ve vatandaş verilerini korumayı amaçlayan kapsamlı güvenlik politikasına ve girişimine sahip olunmasını hedeflemektedir. Dijital çağda, elektronik ve siber tehditler ulusal güvenlik için önemli bir risk oluşturmakta, hükümetler elektronik harp unsurlarını güçlendirmeyi birinci öncelik haline getirmelidir. Elektronik harp Stratejisi dört ana dayanağı şöyle olmalıdır: toplumları meydana getiren vatandaşları, vatanını ve sosyo-kültürel yaşam tarzını korumak, toplum refahını desteklemek, teknolojik güç yoluyla barışı korumak ve yaşanılabilir bir dünya etkisini ilerletmektir[453]. Bu elektronik harp bileşenler ile strateji, kritik altyapıyı korumak, uluslararası iş birliğini teşvik etmek ve elektronik harp iş gücü oluşturmak ortak hedef olarak barışçıl bir dünya olması gerektiği düşünülmektedir. Hükümetler, elektronik harp güvenlik araştırma ve geliştirmeye yönelik yatırımları artırmak, siber tehdit istihbaratı paylaşımını iyileştirmek ve bilgi ve iletişim teknoloji sistemlerini modernize etmek gibi bir dizi girişimle bu hedeflere ulaşılması gerekmektedir[454].

Elektronik harp ve Bilgi Güvenliği ajansları oluşturulmalı, ülkenin kritik altyapısını fiziksel ve siber tehditlerden korumaktan sorumlu kurum olarak faaliyetleri hayata geçirmelidir. Elektronik harp ve bilgi güvenliği risklerini belirlemek, değerlendirmek ve yönetmek için kamu ve özel sektör ortaklarıyla birlikte çalışmalara yer vermelidir. Güvenlik açığı değerlendirmeleri, olay müdahalesi ve elektronik korunma rehberliği gibi bir dizi hizmeti vatandaşlara sunulması gerekmektedir.

Kişisel verilerin korunmasına ilişkin kurumların bilgi ve bilgi sistemlerini korumak için bir bilgi güvenliği ve elektronik harp programı geliştirmesini, uygulamasını ve sürdürmesini gerektiren bir yasa ile desteklenmelidir. Kurumların kendi bilgi güvenliği risklerini belirlemesini ve değerlendirmesini, riske dayalı

---

[453] Ahmet Emre Köker, "Ulusal Siber Güvenlik Stratejisi: Fransa", **UPA Strategic Affairs,** Cilt.3, Sayı.1, 2022, ss. 42-78

[454] Kökler, **a.g.e**., ss.42-78

güvenlik kontrolleri uygulamasını ve düzenli güvenlik değerlendirmeleri ve denetimleri gerçekleştirmesini zorunlu kılacak yasalar hayata geçirilebilir[455].

Elektronik harp, kuruluşların elektronik güvenlik risklerini yönetmeleri ve azaltmaları için hukuk normları çerçevesinde, kuruluşların elektronik harp duruşlarını değerlendirmeleri, boşlukları belirlemeleri ve elektronik harp yatırımlarına öncelik vermeleri ve hükümetler tarafından desteklenmelidir. Elektronik harp özetle tanımlama, koruma, tespit etme, yanıt verme ve kurtarma gibi her işlev kuruluşların bilgi güvenliği programlarını geliştirmek için kullanabilecekleri bir dizi kategori ve alt kategori içermelidir. Hükümetler kurumları elektronik harp ve bilgi güvenliklerini iyileştirmek için adımlar atmaya ve kritik altyapıyı korumak için endüstri ortaklarıyla çalışmaya teşvik etmelidir. Kişisel verilerin korunması Kanunu, kişisel bilgilerin güvenliğini sağlamaya ve veri ihlali durumunda kişilere bildirimde bulunmaya yönelik hükümler içermektedir[456].

Hükümetler vatandaşlarını, altyapısını ve hükümet sistemlerini elektronik harp tehditlerinden korumayı amaçlayan çok çeşitli elektronik harp politikalarına ve girişimlerine yer verilmesi gerekmektedir. Devletler, gelişen tehditlere ve teknolojik gelişmelere ayak uydurmak için elektronik harp politikalarını ve girişimlerini iyileştirmeye ve güncellemeye devam etmesi güvenlik endişelerini azaltmaktadır[457].

Elektronik harp, dünyanın dört bir yanındaki hükümetler için kritik bir konu olarak değerlendirilmektedir. Hükümetler, ülkenin kritik altyapısını ve vatandaşlarını siber tehditlerden korumak için çeşitli politikalara yer vermektedir. Elektronik harp, modern askeri operasyonların kritik bir bileşenidir ve gelişmiş ülkeler, silahlı kuvvetlerinin bir EH ortamında faaliyet gösterecek şekilde donatılmasını sağlamak için çeşitli politikalar ve girişimler uygulamaktadır. Politika, EMS operasyonlarının askeri operasyonlar için önemini ve devletlerin EMS'ye erişimini koruma ihtiyacını

---

[455] Omca Altın, "AB'nin Siber Güvenlik Alanındaki Politikalarının ve Uygulamalarının Etkinliği: Bir Siber Güvenlik Temsilcisi Olarak AB'nin Yeterliliği", **Çankırı Karatekin Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi,** Cilt.13, Sayı.2, 2023, ss.482-507

[456] Altın, **a.g.e.,** ss.482-507

[457] Ceray Aldemir ve Merve Kaya, "Bilgi Toplumu, Siber Güvenlik ve Türkiye Uygulamaları", **Kamu Yönetimi ve Politikaları Dergisi**, Cilt.1, Sayı.1, 2020, ss.6-27

vurgulanmaktadır. EMS politikası ayrıca devletlerin silahlı kuvvetlerince Elektronik harp operasyonlarına yaklaşımını, durumsal farkındalığın, diğer askeri yeteneklerle entegrasyonun ve ileri teknolojilerin kullanımının önemini vurgulamaktadır[458]. Politika ayrıca elektronik harp operasyonlarında uluslararası iş birliğinin önemini de kabul etmektedir.

Elektronik Harp Planlama ve Yönetim faaliyetlerine yönelik politikalar Eh planlama ve yönetimini desteklemek için geliştirilmiş yazılımlar ile araç, senaryo geliştirme, görev planlama ve gerçek zamanlı durumsal farkındalık dahil olmak üzere bir dizi faaliyetlere yer verilmelidir[459]. Elektronik harp planlama ve yönetimi ayrıca farklı askeri birimler arasındaki koordinasyonu destekleyerek ve elektronik harp ile ilgili bilgi ve en iyi uygulamaların paylaşımı için bir müşterek platform oluşturulması müşterek Elektromanyetik Spektrum Harekât Merkezi, askeri ve istihbarat operasyonlarına yönelik elektronik tehditleri izlemekten ve bunlara yanıt vermekten sorumlu ortak bir askeri ve sivil tesis oluşturulması gerekmektedir[460]. Bahsi geçen tesisler, düşman elektronik sinyallerini tespit etmek ve belirlemek ve karşı önlemler geliştirmek için ileri teknolojiler ile desteklenmeli, elektronik harp ile ilgili bilgi ve en iyi uygulamaları paylaşmak için diğer devlet kurumları ve endüstri ortakları ile yakın iş birliği, ayrıca silahlı kuvvetler personeline bir elektronik harp ortamında çalışacak donanıma sahip olmalarını sağlamak için eğitim ve destek için kaynaklar aktarılması, elektronik tabanı, silahlı kuvvetleri tarafından karşı önlemler geliştirmek için kullanılan elektronik tehdit verilerinin bir verit abanı oluşturularak veri tabanı, frekans, güç ve modülasyon dahil olmak üzere elektronik emisyonlar hakkında bilgi içermelidir[461].

Elektronik harp entegre yeniden programlama veri tabanı, silahlı kuvvetler personeli tarafından karıştırma ve aldatma teknikleri gibi karşı önlemler geliştirmek

---

[458] Altın, **a.g.e.,** ss.482-507

[459] **a.g.e.,** ss.482-507

[460] Aldemir ve Kaya, **a.g.e**., ss.6-27

[461] Altın, **a.g.e.,** ss.482-507

için kullanılır. Veritabanı ayrıca yeni Elektronik harp teknolojilerinin ve tekniklerinin gelişimini bilgilendirmek için kullanılmaktadır.

Sonuç olarak silahlı kuvvetlerinin ve güvenlik birimlerinin elektronik harp ortamında faaliyet gösterecek donanıma sahip olmasını sağlamak için çeşitli politikalar ve girişimler uygulanması gerekmektedir. Bu politikalar ve girişimler, durumsal farkındalığın, diğer askeri yeteneklerle entegrasyonun ve ileri teknolojilerin kullanımının önemini vurgulamaktadır. Gelişen teknoloji ve tehditlere yanıt verebilmesini sağlamak için elektronik harp yeteneklerine yatırım yapılması gerekmektedir.

3.4. Kamu Yönetiminde Bilgi Güvenliği Bağlamında Elektronik Harp

3.4.1. Bilgi Güvenliği ve Elektronik 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[462]. Birbirine bağlı teknolojilere olan güvenimiz arttıkça, elektronik harbin dijital varlıkları bozma, manipüle etme ve tehlikeye atma potansiyeli de arttığı bilinmektedir. Geleneksel olarak askeri operasyonlarla ilişkilendirilen elektronik harp, erişimini bilgi güvenliği alanına genişleterek yeni zorluklara yol açması ve hassas bilgileri korumak için yenilikçi stratejiler gerektirmektedir[463].

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 manzaraları şekillendiren en değerli varlıklardan biri haline gelmektedir. Ancak dijitalleşmedeki artışla birlikte bu değerli kaynağın kırılganlığı da artmakta ve bilgi

---

[462]Aykut Çalışkan, "Siber Savaş: Bilgi Krizi Mi Yoksa Güvenliği Mi?", **Savunma ve Savaş Araştırmaları Dergisi**, Cilt.33, Sayı.1, 2023, ss.1-32

[463] **a.g.e**., ss.1-32

güvenliği alanında elektronik harbin ortaya çıkışı, sürekli gelişen siber tehditler ve savunmalar manzarasına yeni bir boyut kazandırmaktadır[464].

Elektronik harp, 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[465]. 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[466].

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 görebilmektedir[467].

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[468]. Bir siber saldırının kaynağını belirlemek, genellikle devlet destekli aktörleri veya gelişmiş bilgisayar korsanlığı gruplarını içeren karmaşık bir zorluktur ve bu kamu

---

[464] Çalışkan, **a.g.e**., ss.1-32

[465] Ayşe Özdemir ve Çelebi Uluyol, "Kamu Kurum ve Kuruluşlarında Bilgi Güvenliği Farkındalığı", **Türkiye Sosyal Araştırmalar Dergisi**, Cilt.25, Sayı.3, 2021, ss.649-666

[466] **a.g.e.,** ss.649-666

[467] **a.g.e.,** ss.649-666

[468] **a.g.e.,** ss.649-666

yöneticilerinin misillemeyi veya karşı önlemleri zorlaştırır ve gerilimleri tırmandırabilir. Siber saldırılar, hedeflendiklerinde bile istenmeyen sonuçlara yol açabilir ve hizmet sağlayıcılar veya aynı ağdaki kullanıcılar gibi masum tarafları ve vatandaşları doğrudan etkileyebilir[469].

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[470]. 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[471]. 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[472]. 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[473].

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

---

[469] Aşır Sertçelik, "Siber Olayler Ekseninde Siber Güvenliği Anlamak", **Medeniyet Araştırmaları Dergisi**, Cilt.2, Sayı.3, 2015, ss. 25-42

[470] Sertçelik, **a.g.e**., ss.25-42

[471] Özdemir ve Uluyol, **a.g.e.,** ss.649-666

[472] Uğur Güngör ve Oğuzhan Güney, "Uluslararası İlişkilerde Güvenliğin Dönüşümü Çerçevesinde Bilgi Güvenliği ve Siber Savaş", **Karadeniz Araştırmaları Merkezi**, Cilt.15, Sayı.55, 2017, ss.131-146

[473] Güngör ve Güney, **a.g.e**., ss.131-146

ederek düzenleyici boşluklara ve belirsizliklere yol açabilmektedir. Bir siber olay birden fazla yargı bölgesini etkilediğinde, hangi ülkenin yasalarının geçerli olması gerektiği konusunda anlaşmazlıklar ortaya çıkabilir[474]. 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. Uluslar, diyaloğu teşvik ederek, normlar oluşturarak ve anlaşmaları müzakere ederek, siber tehditlerin ve çatışmaların ortaya çıkardığı zorlukları toplu olarak ele alarak, uluslararası siber anlaşmalara giden yol, herkes için güvenli ve esnek bir dijital geleceği şekillendirmek için özveri, iş birliği ve ortak bir taahhüt gerektirir[475].

Elektronik harp bilgi güvenliği ve kamu yönetimlerinde, kuruluşları sürekli gelişen siber tehdit ortamından korumak için etkili güvenlik politikaları oluşturmanın temel görevini ve politika geliştirmenin inceliklerini, risk değerlendirmesi, politika bileşenleri, uygulama stratejileri ve yinelemeli politika uyarlama süreci hakkında öngörü sağlamaktadır[476]. 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[477]. 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

---

[474] Güngör ve Güney, **a.g.e**., ss.131-146

[475] **a.g.e**., ss.131-146

[476] Özdemir ve Uluyol, **a.g.e.,** ss.649-666

[477] Sertçelik, **a.g.e**., ss.25-42

olan yeni bir savaş biçiminin ortaya çıkmasına neden olmaktadır[478]. 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[479]. 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[480].

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[481]. Teknoloji ilerlemeye devam ettikçe, elektronik harp dünyasında saldırı ve savunma arasındaki denge hassas olmaya devam edecek ve bilgi güvenliği alanında sürekli uyanıklık ve yenilik ihtiyacını doğurmaktadır[482]. 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 kullanılabilir ve zayıf noktaların kullanılmasına olanak tanıyabilmektedir[483]. Elektronik harp stratejileri daha sofistike hale geldikçe, bilgi güvenliği önlemleri de buna ayak

---

[478] Güngör ve Güney, **a.g.e**., ss.131-146

[479] Onur Korucu, "Yeni Normal Dünya Düzeninin Siber Güvenlik ve Bilgi Güvenliği Etkileri", **Yönetim Bilişim Sistemleri Dergisi**, Cilt.7, Sayı.1, 2021, ss.44-60

[480] Güngör ve Güney, **a.g.e**., ss.131-146

[481] Sertçelik, **a.g.e**., ss.25-42

[482] Korucu, **a.g.e**., ss.44-60

[483] Özdemir ve Uluyol, **a.g.e.,** ss.649-666

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[484].

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. Bu çalışma, bilgi güvenliği önlemlerinin çok yönlü dünyasını ve bunların elektronik harp alanındaki önemli rolünü inceleyerek kritik dijital varlıkların korunmasındaki önemini vurgulamaktadır.

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[485]. Bilgi güvenliği ise ister dijital ister analog olsun, her türlü bilginin yetkisiz erişime, ifşaya, değiştirilmeye veya imhaya karşı korunmasını kapsayan daha geniş bir kavram olarak, dijital sistemlerin ötesinde daha geniş bir varlık yelpazesini kapsar ve fiziksel belgeleri, iletişim kanallarını ve fikri mülkiyeti kapsamaktadır[486].

---

[484] Sertçelik, **a.g.e**., ss.25-42

[485] Korucu, **a.g.e**., ss.44-60

[486] Özdemir ve Uluyol, **a.g.e.,** ss.649-666

Bilgi güvenliğinin sağlanabilmesi ve elektronik harp saldırılarına karşın, düzenli yazılım güncellemeleri, güçlü parola yönetimi ve kullanıcı eğitimi gibi en iyi uygulamaları teşvik etmek, elektronik harbin temel bileşenleri arasında yer almaktadır[487]. 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[488].

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[489]. 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[490].

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[491]. 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

---

[487] Yılmaz, Ulus ve Gönen, **a.g.e,** ss.133-146

[488] Hakan Aydın, "Yönetim Bilgi Sistemlerinde (YBS) Siber Güvenliğin Önemi", **Bilgisayar Bilimleri ve Teknolojileri Dergisi**, Cilt.3, Sayı,2, 2022, ss.1-8

[489] Yılmaz, Ulus ve Gönen, **a.g.e,** ss.133-146

[490] Çalışkan, **a.g.e**., ss.1-32

[491] Yılmaz, Ulus ve Gönen, **a.g.e,** ss.133-146

planlamaları gerçekleştirilebilir[492]. 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[493].

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[494]. 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[495]. 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[496].

Elektronik harp güvenlik operasyon merkezleri, güvenlik olaylarını izlemek, tespit etmek ve bunlara yanıt vermek için merkezi bir merkez 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

---

[492] Aydın, **a.g.e.**, 2022, ss.1-8

[493] Yılmaz, Ulus ve Gönen, **a.g.e,** ss.133-146

[494] Aldemir ve Kaya, **a.g.e**., ss.6-27

[495] Yılmaz, Ulus ve Gönen, **a.g.e,** ss.133-146

[496] Aldemir ve Kaya, **a.g.e**., ss.6-27

bileşenleridir[497]. 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[498].

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[499]. 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[500].

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. Ülkeler, elektronik harp tehditlerini ele almak için iç yasalarını güncellemeli ve güçlendirmeli ve elektronik harp tehditleri, siber suçların tanımlanması, cezaların ana hatlarını belirlemeyi ve siber suç soruşturmalarında sınır ötesi iş birliği için mekanizmalar oluşturulması gerekmektedir[501]. Kamu yönetimleri ülkelerin ulusal hükümetler ve özel sektör kuruluşları arasındaki iş birliği, 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.

---

[497] Aydın, **a.g.e.**, 2022, ss.1-8

[498] Korucu, **a.g.e**., ss.44-60

[499] **a.g.e**., ss.44-60

[500] Yılmaz, Ulus ve Gönen, **a.g.e,** ss.133-146

[501] Korucu, **a.g.e**., ss.44-60

3.4.2. Kamu Yönetimi ve Elektronik 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 edeceği öngörülmektedir. 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 genel halk arasında elektronik harp tehditleri hakkında farkındalığı artırmak, bilgi açığını kapatmaya ve genel hazırlığı geliştirmeye yardımcı olacağı değerlendirilmektedir[502].

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 yaklaşım paydaşların, dijital çağın karmaşıklıklarını doğrudan ele alarak herkes için daha güvenli, düzenlenmiş ve dayanıklı bir elektronik ortam içerisinde çalışabilmesine imkân vereceği düşünülmektedir[503].

Bilgi güvenliği yeteneklerinin geliştirilmesi, 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[504]. Kapasite geliştirme girişimleri, bilgi güvenliği bağlamında elektronik harbin istikrarı ve esnekliği teşvik edebileceği değerlendirilmektedir. Elektronik harp diplomasisi yoluyla ülkeler, siber güvenlik

---

[502] Güngör ve Güney, **a.g.e**., ss.131-146

[503] **a.g.e**., ss.131-146

[504] Aldemir ve Kaya, **a.g.e**., ss.6-27

uygulamaları için uluslararası kabul görmüş standartlar geliştirmek üzere birlikte çalışabilir ve bu standartlar, sınırlar ötesindeki politikalara, düzenlemelere ve uygulamalara rehberlik edebileceği öngörülmektedir[505].

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[506]. 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[507]. 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[508]. Teknoloji

[505] Güngör ve Güney, **a.g.e**., ss.131-146

[506] Yılmaz, Ulus ve Gönen, **a.g.e,** ss.133-146

[507] Özdemir ve Uluyol, **a.g.e.,** ss.649-666

[508] Aydın, **a.g.e**, 2017, s.10

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[509]. 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 çıkartmaktadır[510].

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[511]. 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[512].

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

---

[509] Cenay Babaoğlu ve Hasan Alpay Karasoy, "Kamu Yönetiminde Blokzincir: Kullanım Alanları ve Örnek Uygulamalar", **Sosyoekonomi**, Cilt.30, Sayı.52, 2022, ss.283-297

[510] Özdemir ve Uluyol, **a.g.e.,** ss.649-666

[511] Babaoğlu ve Karasoy, **a.g.e**., ss. 283-297

[512] Mustafa Veysel Güldoğan ve Şevki Işıklı, "Siber Savaşta Mütekabiliyet", **Academic Journal of Information Technology**, Cilt.13, Sayı.51, 2022, ss.289-319

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[513]. 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[514].

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 oluşturması 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[515]. Devlet kurumları, özel sektör paydaşları ve uluslararası ortaklar arasındaki iş birliği, elektronik tehditleri azaltmak için 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[516]. Dijital devrimle birlikte, elektronik harp teknikleri iletişim ağları, ulaşım sistemleri ve devlet hizmetleri

---

[513] Babaoğlu ve Karasoy, **a.g.e**., ss. 283-297

[514] Güldoğan ve Işıklı, **a.g.e.,** ss.289-319

[515] **a.g.e.,** ss.289-319

[516] Annamaria Edegbeme-Belaz ve Andras Kerti, "A New Approach to Information Security Auditing in Public Administration", **Hadmernok**, Cilt.17, Sayı.3, 2022, ss.109-131

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[517].

Dijital altyapıya artan güven, kamu yönetimini bilgisayar korsanlığı girişimlerinden veri ihlallerine kadar değişen siber tehditlere karşı duyarlı hale getiriyor[518]. 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 bir 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[519].

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[520]. 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.

---

[517] Edegbeme-Belaz ve Kerti, **a.g.e.,** ss.109-131

[518] Oğuz Özaltın ve Mevlüt Ersoy, "Kamu Yönetiminde Blokzincir Kullanımı: D5 Örneği", **Nevşehir Hacı Bektaş Veli Üniversitesi SBE Dergisi**, Cilt.10, Sayı.2, 2020, ss.746-763

[519]Özaltın ve Ersoy, **a.g.e.**, ss.746-763

[520] **a.g.e**., ss.746-763

Teşkilatlar arasında uyanık, uyumlu ve işbirlikçi kalarak kamu yönetimi, hizmet ettikleri vatandaşlara karşı temel sorumluluklarını yerine getirirken elektronik harp ortamında yol katedebilir[521]. 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[522]. 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;

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,

---

[521] Yusuf Uysal, "Klasik Kamu Yönetiminden Yeni Kamu İşletmeciliği ve Post-YKİ'ye Kamu Hizmetlerinin Değişimi ve Dönüşümü Üzerine Bir Değerlendirme", **International Journal of Management and Administration**, Clit.4, Sayı.7, 2020, ss.112-135

[522] Uysal, **a.g.e.,** ss.112-135

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

Yetkisiz erişimi engellemenin en etkili önlemlerinden biri, çok faktörlü kimlik doğrulama uygulanması, çok faktörlü kimlik doğrulama, 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 azaltır,

Kamu yönetimi, kişisel bilgiler, mali kayıtlar ve tıbbi geçmişler dahil olmak üzere çok sayıda hassas vatandaş verisiyle ilgilenir ve güçlü şifreleme yöntemlerinin uygulanması, verilerin ele geçirilse bile yetkisiz kişiler tarafından okunamaz ve kullanılamaz durumda kalmasını sağlanması gibi önlemler ile gerçekleştirile bilinmektedir[523].

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[524]. 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,

[523] Edyta Karolina Szczepaniuk ve diğerleri, "Information Security Assessment in Public Administration", **Computers & Security**, Cilt.90, 2020, ss.1-11
[524] Szczepaniuk ve diğerleri, **a.g.e**., ss.1-11

elektronik harp ve bilgi güvenliğinin çeşitli yönlerini içeren kapsamlı bir güvenlik çerçevesi oluşturmalıdır.

Bilgi güvenliğinde elektronik harp, elektronik sistemleri hedeflemek ve korumak için çeşitli yöntemleri içermektedir. Bu bağlamda elektronik harp temel yönlerinden bazıları şunlardır;

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 kalmakta, hassas bilgileri, kritik altyapıyı ve vatandaşların güvenini koruma sorumluluğu doğrudan kamu yöneticilerinin omuzlarındadır[525]. Kamu yönetimi, potansiyel tehditleri gerçek zamanlı olarak tespit etmek için sürekli izleme sistemleri kurmalıdır. Bu, güvenlik olaylarına anında yanıt verilmesini sağlayarak, iyi tanımlanmış prosedürler, iletişim protokolleri ve rollerden oluşan bir olay müdahale planı, güvenlik ihlallerine koordineli ve verimli bir şekilde yanıt verilmesini sağlamak için gereklidir[526].

Fiziksel güvenlik, dijital güvenlik kadar önemli olup, kamu idareleri, devlet binalarını, hassas teçhizatı ve personeli korumak için fiziksel erişim kontrolleri, gözetim sistemleri ve güvenlik personeli uygulamalıdır. Kamu yönetimleri, güvenli iletişim kanalları gerektiren hassas bilgilerle ilgilenir ve elektronik posta iletişimleri, güvenli mesajlaşma platformları ve sanal özel ağlar için uçtan uca şifreleme, verileri iletim sırasında müdahaleye karşı koruyabilir ve son olarak güvenlik ihlallerinin ve diğer felaketlerin etkisini azaltmak için kamu idarelerinin sağlam iş sürekliliği ve felaket kurtarma planları olmalıdır[527]. Bu planların düzenli olarak test edilmesi ve

---

[525] S.Mustafa Önen ve Salim Kurnaz, "Siber Güvenlik Politikalarının Kamu Yönetimine Yansıması", **Turgut Özal Uluslararası Ekonomi ve Siyaset Kongresi** IV, 11-12 Mayıs 2017, Malatya, ss.732-752

[526] **a.g.e.**, ss.732-752

[527] **a.g.e.**, ss.732-752

güncellenmesi, krizler sırasında dayanıklılığı ve minimum kesinti süresini sağlamak için çok önemlidir.

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[528]. 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:

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

[528] Önen ve Kurnaz, **a.g.e.**, 2017, ss.732-752

stratejileri ve uygulamaları ile sağlıklı bir kamu yönetişimi gerçekleştirmek mümkün hale gelmektedir[529].

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[530]. Kamu idareleri, kişisel verileri korumak için veri koruma düzenlemelerine uymalıdır. Avrupa Birliği'ndeki Genel Veri Koruma Yönetmeliği gibi yasalar 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[531]. 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[532].

---

[529] Önen ve Kurnaz, **a.g.e.**, 2017, ss.732-752

[530] Ahmet Barbak, "Sürdürülebilir Güvenlik Yaklaşımı ve Kamu Yönetimi İlişkisi Üzerine Kavramsal Bir İnceleme", **AKÜ iktisadi ve İdari Bilimler Fakültesi Dergisi**, Cilt.20, Sayı.2, 2018, ss.37-50

[531] Barbak, **a.g.e.,** ss.37-50

[532] Önen ve Kurnaz, **a.g.e.**, 2017, ss.732-752

3.4.3. Elektronik Harp'te Etik Kavramı

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[533]. 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[534].

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[535].

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 yayılması kamu idareleri, siber silahların geliştirilmesinde ve kullanılmasında etik ikilemlerle karşı karşıya kalabilmekte ve bu tür silahların saldırı

---

[533] Müslüm Kayacı, "Kamu Yönetiminde Etik Bağlamında Güvenlik Hizmetleri Etiğine Bir Bakış", **Sosyal Bilimler Akademi Dergisi**, Cilt.2, Sayı.1, 2019, ss.50-69

[534] Önen ve Kurnaz, **a.g.e.**, 2017, ss.732-752

[535] **a.g.e.**, 2017, ss.732-752

operasyonlarında kullanılması potansiyel olarak daha geniş bir silahlanma yarışına ve siber çatışmaların tırmanmasına yol açabilir[536]. 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[537]. 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[538].

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[539]. 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

---

[536] Kayacı, **a.g.e**, ss.50-69

[537] **a.g.e**, ss.50-69

[538] **a.g.e**, ss.50-69

[539] Barbak, **a.g.e.,** ss.37-50

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[540]. 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[541]. 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[542].

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[543].

Elektronik harp ve bunun etik sonuçları hakkındaki tartışmalarda halkla ve paydaşlarla etkileşim kurmak çok önemli olduğu düşünülmektedir. Kamu idareleri

---

[540] Barbak, **a.g.e.,** ss.37-50
[541] Önen ve Kurnaz, **a.g.e.**, 2017, ss.732-752
[542] Kayacı, **a.g.e**, ss.50-69
[543] **a.g.e**, ss.50-69

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.

3.4.4. Elektronik Harp ve Hukuk İlişkisi

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[544]. 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[545]. 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[546].

Kamu yöneticileri, elektronik harp uygulamalarını ulusal güvenlikte yürütürken ulusal yasa ve yönetmeliklere uymak zorundadır. Bu yasalar, veri koruma, mahremiyet ve siber yeteneklerin saldırgan amaçlarla kullanılması gibi konuları ele almaktadır. 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[547]. Kamu idareleri, siber olayların sorumluluğunu doğru bir şekilde atfetmek için proaktif mekanizmalara sahip olmalı ve siber atıf, siber

---

[544] Önen ve Kurnaz, **a.g.e.**, 2017, ss.732-752

[545] Nurullah Sandilaç, "Siber Suç, Siber Terör ve Siber Savaş Üçgeninde Siber Dünya", **Bilişim Hukuk Dergisi,** Cilt.4, Sayı.1, 2022, ss.141-190

[546] Çalışkan, **a.g.e**., ss.1-32

[547] Sandilaç, **a.g.e.,** ss.141-190

tehditlere yanıt verirken yasal ve diplomatik amaçlar için kritik öneme sahip olmaktadır[548].

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[549]. 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[550]. 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[551]. Bilgi güvenliği, bilgileri ve dijital varlıkları yetkisiz erişim, ifşa, değiştirme veya imhadan korumak için tasarlanmış bir dizi uygulama, teknoloji ve politikayı kapsamaktadır[552]. 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[553]. Ancak bilginin güvenliği yine elektronik harp uygulamalarından olan elektronik taarruz ve elektronik destek faaliyetlerinden

---

[548] Sandilaç, **a.g.e.,** ss.141-190

[549] **a.g.e.,** ss.141-190

[550] Kayacı, **a.g.e**, ss.50-69

[551] Önen ve Kurnaz, **a.g.e.**, 2017, ss.732-752

[552] Dülger, **a.g.k.**

[553] Szczepaniuk ve diğerleri, **a.g.e**., ss.1-11

korunarak bilgi orijinal kalmaktadır. 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[554].

3.4.5. Ulusal Güvenlikte Elektronik Harp

Kamu yönetimi, devletin yönetim faaliyetlerinin yararlı ve verimli bir biçimde düzenlenmesiyle uğraşan bilim dalı olarak tanımlanmasından kaynaklı milli güvenliği ilgilendiren devlet yönetim faaliyetleri elektronik harp ile doğrudan bağlantısı bulunmakta, bilgi ve teknoloji çağında diğer ulusların saldırılarına ve tehditlerine karşı koruma ve misilleme gerçekleştire bilinmesi için elektronik harbe ihtiyaç duyulmaktadır[555]. Milli güvenliğin sağlanması için kamu yönetimlerinde yer alan tüm kamu da iş yapabilme gücüne sahip kişilerin elektronik harp hakkında bilgilendirilmesi gerekmektedir.

Devletlerin milli güvenliği sağlamak maksadıyla önemli bir role sahip olan elektronik harp, sivil ve askeri operasyonlarda aktif olarak kullanılmaktadır. Mili güvenlik politikalarında istihbarat ve askeri birliklerin terör örgütleri, yabancı devletler ve her türlü milli güvenlik tehdidine karşın bilgi toplama ve muhtemel tehlikelerin bertaraf edilmesine elektronik harp uygulamalarının doğrudan veya dolaylı olarak katkısı bulunmaktadır. Devletlerin güvenlik açıklıklarının tespit edilmesi, tehdit oluşturacak faaliyetlere karşı stratejik çözümler üretilmesi ve karar vericilere doğru politikalar izlenmesi konusunda yardımcı olmaktadır[556].

Elektronik harp, istihbarat literatüründe ciddi bir öneme sahip ve elektronik harp bileşenlerinin temelini oluşturan teknik istihbarat faaliyetleri küresel politikaların

---

[554] Önen ve Kurnaz, **a.g.e.**, 2017, ss.732-752

[555] Sandilaç, **a.g.e.,** ss.141-190

[556] Barbak, **a.g.e.,** ss.37-50

şekillenmesinde öncü olmaktadır. Bilgi ve iletişim teknolojilerinin 21. Yüzyılda hızlı gelişimi, toplumların sosyal yaşamında ve devletler arası ilişkilerde, teknoloji kabiliyetlerinin tespit ve analiz edilmesinin önemi ortaya çıkmaktadır.

Elektronik harp ile aktif bilgi kullanımı, analiz edilen verilerin, kişisel, kurumsal veya devletlerin kendi menfaatleri doğrultusunda bilgi ve iletişim teknolojileri kabiliyetlerini geliştirmek, devlet yöneticilerine politika oluşturulmasında ve milli güvenlik stratejilerinin belirlenmesinde üstünlük sağlamak maksadıyla gerçekleştirilmektedir. Elektronik harp ile analizi gerçekleştirilen bilginin gücü ile karar verme süreçlerinin doğruluğu, devlet kurumları, savunma ve güvenlik kuruluşları yanı sıra sivil paydaşlar ile bilginin yayılması toplumların güveninin ve refahının artması mümkündür.

Elektronik harp düşman ve potansiyel tehdit unsurlarının faaliyetlerini sentezlenerek, savunma sanayi ve teknolojilerinin imkân ve kabiliyetlerinin tespit ve analiz edilmesi ile milli güvenliğe karşı oluşabilecek tehditlere hazırlıklı olunması ve hızlı karşı cevap verme imkânı tanımaktadır[557]. Tehditlerin değerlendirilmesi, bilgilendirici savunma stratejileri ve küresel silah sistemlerinin tespit edilerek hazırlık yapılması milli güvenlikte elektronik harbin rolünü ifade etmektedir.

Bilgi ve iletişim teknolojilerini yakından takip etmek, ulusal teknoloji araştırma ve geliştirme politikaları için fırsatların değerlendirilmesi istihbarat faaliyetleri ile desteklenmektedir. Diğer devletlerin bilgi ve iletişim teknolojilerinin tespit ve analiz edilmesi, kamu kuruluşları, özel şirketlerin ve endüstrilerin küresel pazarda rekabet avantajlarının korunmasına ve teknoloji transferi, bahsedilen istihbarat faaliyetleri ile gerçekleştirilmektedir. Elektronik harp milli güvenlik ve savunma stratejilerinde hayati bir öneme sahiptir. Diğer devletlerin ve tehdit olabilecek unsurların kabiliyetleri ve niyetlerini etkin bir öngörü meydana gelmesi için elektronik harp çalışmalarına daha çok yer verilmesi gerekmektedir[558].

---

[557] Önen ve Kurnaz, **a.g.e.**, 2017, ss.732-752

[558] Sandilaç, **a.g.e.,** ss.141-190

Sonuç

Teknolojik gelişmelerin ve gelişen tehdit ortamının damgasını vurduğu bir çağda, kuruluşlar ve bireyler, proaktif güvenlik önlemleri almanın önemini anlamalıdır. Etkili güvenlik politikaları uygulayarak, düzenli risk değerlendirmeleri yaparak, ortaya çıkan tehditlere karşı cevap vererek ve bir güvenlik bilinci kültürü geliştirerek, riskleri azaltmaya ve kendimizi olası zararlardan korumaya çalışabiliriz. Bilgi güvenliği tek seferlik bir çaba değil, sürekli adaptasyon ve aktif bir zihniyet gerektiren sürekli bir taahhüttür. Yalnızca birlikte çalışarak, bilgi ve en iyi uygulamaları paylaşarak ve tetikte kalarak bu sürekli bağlantılı dijital dünyada değerli bilgi varlıklarımızı etkili bir şekilde koruyabiliriz. Bilgi Güvenliği Yönetim Sistemleri, hassas bilgilerini korumayı ve güvenlik risklerini azaltmayı amaçlayan kuruluşlar için vazgeçilmez bir araç haline gelmiştir. Kamu kurumları ve özel kuruluşlar, bir bilgi güvenliği yönetim sistemini uygulayarak, sürekli değişen tehdit ortamını ele alan, güvenlik duruşlarını geliştiren ve ilgili düzenlemelere ve standartlara uyumu sağlayan sağlam bir çerçeve oluşturabilir. Risk değerlendirmesi, güvenlik kontrolleri, olay yönetimi ve sürekli izleme ve iyileştirme dahil olmak üzere bir bilgi güvenliği yönetim sisteminin temel bileşenleri, bilgi varlıklarının korunmasına yönelik kapsamlı bir yaklaşım sağlar. Ayrıca, bilgi güvenliği yönetim sisteminin faydaları, yalnızca güvenliğin ötesine geçerek artan paydaş güvenini, gelişmiş iş sürekliliğini ve iyileştirilmiş genel kurumsal esnekliği kapsamaktadır. Kuruluşlar gelişen dijital ortamda gezinmeye devam ettikçe, Bilgi Güvenliği Yönetim Sistemlerinin benimsenmesi, bilgilerin gizliliğini, bütünlüğünü ve kullanılabilirliğini korumada hayati bir rol oynayacak ve onların güvenli ve esnek bir şekilde gelişmelerini sağlayacaktır.

Kişisel verilerin korunması dijital hayatımızın vazgeçilmez bir parçası haline gelmiştir. Teknolojiye giderek artan güven ve toplanan, saklanan ve paylaşılan çok büyük miktarda kişisel bilgi ile, gizliliğe ve güvenliğe öncelik vermek çok önemlidir. Hükümetler, kuruluşlar ve bireyler, güçlü veri yönetişim çerçeveleri, şifreleme protokolleri, güvenli depolama uygulamaları ve kullanıcı onayı mekanizmaları dahil

olmak üzere kapsamlı veri koruma önlemleri uygulamanın önemini anlamalıdır. Çalışmanın birinci bölümünde bilgi güvenliği ve kişisel verilerin mahremiyeti konusunda farkındalığı artırmak ve sorumlu veri işleme uygulamalarını teşvik etmek, bireylerin kişisel bilgilerini korumalarını sağlamak için çok önemli olduğuna değinilmiştir. Kişisel verilerin korunduğu ve mahremiyete saygı duyulan güvenilir bir dijital ekosistemi yalnızca kolektif çabalar, paydaşlar arasındaki iş birliği ve aktif veri koruma standartlarına bağlılık ile bilgi güvenliği yönetim sistemleri incelenmiştir.

Çalışmanın ikinci bölümünde değinilen dijital dönüşüm, modern çağda kurumsal büyüme ve dayanıklılık için bir katalizör olarak ortaya çıkmıştır. Dijital teknolojilerin derin etkisi ve müşterilerin ve paydaşların sürekli gelişen beklentileri, dijital ortama uyum sağlamak ve gelişmek için aktif bir yaklaşım gerektiriyor. Dijital dönüşümü benimseyen kuruluşlar, yenilik için yeni fırsatların, gelişmiş müşteri deneyimlerinin, kolaylaştırılmış operasyonların ve artan verimliliğin kilidini açmaktadırlar. Ancak dijital dönüşüm tek seferlik bir proje değil; sürekli öğrenme, çeviklik ve değişimi ve teknolojik ilerlemeyi kucaklamaya yönelik kültürel bir değişim gerektiren devam eden bir süreç olduğu ve günümüzde dijital dönüşümün başlıca etmenlerine yer verilmiştir. Kamu kurumları ve özel kuruluşlar, dijital dönüşümü benimseyerek ve gelişen teknolojilerden kendi avantajlarına yararlanarak, dijital ortamda gezinmek ve sunduğu fırsatlardan yararlanmak için, donanımlı olarak kendilerini sektörlerinde liderler olarak konumlandırabilmesi için dijital dönüşümde yer alan faktörler hakkında açıklayıcı bir bölüm oluşturulmuştur.

Sosyal bilimlerde ve siyasal iletişimde dijital dönüşüm, araştırmacıların ve uygulayıcıların kendi alanlarını yeni ve dinamik yollarla keşfetmelerini ve bunlarla ilişki kurmalarını sağlayarak sosyal bilimler ve siyasal iletişimi yeniden şekillendirdi. Dijital platformların ve araçların kullanımı, büyük miktarda verinin toplanmasına ve analiz edilmesine olanak tanıyarak insan davranışı, siyasi tercihler ve bilgi akışı kalıpları hakkında öngörüler sunuyor. Bununla birlikte, dijital çağ aynı zamanda yanlış bilgilerin yayılması, mahremiyet endişeleri ve dijital uçurum gibi zorluklar da sunuyor. Araştırmacıların, politika yapıcıların ve iletişimcilerin bilgiyi ilerletmek, demokratik söylemi kolaylaştırmak ve toplumsal sorunları ele almak için dijital

teknolojinin potansiyelinden yararlanırken bu zorlukları etik ve sorumlu bir şekilde aşması zorunlu hale gelmektedir. Dijital yenilikleri, disiplinler arası iş birliğini ve dijital verilere eleştirel bir yaklaşımı benimseyerek, toplumun karmaşıklıklarına dair daha derin öngörüler elde etmek, bilgiye dayalı politikaları şekillendirmek ve daha anlamlı ve kapsayıcı siyasi iletişimi teşvik etmek için dijital çağın gücünden yararlanılmaktadır.

Çalışmanın üçüncü bölümünde, elektronik harp modern askeri operasyonların vazgeçilmez bir yönü haline geldiği ve giderek daha fazla teknoloji odaklı bir savaş alanında stratejik avantajlar sunmasından bahsedilmiştir. Bir yandan kendi elektronik sistemlerini korurken bir yandan da düşmanın elektronik sistemlerini bozma, imha etme veya aldatma yeteneği, taktiksel bir üstünlük sağlamada çok önemlidir. Teknoloji hızlı bir şekilde ilerlemeye devam ederken, elektronik savaş da karmaşık siber tehditlerin çoğalması ve birbirine bağlı ağlara artan güven gibi ortaya çıkan zorlukları ele almak için gelişmelidir. Akademik çalışmalar ve güvenlik birimleri arasındaki iş birliği ile birlikte, elektronik harp sistemlerinin geliştirilmesi ve satın alınması, operasyonel başarının yanı sıra milli güvenliğin sağlanmasında etkili olacaktır.

Elektronik harp ile gerçekleştirilen istihbarat faaliyetlerini sırasıyla inceledik. Teknik istihbarat, çeşitli aktörlerin yetenekleri ve niyetleri hakkında temel ön görüler sağlayarak, istihbarat topluluğunda bir mihenk taşı görevi görür. Teknik verilerin toplanması, analizi ve yorumlanması yoluyla kuruluşlar ve hükümetler rekabet avantajı elde edebilir, tehditleri değerlendirebilir ve bilinçli kararlar alabilir. Mühendislik, fizik, bilgisayar bilimi ve diğer bilimsel disiplinleri birleştiren teknik istihbaratın disiplinler arası doğası, analistlerin karmaşık teknik sistemleri anlamalarını ve güvenlik açıklarını belirlemelerini sağlamaktadır. Teknoloji hızlı bir şekilde ilerlemeye devam ederken, ortaya çıkan tehditlere ve gelişmelere ayak uydurmada teknik istihbaratın rolü daha da kritik hale geliyor. Hükümetler, elektronik harp yeteneklerine yatırım yaparak, bilimsel uzmanlar arasında iş birliğini teşvik ederek ve gelişmelere sürekli uyum sağlayarak ulusal güvenliği geliştirmek, kritik altyapıyı korumak ve giderek daha karmaşık ve birbirine bağlı bir dünyada önde olmak için elektronik harbin gücünden yararlanmaktadır.

Günümüz de elektroniğin hayati önemi, kamu yönetimlerinde, endüstrilerde ve gündelik sosyal yaşamın her anında bir elektronik bileşen yer almaktadır. Elektronik harp ’in önemi teknoloji çağının vazgeçilmezi olan elektronik bileşenlerin hayatımız kolaylaştırmak için, zaman tasarrufu gibi birçok avantaj sağlamakta iken, devletler için bu durum ulusal güvenlik problemlerini ortaya çıkartmaktadır. Bilgi güvenliği ve elektronik harp çalışması bu problemlerin tümünü incelemekte ve çözüm önerileri sunmaktadır.

Çalışmanın amacı ise günümüzde kullanılan sosyal medya uygulamaları, mesajlaşma programları ve benzeri bütün elektronik uygulamaların günlük hayatımız kolaylaştıran bu uygulamaların tümü kişisel verilere erişimi 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 kullanılamayacağı açıkça ortadadır. Çalışma günümüz sosyal bilimlerinde elektronik harp ’in yerini alması ve elektronik harp üzerinde çalışmalara daha çok yer verilmesinin gerekliliğini ifade etmektedir. Çalışmanın son bölümünde kamu yönetimlerini doğrudan ilgilendiren ulusal güvenlik ve bilgi güvenliğinin elektronik harp ile bağlantılı olduğu ifade edilmiştir. 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 alan her personelin bilgilendirilmesi gerekliliği ifade edilmektedir. Elektronik harp hakkında oluşabilecek endişelerin başında yer alan etik konusuna değinilmiş, hukuki olarak ulusal ve uluslararası çalışmaların gerekliliğinden söz edilmiştir.

Bilgi ve iletişim teknolojilerinin temelini oluşturan elektronik kavramı, ikinci bölümde detaylı bir şekilde ifade edilmiş olup, elektronik kavramını 21.yüzyılda hayatımızda çıkartılamaz bir parçası olduğu, bireysel, kurumsal ve devlet

yönetimlerinde, geleneksel yönetim ve işleyişlerin yerini yeni teknolojilere bırakmaktadır. Ulusal güvenlik endişelerinin, bilgi ve iletişim teknolojileri vasıtasıyla gerçekleştirilen istihbarat faaliyetleri genelde siber uzay kavramı içerisinde yer almakta olup, elektronik olmadan siber uzay bileşenlerin bir anlam ifade etmeyeceği dolayısıyla teknik istihbarat, sinyal, elektronik, muhabere, görüntü sosyal medya ve siber istihbarat kavramsal olarak elektronik harp başlığı altında literatürde yer alması çalışmanın amacını ifade etmektedir.

KAYNAKÇA

ADA, Mehmet; "Nato Üyesi Ülkelerin Siber Güvenlik Stratejileri Açısından İncelenmesi", **Yüksek Lisans Tezi,** Gazi Üniversitesi, 2018, ss. 43-49

AĞIR, Ahmet; "Bilişim Toplumuna Geçiş Sürecinde Bilgi Yönetimi Yaklaşımı", **İstanbul Üniversitesi İletişim Fakültesi Dergisi**, Cilt 0, Sayı 30, 2007, s. 4

AHMAD, Atif ve Rachelle Bousa; "Protecting Organizational Competiteve Advantage: A Knowledge Leakage Perspective", **Elsevier (Computers & Security)**, Cilt 1, Sayı 42, 2014, ss. 27-39.

AKAL, Mert; "Bilişim Firmalarında Bilgi Güvenliği Farkındalığı", **Yüksek Lisans Tezi**, Ufuk Üniversitesi, Ankara, 2022, s. 24

AKÇAY, Muammer Mehmet Canbaz ve Muhemmet Ömer Diş; "Akıllı Konut Uygulaması", **Estudam Bilişim Dergisi,** Cilt.3, Sayı.1, 2022, ss.1-5

AKDOĞAN, Zeynep; "Kamu Kurumlarında Bilgi Güvenliği Yönetim Sistemleri Politika Geliştirme Metodolojisi", **Doktora Tezi**, Ankara Üniversitesi, Ankara, 2022, s. 99

AKKAYA, Ahmet Zeki ve diğerleri; "**Analog-Dijital Elektronik Atölyesi**", 1.Baskı, Meb Yayınları, Ankara, 2020, ss. 22-59.

AKKAYA, Cenk ve Ceren Uzar; "Data Mining and Application Of It To Capital Markets", **International Journal Of Economics and Finance Studies**, Cilt.3., Sayı.2, 2011, ss.58-67

AKKAYA, Sinem ve Harun Özbay; "Otonom Araçların Akıllı Ulaşım Politikaları Üzerindeki Etkileri", **Akıllı Ulaşım Sistemleri ve Uygulamaları Dergisi,** Cilt.5, Sayı.2, 2022, ss. 200-210

AKKEMİK, K. Ali; "Bilgi Ekonomileri ve Ekonomik Kalkınma: Bir İktisadi Model Yardımıyla Çeşitli Senaryoların Sonuçları", **Bilgi Yönetimi Disiplini ve Uygulamaları,** Ed. Mustafa Sağsan, 1.Baskı, Siyasal Kitabevi, Ankara, 2010, ss. 122-141

AKKUŞ, Berkant; "Devletlerin Pozitif İnsan Hakları Yükümlülüğü ve Kolluk Operasyonları Sırasında Otonom Silah Sistemlerinin Kullanımı", **Mehmet Akif Ersoy Üniversitesi Sosyal Bilimler Enstitüsü Dergisi**, Cilt. 1, Sayı.36, 2022, ss. 76-94

AKSARAY, Semra; "Siber Zorbalık", **Çukurova Üniversitesi Sosyal Bilimler Enstitüsü Dergisi**, Cilt.20, Sayı.2, 2011, ss.405-432

AKTAN, Ertuğrul ve Belgin Aydıntan; "Cameron-Freeman Örgüt Kültürü Türleri Ekseninde Örgüt Kültürü ve Bilgi Güvenliği Algısı İlişkisi: Devlet Üniversitelerinde Bir Uygulama", **Journal of Business Research Turk,** Cilt.8, Sayı.4, 2016, ss.324-344

AKTEL, Mehmet Süleyman Öğrekçi ve Bedrettin Özmen; "E-Devlet ve Yönetim İlişkileri", **Gazi Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi**, Cilt.19, Sayı.3, 2017, ss.765-787

AKYÖN, Fehmi Volkan; "Bilgi Kavramı Ve Yönetimi", **Öneri Dergisi,** Cilt. 4, Sayı. 15, 2001, ss.167-172.

AL-SEHRAWY, Ramy vd.; "A Knowledge Management Strategy for Urban Digital Twins", https://www.researchgate.net/publication/362127397_, (Erişim Tarihi: 13.03.2023).

ALDEMİR, Ceray ve Merve Kaya; "Bilgi Toplumu, Siber Güvenlik ve Türkiye Uygulamaları", **Kamu Yönetimi ve Politikaları Dergisi**, Cilt.1, Sayı.1, 2020, ss.6-27

ALGULIYEV, Rasim ve diğerleri; "Information Security as a National Security Component", **Information Security Journal A Global Perspective**, Cilt 30, Sayı 47, 2022, ss, 1-18.

ALPTEKİN, Zeynep Mine; "Dijitalleşme ve Dijital Sosyal Sorumluluk İletişimi", **Uluslararası Medya ve İletişim Araştırmaları Hakemli Dergisi**, Cilt.3, Sayı.2, ss.136-155

ALSAFFAR, Hussain; "Operations and Information Management", https://www.researchgate.net/publication/346096473 , Erişim Tarihi: 20.03.2023).

ALTIN, Omca; "AB'nin Siber Güvenlik Alanındaki Politikalarının ve Uygulamalarının Etkinliği: Bir Siber Güvenlik Temsilcisi Olarak AB'nin Yeterliliği", **Çankırı Karatekin Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi,** Cilt.13, Sayı.2, 2023, ss.482-507

ANDREEV, Dmitriy; "The "Smart City" Consept and it's Implementation Prospects", Ural Environmental Science Forum "Sustainable Development of Industrial Region", 31.May 2023, **M. K. Ammosov North-Eastern Federal University, Department of Technosphere Safety**, Yakutie Russia ,2023, ss.1-6

ANDREW, Ng; "İlk Yapay Zekâ Projenizi Nasıl Seçmelisiniz?", **Harvard Business Review Press Artificial Inteligence** , Ed. Utku Umut Bulsun, Çev. Levent Göktem, 1.Baskı, Optimist Yayın Grubu, 2020, ss.127-140

ARABACI, Caner; "Bir Radyo Alıcısının Serencamı", **Selçuk İletişim Dergisi**, Cilt.1, Sayı.1, 1999, ss.133-139

ARIK, Muharrem; "Next-Generation Radar and Electronic Warfare Systems", https://libdigitalcollections.ku.edu.tr/digital/collection/TEZ/id/28127 ,(Erişim Tarihi: 19.05.2023).

ASİLTÜRK, Ayşe; "İşletmelerde Dijital Dönüşüm Yönetiminde Nihai Hedef: Dijital Olgunluk", **Alanya Akademik Bakış Dergisi**, Cilt.5, Sayı,2, 2021, ss.647-669

ATAN, Alper ve diğerler; "**Elektrik -Elektronik Esasları**", 1.Baskı, Meb Yayınları, Ankara, 2020, s.30.

ATMACA, Yıldız ve Faysal Karaçay; "Türkiye'deki Kamu Yönetimi Reformlarında Dijitalleşme ve E-Yönetişim", **Internationl Journal of Management and Administration**, Cilt.4, Sayı.8, 2020, ss. 260-280

AUST, Stefon ve Thomas Ammann; "**Dijital Diktatörlük- Kitlesel Gözetim, Verilerin Kötüye Kullanımı, Siber Savaş**", Çev. Erdinç Yücel ve Hasan Yılmaz, Ed. Hayriye Ünal 3.Baskı, Hece Araştırma, Ankara, 2019, ss. 145-174

AVCI, İsa; "Akıllı Evlerde IoT Teknolojileri ve Siber Güvenlik", **Avrupa Bilim ve Teknoloji Dergisi**, Özel Sayı.34, 2022, ss.226-233

AVUNDUK, Hüseyin ve Merve Kızgın; "Büyük Veri ve Sürekli Denetimde Veri Analizi", Journal of Business in The Digital Age, Cilt.3, Sayı.1, 2020, ss.76-83

AYDEMİR, Emrah; "Siyasal İletişimde Dijital Diplomasi", **Siyasal İletişimin Dijital Dönüşümü**, Ed. Başak Solmaz, 1.Baskı, Literatürk Academia, Konya, 2019, ss. 315-333

AYDIN, Hakan; "Yönetim Bilgi Sistemlerinde (YBS) Siber Güvenliğin Önemi", **Bilgisayar Bilimleri ve Teknolojileri Dergisi**, Cilt.3, Sayı,2, 2022, ss.1-8

AYDIN, Özgür; "Elektronik Harp ile Toplanan Verilerin Veri Madenciliği Yöntemleri ile Analiz Edilmesi", **Yüksek Lisans Tezi**, Bahçeşehir Üniversitesi, İstanbul, 2017, s. 10

BABAOĞLU Cenay ve Hasan Alpay Karasoy; "Kamu Yönetiminde Blokzincir: Kullanım Alanları ve Örnek Uygulamalar", **Sosyoekonomi**, Cilt.30, Sayı.52, 2022, ss.283-297

BAĞCI, Ebru; "Risk Analizi ve Yönetimi", **Turizm İşletmelerinde Güncel Stratejik Yaklaşımlar**, Ed. Ülker Çolakoğlu, Melahat Avşar, H. Erhan Altun ve Ramazan Demir, 1. Baskı, Detay Yayıncılık, Ankara, 2020, ss.161-171

BARAN, Selma ve Emine Şener; "Örgütsel Bilgi Paylaşımı Reddi ile Bilgi Güvenliği Kültürünün İlişkisinin İncelenmesi", **İnsan ve Toplum Bilimleri Araştırmaları Dergisi**, Cilt 1, Sayı 9, 2020, ss. 299-325.

BARBAK, Ahmet; "Sürdürülebilir Güvenlik Yaklaşımı ve Kamu Yönetimi İlişkisi Üzerine Kavramsal Bir İnceleme", **AKÜ iktisadi ve İdari Bilimler Fakültesi Dergisi**, Cilt.20, Sayı.2, 2018, ss.37-50

BAŞTAN, Serhat ve Ramazan Gökbunar; "Kamu Hizmetlerinin Sunumunda E-Devletle İlgili Yeni Gelişmeler: Tümleşik E-Devlet Sistemlerine Doğru", https://acikerisim.deu.edu.tr/ (Erişim Tarihi:25.04.2023).

BAYRAKTAR, Gökhan; "**Siber Savaş ve Ulusal Güvenlik Stratejisi**", 1.Baskı, Yeniyüzyıl Yayınları, İstanbul, 2015, s. 45

BERKE, Allison; "Blok Zincirleri Ne Kadar Güvenli", **Harvard Business Review Press Blockchain** , Ed. Çiğdem Zeynep Aydın, Çev. Taner Gezer, 1.Baskı, Optimist Yayın Grubu, 2019, ss.83-94.

BİLİCİ, Zekeriya ve Veysel Babahanoğlu; "Akıllı Kent Uygulamaları ve Konya Örneği", **Akademik Yaklaşımlar Dergisi**, Cilt.9, Sayı.2,2018, ss.124-139

BORNMAN, Werner ve Les Labuschagne; "A Framework for Information Security Risk Management Communication", https://www.researchgate.net/publication/220803387 , (Erişim Tarihi:30.03.2023).

BOUDRIGA, Noureddine ve Benebdallah Salah; **"**Laying out the Foundation for a Digital Government Model Case Study: Technology, Human Factors, and Policy," Kluwer Academic Publishers, Boston, 2002, s.292'den akt. Ali Şahin ve Erhan Örselli, **Teoriden Uygulamaya E-Devlet**, 2. Baskı, Atlas Akademi, Konya, 2016, s.10

BOZKURT, Aras v.d.; "Dijital Bilgi Çağı: Dijital Toplum, Dijital Dönüşüm, Dijital Eğitim ve Dijital Yeterlilikler", **Açık Öğretim Uygulamaları ve Araştırmaları Dergisi**, Cilt.7, Sayı.2, 2021, s.39

BRYNJOLFSSON, Eric ve Andrew McAfee; "Yapay Zekânın Vaat Ettikleri", **Harvard Business Review Press Artificial Inteligence** , Ed. Utku Umut Bulsun, Çev. Levent Göktem, 1.Baskı, Optimist Yayın Grubu, 2020, ss.19-56

BURAL, Erol Başaran; "**Açık Kaynak İstihbaratında Yeni Bir Boyut Sosyal Medya İstihbaratı**", 1.Baskı, Yeditepe Akademi, İstanbul, 2021, s. 101

CANBEK, Gürol ve Şeref Sağıroğlu; "Bilgi, Bilgi Güvenliği ve Süreçleri Üzerine Bir İnceleme", **Politeknik Dergisi,** Cilt.9, Sayı.3, 2006, ss. 165-174.

CENGİZ, Gönül; "Siber Suçlar, Sosyal Medya ve Siber Etik", **İletişim Çalışmaları Dergisi**, Cilt.7, Sayı.3, 2021, ss.407-424

CHOHAN, Afad Hyder ve diğerleri; "Development of Smart Application for House Condition Survey", **Ain Shams Engineering Journal**, Cilt.13, Sayı.3,2022, ss.1-9

ÇELİK, Murat ve Mehmet Emin Yardımcı; "Dijital Devlet ve İyi Yönetişimin Kökleri", **Siyasal Ekonomik ve Entelektüel Boyutlarıyla İyi Yönetişim**, Ed. Mehmet Karakaş, Selin Karatepe ve Fatma Benli, 1.Baskı, Beta Yayıncılık, İstanbul, 2018, ss.409-430

ÇETİNKAYA, Mehtap; "Kurumlarda Bilgi Güvenliği Yönetim Sisteminin Uygulanması", https://ab.org.tr/ab08/kitap/Bildiriler/MCetinkaya_AB08.pdf , (Erişim Tarihi: 27.03.2023).

ÇITAK, Emre; "Çağımızın Gerekliliği Olarak Sinyal İstihbaratı", **Hitit Üniversitesi Sosyal Bilimler Enstitüsü Dergisi**, Cilt.8, Sayı.2, 2015, ss. 751-770

ÇITAK, Emre; "**Güvenlik ve İstihbarat**", 1.Baskı, Yeniyüzyıl Yayınları, İstanbul, 2017, s. 175

ÇOLAKOĞLU, Çağatayhan; "Tactical Command and Control System and Network Centric Warfare", **Journal of Military and Information Science**, Cilt.2, Sayı.3, 2014, ss. 70-76

CİBAROĞLU, Mehmet Oytun; "Bilgi Teknolojilerinin Bilgi Erişime Etkileri: Literatüre Dayalı Nitel Bir Çalışma", **Bilgi Yönetimi Dergisi**, Cilt.3, Sayı.1, 2020, s.15.

CİNER, Şahin; "**Dijital Demokrasi**", 1.Baskı, Sokak Kitapları Yayıncılık, İstanbul, 2017, s. 45

COENEN, Frans; "Data Mining: Past,Present and Future", **The Knowledge Engineering Review,** Cilt.26, Sayı.1, 2011, ss.25-29

ÇALIŞKAN, Aykut; "Siber Savaş: Bilgi Krizi Mi Yoksa Güvenliği Mi?", **Savunma ve Savaş Araştırmaları Dergisi**, Cilt.33, Sayı.1, 2023, ss.1-32

ÇUBUKÇU, Faruk; **Bilgi Güvenliği Yönetim Sistemi**, 1.Baskı, Pusula 20 Teknoloji ve Yayıncılık A.Ş, İstanbul, 2018, s. 2

DARICILI, Ali Burak; "**İstahbarat 101**", 1.Baskı, Dora Basım-Yayın, Bursa, 2023, s. 190

DARICILI, Ali Burak; "**Siber Uzay ve Siber Güvenlik Nedir**?", 1.Baskı, Dora Basım-Yayın, Bursa, 2017, ss. 14-46

DAVENPORT, Thomas H. ve Thomas C. Redman; "**Dijital Dönüşüm Dört Alandaki Yeteneklere Dayanır**", Çev. Ümit Şensoy 1.Baskı, Optimist Yayın Grubu, İstanbul, 2021, ss. 227-234.

DİNÇ, Veysel; "Elektronik Harp Teknikleri", **Yüksek Lisans Tezi**, Gazi Üniversitesi, Ankara, 2010, s. 8

DÜLGER, Murat Volkan; "İnsan Hakları ve Temel Hak ve Özgürlükler Bağlamında Kişisel Verilerin Korunması", **İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi**, Cilt.5, Sayı.1, 2018, ss.72-143

DÜLGER, Murat Volkan; "Kişisel Verilerin Korunması Hukukunun Getirdikleri ve Yapılması Gerekenler", https://www.researchgate.net/publication/349533304 , (09.04.2023).

EDEGBEME-BELAZ, Annamaria ve Andras Kerti; "A New Approach to Information Security Auditing in Public Administration", **Hadmernok**, Cilt.17, Sayı.3, 2022, ss.109-131

EFENDİOĞLU, Akın ve Emre Sezgin; "E-Devlet Uygulamalarında Bilgi ve Paylaşım Güvenliği", **Çukurova Üniversitesi Sosyal Bilimler Enstitüsü Dergisi**, Cilt.16, Sayı.2, 2007, ss. 219-236

EL KHATIB, Mounir M., Humaid Al Shehhi ve Mohammed Al Nuaimi; "How Big Data and Big Data Analytics Mediate Organizational Risk Management", **Journal of Financial Risk Management**, Cilt.12, Sayı.1, 2023, ss.1-14

ELATTRESH, Jamal Abdulsalam Mohamed; "Bilgi Güvenliği Hizmet Yönetimi: Bilgi Güvenliği Yönetimine Bir Hizmet Yönetimi Yaklaşımı ve Bir Kurumun Müşterilerinin Memnuniyeti ve Güvenirliği Üzerindeki Etkisi", **Doktora Tezi**, Kastamonu Üniversitesi, Kastamonu, 2022, s. 38

EMİNAĞAOĞLU, Mete ve Yılmaz Gökşen; "Bilgi Güvenliği Nedir, Ne Değildir, Türkiye'de Bilgi Güvenliği Sorunları ve Çözüm Önerileri", **Dokuz Eylül Üniversitesi Sosyal Bilimler Enstitüsü Dergisi**, Cilt.11, Sayı.4, 2009, ss. 1-15

ENGİN, Mustafa ve Dilşad Engin; "**Sayısal Elektronik-I**",1.Baskı, Ege Üniversitesi Yayınları, İzmir, 1999, ss.6-41

ERASLAN, Levent; "**Sosyal Medya ve Algı Yönetimi Sosyal Medya İstihbaratına Giriş**", 2.Baskı, Anı Yayıncılık, Ankara, 2020, s. 112

ERDİN, Kadir; "Elektromanyetik Dalgaların Oluşumu ve Uzaktan Algılama", **İstanbul Üniversitesi Orman Fakültesi Dergisi**, Cilt.28, Sayı.2, 1978, ss. 158-167

EREN, Mehmet; "**Avrupa Birliği'nin Siber Güvenlik Politikası**", 1.Baskı, Beta Basım Yayım Dağıtım, İstanbul, 2017, s. 23

EROĞLU, Erhan; "Siyasal İletişimde Kültürün Dijital Dönüşümü", **Siyasal İletişimin Dijital Dönüşümü**, Ed. Başak Solmaz, 1.Baskı, Literatürk Academia, Konya, 2019, ss. 334-359

EROL, Kazım Mehmet; "**Açık Kaynak İstihbaratı ve Askeri İstihbarat Haşdi Şabi Örgütü Üzerinde Uygulama**", 1. Baskı, Nobel Bilimsel, Ankara, 2022, s. 25

ERTAŞ, Handan; "Yönetişim – E-Devlet Bağlamında Kamu Yönetiminin Dönüşümü", **Teoriden Uygulamaya E-Devlet**, Ed. Ali Şahin ve Erhan Örselli 2. Baskı, Atlas Akademi, Konya, 2016, s.40.

FERNANDEZ, Luis Alex Valenzuela ve diğerleri; "E-Goverment and Its Development in The Region: Challenges", **International Journal of Professional Business Review**, Cilt.8, Sayı.1, 2023, ss. 1-15

FİDANCI, Ömer Şaban; "Kurumlar İçin Bilgi Güvenliği Yönetim Sisteminin Oluşturulması", **Yüksek Lisans Tezi**, KTO Karatay Üniversitesi, Konya, 2022, s. 16

FORDE, Brian; "Blok Zincirinin Kamusal Verilerin Kamuya Açılması Amacıyla Kullanılması", **Harvard Business Review Press Blockchain** , Ed. Çiğdem Zeynep Aydın, Çev. Taner Gezer, 1.Baskı, Optimist Yayın Grubu, 2019, ss.189-200.

GOODMAN, Marc; "**Geleceğin Suçları Dijital Dünyanın Karanlık Yüzü**", Ed. Yavuz Türk ve Kadir Güven, 3.Baskı, Timaş Yayınları, İstanbul, 2020, ss. 454-499

GÖÇOĞLU, Volkan; "Kamu Hizmetlerinin Sunumunda Dijital Dönüşüm: Nesnelerin İnterneti Üzerine Bir İnceleme", **Manas Sosyal Araştırmalar Dergisi**, Cilt.9, Sayı.1, 2020, ss. 616-628

GÖKOZAN, Hayrettin ve Mehmet Taştan; "Akıllı Taşıtlar ve Kontrol Sistemleri", **Mesleki Bilimler Dergisi**, Cilt.7, Sayı.2, 2018, ss.58-62

GÖKTUN, Sargun ve diğerleri; "Elektronik Harp", https://www.milsoft.com.tr/wp-content/uploads/2020/12/Elektronik-Harp_MilSOFT.pdf , (19.05.2023).

GÖNEN, Serkan ve Ercan Gürcan Yılmaz; "Bilişim Alanında İşlenen Suçlar ve Kişisel Verilerin Korunması", **Bilişim Teknolojileri Dergisi**, Cilt.9, Sayı.3, 2016, ss.229-236

GÖZÜYEŞİL, Fevzi Fırat; "Denizde Çatışmanın Önlenmesine Dair Uluslararası Kurallar Bağlamında İnsansız ve Otonom Gemilerde İyi Gemicilik İlkesi ve Gözcülük Görevi", **Adalet Dergisi**, Cilt.1, Sayı.66, 2021, ss.193-225

GUPTA, Manish Hareesh G. ve Arvind Kumar Mahla; "Electronic Warfare: Issues and Challenges for Emiter Classification", **Defence Science Journal**, Cilt. 61, Sayı.3, 2011, ss. 228-234

GUPTA, Vinay; "Blok Zincirinin Kısa Tarihi", **Harvard Business Review Press Blockchain** , Ed. Çiğdem Zeynep Aydın, Çev. Taner Gezer, 1.Baskı, Optimist Yayın Grubu, 2019, ss.53-60

GUTMANN, Myron Emily Rose Merchant ve Evan Roberts; " "Big Data" in Economic History", **The Journal of Economic History,** Cilt.78, Sayı.1, 2018, ss.268-299

GÜÇLÜ, Nezahat ve Kseanela Sotirofski; "Bilgi Yönetimi", **Türk Eğitim Bilimleri Dergisi**, Cilt.4, Sayı.4, 2006, ss.351-371

GÜLDOĞAN, Mustafa Veysel ve Şevki Işıklı; "Siber Savaşta Mütekabiliyet", **Academic Journal of Information Technology**, Cilt.13, Sayı.51, 2022, ss.289-319

GÜMÜŞ, Salih, Aras Bozkurt ve Erdem Erdoğdu; "**Dijital Yayıncılık ve Dijital Yayıncılık Araçları**", 1.Baskı, Anadolu Üniversitesi Yayınları, Eskişehir, 2017, ss.95-125

GÜNDOĞDU Köksal ve Ali Çalhan; "İnsansız Askeri Kara Aracı Tasarımı", **İleri Teknoloji Bilimleri Dergisi**, Cilt.2, Sayı.1, 2013, ss. 36-45

GÜNEŞ, Ayşegül; "Küresel Güçlerin Ulusal Siber Güvenlik Stratejileri: ABD Örneği", http://cyberpolitikjournal.org/index.php/main/article/view/18/18 , (Erişim Tarihi: 05.05.2023).

GÜNGÖR, Uğur ve Oğuzhan Güney; "Uluslararası İlişkilerde Güvenliğin Dönüşümü Çerçevesinde Bilgi Güvenliği ve Siber Savaş", **Karadeniz Araştırmaları Merkezi**, Cilt.15, Sayı.55, 2017, ss.131-146

GÜRSEL, İlke; "Protection Of Personal Data in İnternational Law And The General Aspects Of The Turkish Data Protection Law", **D.E.U Hukuk Fakültesi Dergisi**, Cilt.18, Sayı.1, 2016, ss. 33-61.

HEKİM, Hakan ve Oğuzhan Başıbüyük; "Siber Suçlar ve Türkiye'nin Siber Güvenlik Politikaları", https://www.researchgate.net/publication/348241799 , (09.04.2023).

HENKOĞLU, Türkay ve Nazan Özenç Uçak; "Protection Of Personal Data in University Libraries", **Bilgi Dünyası**, Cilt.16, Sayı.1, 2015, ss. 45-74

IANSITI, Marcon ve Karim R. Lakhani; "Blok Zinciri Hakkındaki Gerçekler", **Harvard Business Review Press Blockchain** , Ed. Çiğdem Zeynep Aydın, Çev. Taner Gezer, 1.Baskı, Optimist Yayın Grubu, 2019, ss.19-52

IDRISOV, Hussein Vakhaevich; "Information Security in the National Security Systems in the Modern Age", **Fiat Justisia Jurnal Ilmu Hukum**, Cilt 16, Sayı 4, 2022, ss. 321-330.

IVANCIK, Radoslav; "Information War – One Of The Multidisciplinary Phenomennes Of Current Human Society" , https://www.researchgate.net/publication/350963287 , (Erişim Tarihi: 19.05.2023).

İRALI, Ali Efe; "Uyumlu Tasarıma Geçişte Kitle İletişim Araçlarının Gelişimi", **Selçuk İletişim Dergisi**, Cilt.14, Sayı.2, 2021, ss. 982-1004

İŞLİYEN, Fadime Şimşek; "Dijital Çağda Bilginin Değişen Niteliği ve İnfobezite: Z Kuşağı Üzerine Bir Odak Grup Çalışması", **Selçuk İletişim Dergisi**, Cilt.13, Sayı.1, 2020, s.256.

JAWHLY, Thaisa ve Ramesh Chandra Tiwari; "Simple VHF and UHF Loss Model**",** **Journal of Latex Class Files,** Cilt. 14, Sayı. 8, 2015, 1-4

JONES, Marc; "Hacking, Bots and İnformation Wars in The Qatar Spat", https://d1wqtxts1xzle7.cloudfront.net/56335866/POMEPS_GCC_Qatar-Crisis.pdf?1523917784 , (Erişim Tarihi: 19.05.2023).

KAHRAMAN, Selçuk ve Önder Kutlu; "Türkiye'de Kişisel Verilerin Korunması Politikasının Analizi", **Siyaset, Ekonomi ve Yönetim Araştırmaları Dergisi,** Cilt.5, Sayı.4, 2017, ss.45-62

KAO, B. ve C. Tseng; "Big Data And Artificial İntelligence For Supply Chain Management: A Review and Future Research Directions", **International Journal of Production Research**, Cilt.60, Sayı.2, 2022, 618-639

KARA, Mehmet; "**Kurumsal Bilgi Güvenliği**", 1.Baskı, Papatya Yayıncılık, İstanbul, 2018, s.15

KARAKOÇAK, Kemal; "Bilgi Üretiminin Verimliliğe Etkisi: TBMM Örneği", **Bilgi Yönetimi Disiplini ve Uygulamaları,** Ed. Mustafa Sağsan, 1.Baskı, Siyasal Kitabevi, Ankara, 2010, s. 163

KARASOY, Alpay; "E-Devlet Uygulamalarının Hizmet Kalitesine Etkileri", **Selçuk Üniversitesi Sosyal Bilimler Meslek Yüksek Okulu Dergisi,** Cilt.12, Sayı.1-2, ss.279-294

KAYACI, Müslüm; "Kamu Yönetiminde Etik Bağlamında Güvenlik Hizmetleri Etiğine Bir Bakış", **Sosyal Bilimler Akademi Dergisi**, Cilt.2, Sayı.1, 2019, ss.50-69

KEKİK, Ahmet ve diğerleri; "**Temel Elektrik-Elektronik Atölyesi**", 1.Baskı, Meb Yayınları, Ankara, 2022, ss. 188-197.

KORKMAZ, Şahin; "İzleme ile Güvenliğin Sağlanması" **İşletim Sistemleri Güvenliği**, Ed.Çelebi Uluyol 1.Baskı, Gece Akademi, Ankara, s.54

KORUCU, Onur; "Yeni Normal Dünya Düzeninin Siber Güvenlik ve Bilgi Güvenliği Etkileri", **Yönetim Bilişim Sistemleri Dergisi**, Cilt.7, Sayı.1, 2021, ss.44-60

KÖKER, Ahmet Emre; "Ulusal Siber Güvenlik Stratejisi: Fransa", **UPA Strategic Affairs,** Cilt.3, Sayı.1, 2022, ss. 42-78

KÖKTÜRK, Önder; "The Protection Of Personal Data – Kişisel Verilerin Korunması (Turkish)", https://www.researchgate.net/publication/335813724 , (Erişim Tarihi:09.04.2023).

KRASMANN, Susanne; " On The Boundaries of Knowledge: Security, the Sensible and the Law", https://www.researchgate.net/publication/293827664 , (Erişim Tarihi:30.03.2023).

KUDOZIA, Roland Yaw; "Organizational Knowledge Management Practices Among Ghanaian Enterprises: Assessing Knowledge Management Practices In The Service Industry İn Accra", **Aspen Journal of Scholary Works**, Cilt.3, Sayı.1, 2023, ss.212-229

KUMAŞ, Esra ve Serpil Erol; "Endüstri 4.0'da Anahtar Teknoloji olarak Dijital İkizler", **Politeknik Dergisi**, Cilt.24, Sayı.2, 2021, ss.609-701

KURNAZ, Salim ve Mustafa Önen; "Avrupa Birliği'ne Uyum Sürecinde Türkiye'nin Siber Güvenlik Stratejileri", https://dergipark.org.tr/en/pub/ijps/issue/41280/581227 , (Erişim Tarihi: 05.05.2023).

KÜÇÜKKIRALI, Zeynep ve Kerim Eser Afşar; "Dijital Verinin Finansallaşması ve Platform Kapitalizmi", **Marmara Üniversitesi Öneri Dergisi**, Cilt.17, Sayı.58, 2022, ss.665-690

KÜÇÜKSİLLE, Ecir Uğur Sevda Nur Genç ve Yunus Emre Karabulut; "Dünyada Siber Güvenlik Stratejileri ve Bir Siber Güvenlik Stratejisinin Oluşumu" , https://www.researchgate.net/publication/338557611 , (Erişim Tarihi:05.05.2023).

KÜZECİ, Elif ; "Sayı-sal Fil", 1.Baskı, İnkılâp Yayınevi, İstanbul, 2021, s.233

MAHFUTH, Amjad; "Security Knowledge Required to Improve Employee Security Behavior in Information Security Culture", **International Journal of Comuputer Science and Information Security**, Marc 2022, ss. 1-10

MAHIDHAR, Vikram ve Thomas H. Davenport; "Yapay Zekaya Geçmek İçin Beklemeyi Tercih Eden Şirketler Treni Neden Yakalayamayabilir?", **Harvard Business Review Press Artificial Inteligence** , Ed. Utku Umut Bulsun, Çev. Levent Göktem, 1.Baskı, Optimist Yayın Grubu, 2020, ss.91-106

MAINELLI, Michael; "Blok Zinciri Dijital Dünyada Kimliğimizi Kanıtlamamıza Yardımcı Olacak", **Harvard Business Review Press Blockchain** , Ed. Çiğdem Zeynep Aydın, Çev. Taner Gezer, 1.Baskı, Optimist Yayın Grubu, 2019, ss.201-212.

MANYIKA, J. ve diğerleri; "Big Data : The Next Frontier For İnnovation, Competition and Productivity", **McKinsey Global Institute**, Cilt.1, Sayı.4, ss.1-25

MARTINHO-TRUSWELL, Emma; "Teknik Ekipten Olmayan Çalışanların Yapay Zeka Hakkında Yanıtlayabilmesi Gereken 3 Soru", **Harvard Business Review Press Artificial Inteligence** , Ed. Utku Umut Bulsun, Çev. Levent Göktem, 1.Baskı, Optimist Yayın Grubu, 2020, ss.107-118

MATEEVA, Zhivka; "Protection of Persons of Personal Data Before The National Supervisory Authoriy", **Eastern Academic Journal**, Cilt.3, Sayı.1, 2020, ss.39-49

MAULANA, H.Agus; "Model SECI Knowledge Management", https://www.researchgate.net/publication/352559412 , (Erişim Tarihi: 13.03.2023).

MCAFEE, A. ve E. Brynjolfsson; "Big Data: The Management Revoluiton", **Hardvard Business Review**, Vol.90, Issue. 10, 2012, ss.60-68

MCDERMOTT, Richard; "Why Information Technology Inspired But Cannot Deliver Knowledge Management", **California Management Review**, Cilt 4, Sayı 41, 1999 s. 103

MİL, Halil İbrahim Saffet Gülep ve Ahmet Ünal; "Türkiye'nin Siber Güvenlik Stratejileri", https://www.researchgate.net/publication/349052551 , (Erişim Tarihi: 05.05.2023).

MUTEBI, Joe ve diğerleri; "Relative Influence of Social Media Socio-Technical Information Security Factors on Medical Information Breaches in Selected Medical Institutions in Uganda", https://www.researchgate.net/publication/365365748 , (Erişim Tarihi : 20.03.2023).

NACAK, Ayşegül Arif Sarı ve Onurhan Yılmaz; "Küreselleşen Dünyada Siber Güvenliğin Artan Önemi ve Gelişmiş Ülkelerde Siber Güvenlik Stratejileri", https://www.researchgate.net/publication/303945885 , (Erişim Tarihi: 05.05.2023).

OGANESIAN, Tigran; "Protection Of Personal Data: Positions Of İnternational Courts", https://www.researchgate.net/publication/333708289 , (Erişim Tarihi: 09.04.2023).

OĞUZ, Sefer; "Kişisel Verilerin Korunması Hukukunun Genel İlkeleri" , **Bilgi Ekonomisi ve Yönetimi Dergisi,** Cilt.13, Sayı.2, 2018, ss. 121-138.

OH, Hyeontaek ve diğerleri; "Personal Data Trading Scheme for Data Brokers in IOT Data Marketplaces", **IEEE Access Open Access Journal**, Cilt.7, Şubat 2019, ss.40120-40132

OKOKO, Ilolighata Tamarapreye ;"A Review On Radiowave Propagation Models For Very High Frequency And Ultra High Frequency Band", **International Journal of Engineering Science and Application**, Cilt.6, Sayı.4, 2022, ss. 103-112

OSMAN, Abdullahi Sidow; "Data Mining Techniques:Review", **International Journal of Data Science Research**, Cilt.2, Sayı.1, 2019, ss.1-4.

ÖNEN, S. Mustafa ve Salim Kurnaz; "Siber Güvenlik Politikalarının Kamu Yönetimine Yansıması", **Turgut Özal Uluslararası Ekonomi ve Siyaset Kongresi** IV, 11-12 Mayıs 2017, Malatya, ss.732-752

ÖRSELLİ, Erhan ve Yasin Taşpınar; "E-Devlet: Fırsatlar ve Tehditler Bağlamında Bir Analiz", **Teoriden Uygulamaya E-Devlet**, Ed. Ali Şahin ve Erhan Örselli 2. Baskı, Atlas Akademi, Konya, 2016, s.13

ÖZALTIN, Oğuz ve Mevlüt Ersoy; "Kamu Yönetiminde Blokzincir Kullanımı: D5 Örneği", **Nevşehir Hacı Bektaş Veli Üniversitesi SBE Dergisi**, Cilt.10, Sayı.2, 2020, ss.746-763

ÖZCAN, Ali; "Büyük Veri: Fırsatlar ve Tehditler", **Trt Akademi**, Cilt.6, Sayı.11,2021, ss.12-30

ÖZÇELİK, Zübeyir ve Ebru Aykan; "Sosyal Bilimlerde Büyük Veri Kullanımı, Veri Toplamada Akademik Çalışmalara Ne Tür Kolaylıklar Sağlayabilir?", **Anadolu Üniversitesi Sosyal Bilimler Dergisi,** Cilt.20, Sayı.3, 2020, ss.131-142

ÖZDAĞ, Ümit; "**İstihbarat Teorisi**", 15.Baskı, Kripto Basım, Ankara, 2021, s.112

ÖZDEMİR, Ayşe ve Çelebi Uluyol; "Kamu Kurum ve Kuruluşlarında Bilgi Güvenliği Farkındalığı", **Türkiye Sosyal Araştırmalar Dergisi**, Cilt.25, Sayı.3, 2021, ss.649-666

ÖZDEMİRCİ, Fahrettin, Cengiz Aydın; " Kurumsal Bilgi Kaynaklar ve Bilgi Yönetimi", **Türk Kütüphaneciliği Dergisi**, Cilt. 21, Sayı.2, 2007, ss.164-185.

ÖZEL, Kadir Can; "Ana Hatlarıyla Kişisel Verilerin Korunmasının Tarihsel Süreci ile Amacı ve Kişisel Verilerin Korunması Hakkı", **İstanbul Barosu Dergisi**, Cilt.94, Sayı.2, 2020, ss.242-25

ÖZEN, Ahmet ve Fatma Nur Gürel; "Kamu Denetiminde Dijital Dönüşüm: Dijital İkiz Yöntemi", **İzmir Sosyal Bilimler Dergisi**, Cilt.2, Sayı.1, 2020, ss.16-23

ÖZGÜR, Hüseyin ve Saynur Çicek; "Türkiye'de Kamu Yönetimi ve İşletme Eğitiminde Bilişim ve Diğer Teknolojiler: Literatür, Tarihsel Gelişim, Dersler ve Sorunlar", **Pamukkale Üniversitesi İşletme Araştırmaları Dergisi**, Cilt.8, Sayı.1, ss.1-26.

PANDIAN, Narmatha; "The Big Data to Innovative in Education", https://www.researchgate.net/publication/370155713 , (Erişim Tarihi:21.03.2023).

PARLAK, Bekir ve Kadir Caner Doğan; "**E-Yönetişim Kavramsal/Kuramsal Çerçeve, Ülke İncelemeleri ve Türkiye'ye Yansımaları**", 1.Baskı, Beta Yayımcılık, İstanbul, 2019, s.39

PEREIRA, Manuel Joaquim Sousa vd.; "Digital Transformation in Organizations and Its Impact on Knowledge Management" https://www.researchgate.net/publication/363847760 , (Erişim Tarihi: 13.03.2023).

PETERS, Michael A.; "The Information Wars, Fake News and The End Of Globalisation", https://www.tandfonline.com/doi/full/10.1080/00131857.2017.1417200 (Erişim Tarihi: 19.05.2023).

PINTOR, Annie Liza Capili ve diğerleri; "Spectrum Survey Of VHF And UHF Bands İn The Philippines ", https://www.researchgate.net/publication/286850875_ , (Erişim Tarihi:12.04.2023).

PRIETO,Roberto; "Knowledge Management", https://www.researchgate.net/publication/363541812 , (Erişim Tarihi: 30.03.2023).

RAGAB, Ahmed Soumaya Yacout ve Mohamed-Salah Ouali; "Intelligent Data Mining for Automatic Face Recognition", The Online Journal of Science and Technology, Cilt.3, Sayı.2, 2013,ss.97-101

RYAN, Julie J.C.H.; "Political Engineering in Knowledge Security", **VINE**, Cilt.36, Sayı.3, 2006, ss.265-266

SADREDDINI, Zhaleh; "Bilişsel Radyo Ağlarında Çok Ölçütlü Karar Verme Yöntemlerine Dayalı Yeni Bir Spektrum Modeli", **Doktora Tezi**, Karadeniz Teknik Üniversitesi, Trabzon, 2018, ss.1-33

SANDİLAÇ, Nurullah; "Siber Suç, Siber Terör ve Siber Savaş Üçgeninde Siber Dünya", **Bilişim Hukuk Dergisi,** Cilt.4, Sayı.1, 2022, ss.141-190

SARACEL, Nüket ve Irmak Aksoy; "Dijital Sürdürülebilirlik, Boyutları ve Koşulları", **Sosyal Bilimler Araştırma Dergisi**, Cilt. 10, Sayı. 2, 2021, ss.347-356

SAVAŞ, Serkan Nurettin Topaloğlu ve Mithat Yılmaz; "Veri Madenciliği ve Türkiye'deki Uygulama Örnekleri", **İstanbul Ticaret Üniversitesi Fen Bilimleri Dergisi**, Cilt.11, Sayı.21, 2012, ss.1-23

SCHARRE, Paul; "**İnsansız Ordular Katil Robotlar, Otonom Silahlar ve Makine Savaşları**", Ed. Can Uyar, Çev. Kutsi Aybars Çetinalp, 2.Baskı, Kronik Kitap, İstanbul, 2021, s. 27

SCHLEHER, D. Curtis; "**Bilgi Çağında Elektronik Harp**", Çev. Berna Kara 1.Baskı, Doruk Yayımcılık, Ankara, 2004, s. 19

SEÇİM, M. Özgür; "Radyonun Bir Haber Alma Aracı Olarak Kullanılması: Adnan Menderes Üniversitesi Öğrencilerine Yönelik Bir Araştırma", **Karabük Üniversitesi Sosyal Bilimler Enstitüsü Dergisi**, Cilt.7, Sayı.1, 2017, ss. 302-317

SEKER, Sadi Evren; "Bilgi Yönetimi", **YBS Ansiklopedi**, Cilt.1, Sayı.2, 2014 ss.10-17

SERTÇELİK, Aşır; "Siber Olayler Ekseninde Siber Güvenliği Anlamak", **Medeniyet Araştırmaları Dergisi**, Cilt.2, Sayı.3, 2015, ss. 25-42

SEVİNÇ, İsmail ve Niyazi Karabulut; "Kişisel Verilerin Koruma Kurumu Üzerine Bir İnceleme", **Akademik Hassasiyetler Dergisi,** Cilt.7, Sayı.13, 2020, ss. 449-472.

SEVİNÇ, Semih; "Sinyal İstihbaratı Analizi Bağlamında Bir Değerlendirme: Rubicon Operasyonu ve Türkiye", **İstihbarat Çalışmaları ve Araştırmaları Dergisi**, Cilt.2, Sayı.1, 2023, ss. 68-81

SEZGİN, Erkan; "**İstihbarat Üzerine**", 1.Baskı, Cinius Yayınları, İstanbul, 2022, s. 89

SHEDDEN, Piya ve diğerleri; "Incorporating a Knowledge Perspective into Security Risk Assessments", https://www.researchgate.net/publication/235297507_ , (Erişim Tarihi: 30.03.2023).

SHERMAN, Justin; "Data Brokers and Sensitive Data on U.S. Individuals", https://techpolicy.sanford.duke.edu/wp-content/uploads/sites/4/2021/08/Data-Brokers-and-Sensitive-Data-on-US-Individuals-Sherman-2021.pdf , (Erişim Tarihi: 27.03.2023).

SHIBAEV, D. V; "Methods To Counter Information War", **Russian Journal of Legal Studies**, Cilt.4, Sayı.9, 2016, ss.60-68

SINGH, Aman; "E-Governance: Moving Towards Digital Governance", **Peer-Reviewed, Multidisciplinary & Multilingual Journal**, Cilt.2, Sayı.1, 2023, ss. 204-215

SKENDZIC, Aleksandar v.d.; "General Data Protection Regulation – Protection Of Personal Data in An Organisation", https://www.researchgate.net/publication/326708317 , (09.04.2023).

SNETSELAAR, David; "Dreams Lab: Assembling Knowledge Security in Sino-Dutch Research Collaborations", European Security, Cilt 1, Sayı 1, 2022, ss. 1-20

SOLMAZ, Başak; "**Siyasal İletişimin Dijital Dönüşümü**", 1.Baskı, Literatürk Academia, Konya, 2019, ss. 9-35

SOUZA, Jonatas S. De ve diğerleri; "The General Law Principles For Protection The Personal Data And Their İmportance", **AIRCC Publishing Corporation**, Cilt.10, Sayı.11, 2020, ss.110-120

SZCZEPANIUK, Edyta Karolina ve diğerleri; "Information Security Assessment in Public Administration", **Computers & Security**, Cilt.90, 2020, ss.1-11

ŞAHİN, Mustafa Ergin; "**Elektronik Laboratuvarı Deneyleri – Bilgisayar Destekli ve Konu Anlatımlı**" , 1.Baskı, Nobel Akademik Yayıncılık, Ankara, 2018, s.47.

ŞENER, Turan ve Nezihe Ülkü Eren; "E-Devlet'in Yönetişim Bağlamında Değerlendirilmesi", **Karadeniz Araştırmaları Dergisi**, Cilt.18, Sayı.72, 2021, ss.863-873

ŞENGÜL Ramazan ve Özlem Balıkçı; "Yerel Yönetimlerde E-Yönetişim Üzerine Bir Araştırma", **Ordu Üniversitesi Sosyal Bilimler Araştırmaları Dergisi**, Cilt.11, Sayı.2, 2021, ss. 417-436

ŞENGÜL, Razaman ve Hande Yüksel Altınbaş; "Akıllı Kentin Bir Bileşeni Olarak Akıllı Ulaşım Uygulamalarının İncelenmesi: Kocaeli Büyükşehir Belediyesi Örneği", **Uluslararası Kültürel ve Sosyal Araştırmalar Dergisi,** Cilt.6, Sayı.2, 2020, ss.487-502

ŞENGÜR, Dönüş ve Songül Karabatak; "Data Mining Techniques Based Students Achievements Analysis", **Turkish Journal of Science & Technology**, Cilt.13, Sayı.2, 2018, ss.53-59.

TABAN, M. Hayati ve Emre Aydilek; "Dijital Çağda İstihbarat Analizi", **İstihbarat Çalışmaları ve Araştırmaları Dergisi**, Cilt.2, Sayı.1, 2023, ss. 39-67

TALAPINA, Elvira; "Legal Protection Of Personal Data in France", https://www.researchgate.net/publication/341600038 , (Erişim Tarihi: 09.04.2023).

TEKEREK, Mehmet; "Bilgi Güvenilği Yönetimi", **KSÜ Doğa Bilimleri Dergisi**, Cilt.11, Sayı.1, 2008, ss. 132-137.

TOKGÖZ, Oya; "Siyasal Toplumsallaşmada Kitle Haberleşme Araçlarının Rolü Ve Önemi", **Nevşehir Hacı Bektaş Veli Üniversitesi Sosyal Bilimler Enstitüsü Dergisi**, Cilt.33, Sayı.3, 1978, ss. 80-92

TOMAŞ, Melek ve Neslihan Dostoğlu; "Yapay Zekaya Sahip Akıllı Evler", **Avrupa Bilim ve Teknoloji Dergisi**, Cilt.1, Sayı.18, 2020, ss.486-493

TOPLU, Mehmet; "Ekonomik Dönüşüm ve Gelişmelerin Bilgi Yönetimine Etkileri", **Bilgi Yönetimi Disiplini ve Uygulamaları,** Ed. Mustafa Sağsan, 1.Baskı, Siyasal Kitabevi, Ankara, 2010, s. 56

TRKMAN, Peter ve Kevin C. Desouza; "Knowledge Risks in Organizational Networks: An Exploratory Framework", **The Journal of Stategic Infortamation Systems**, Cilt 1, Sayı 21, 2011, s. 9

TUCKER, Catherine; "Blok Zinciri ve Veri Bütünlüğü Devrimi", **Harvard Business Review Press Blockchain** , Ed. Çiğdem Zeynep Aydın, Çev. Taner Gezer, 1.Baskı, Optimist Yayın Grubu, 2019, ss.9-18.

TULCHINSKY, Grigory L.; "Information Wars As A Conflict Of İnterpetations: Activating The 'Third Party'", **Russian Journal of Communication**, Cilt.5, Sayı.3, 2013, ss.244-251

TÜRK Dil Kurumu Sözlüğü, "Dijital Kelime Anlamı" https://sozluk.gov.tr , (Erişim Tarihi: 21.03.2023).

TÜRK MEDENİ KANUNU; "1. Bölüm Gerçek Kişiler, Kişilik, Madde 28", https://www.mevzuat.gov.tr/MevzuatMetin/1.5.4721.pdf , (Erişim Tarihi: 09.04.2023).

UÇKAN, Özgür; **E-devlet, E-demokrasi ve Türkiye**, 1.Baskı, Literatür Yayınları, İstanbul, 2003, s. 70

UNCULAR, Selen; "Kişisel Verilerin Korunması Kanunu'nda Yer Alan Hakların ve Hükümlülerin İş İlişkisindeki Yansımaları", **Çankaya Üniversitesi Hukuk Fakültesi Dergisi**, Cilt.5, Sayı.1, 2020, ss.3405-3427

UYSAL, Yusuf; "Klasik Kamu Yönetiminden Yeni Kamu İşletmeciliği ve Post-YKİ'ye Kamu Hizmetlerinin Değişimi ve Dönüşümü Üzerine Bir Değerlendirme",

International Journal of Management and Administration, Clit.4, Sayı.7, 2020, ss.112-135

UZUN, Erman İlker Yakın ve Ali Gök; "**Elektronik Programlama ve Nesnelerin İnterneti**", 1. Baskı, Tübitak Yayınları, Ankara, 2011, s. 11

ÜLGER, Emir; "Epistemik Perspektiften Bilginin Kamusal Algılanışı ve Değişimi", **Bilgi Yönetimi Disiplini ve Uygulamaları,** Ed. Mustafa Sağsan, 1.Baskı, Siyasal Kitabevi, Ankara, 2010, s. 84

ÜN, Lütfullah; "Kamu Hizmetinde Yeni Konsept: Akıllı Kamu Hizmeti", **Bingöl Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi**, Cilt.6, Sayı.2, 2022, ss.415-440.

ÜNAL, Ahmet Naci; "**Siber Güvenlik ve Elektronik Bileşenleri**", 1.Baskı, Nobel Akademik Yayıncılık, Ankara, 2015, ss. 8-10

VARDİN, Salih, Pınar Demircioğlu ve İsmail Böğrekci; "Arazi Uygulamaları İçin İnsansız Yer Aracı Geliştirilmesi", **Uluborlu Mesleki Bilimler Dergisi,** Cilt.5, Sayı.1, 2022, ss. 1-13

WEBB, Jeb ve diğerleri; "Information Security Risk Management: An Intelligence-Driven Approach", **Australasian Journal of Information Systems**, Cilt 18, Sayı 3, 2014, ss. 391-406.

WILSON, H.James Paul Daugherty ve Chase Davenport; "Yapay Zekanın Geleceğinde Verinin Yeri Daha Fazla Değil Daha Az Olacak", **Harvard Business Review Press Artificial Inteligence** , Ed. Utku Umut Bulsun, Çev. Levent Göktem, 1.Baskı, Optimist Yayın Grubu, 2020, ss.229-242

WILSON, H.James ve Paul Daugherty; "İşbirliğine Dayalı Zekâ: İnsan Ve Yapay Zekâ Güçlerini Birleştiriyor", **Harvard Business Review Press Artificial Inteligence** , Ed. Utku Umut Bulsun, Çev. Levent Göktem, 1.Baskı, Optimist Yayın Grubu, 2020, ss.169-206

WOODSIDE, Joseph M.; "Bemo: A Parsimonious Big Data Mining Methodology", **Online Academic Journal of Infortmation Technology**, Cilt.7, Sayı.24, 2016, ss.114-123

YAKIN, Aziz; "**İstihbarat Casusluk ve Casuslukla Mücadele**", 1.Baskı, Dışişleri Akademisi Yayınları, Ankara, 1969, s. 36

YANG, Min; "Information Security Risk Management Model for Big Data), https://www.hindawi.com/journals/am/2022/3383251 , (Erişim Tarihi: 10.03.2023).

YAZICI, Bülent; "Otonom Silah Sistemlerinin Uluslararası Silah Hukuku ve Politiği Açısından Sorunsal Meseleleri", **Bilecik Şeyh Edebali Üniversitesi Sosyal Bilimler Enstitüsü Dergisi**, Cilt.4, Sayı.1, 2019, ss. 280-292

YELOĞLU, Hakkı Okan ve Senem Oğuz; "Kamu Sektöründe Örgütsel Yeniliklerin Algılanması ve Yenilik Kapasitesinin Belirlenmesine Yönelik Görgül Bir Çalışma", **Bilgi Yönetimi Disiplini ve Uygulamaları,** Ed. Mustafa Sağsan, 1.Baskı, Siyasal Kitabevi, Ankara, 2010, s. 224

YILDIRIM, Arzu; "Kamu Yönetiminde Sağlık Politikalarındaki Dönüşüm: E-Sağlık Uygulamaları", **Kuram ve Uygulamada Sosyal Bilimler Dergisi**, Cilt.6, Sayı.2, 2022, ss.125-140

YILMAZ, Ercan Nurcan, Halil İbrahim Ulus ve Serkan Gönen; "Bilgi Toplumuna Giriş ve Siber Güvenlik", **Bilişim Teknolojileri Dergisi**, Cilt.8, Sayı.3, 2015, ss.133-146

YILMAZ, Ercan, Nurcan Halil İbrahim Ulus ve Serkan Gönen; "Bilgi Toplumuna Geçiş ve Siber Güvenlik", **Bilişim Teknolojileri Dergisi**, Cilt.8, Sayı.3, 2015, ss.133-146

YILMAZ, Malik; "Enformasyon ve Bilgi Kavramları Bağlamında Enformasyon Yönetimi ve Bilgi Yönetimi", **Ankara Üniversitesi Dil ve Tarih – Coğrafya Fakültesi Dergisi,** Cilt.49, Sayı.1, 2009, ss. 95-118.

YILMAZ, Sait; "**21. Yüzyılda Güvenlik ve İstihbarat**", 1.Baskı, Alfa Yayınları, İstanbul, 2006, ss.607-611

YORULMAZ, Murat ve Kaan Karabulut; "Deniz Taşımacılığında Akıllı Gemiler: Gemi Kaptanlarının Bakış Açısı", **Ekonomi, İşletme ve Maliye Araştırmaları Dergisi**, Cilt.3, Sayı.1, 2021, ss.40-54

YÜCEL, Recep; "Bir Disiplin Olarak Bilgi Yönetimi ve Eğitimi", **Bilgi Yönetimi Disiplini ve Uygulamaları,** Ed. Mustafa Sağsan, 1.Baskı, Siyasal Kitabevi, Ankara, 2010, s.16

ZAKHAROV, M. Yu. vd.; " Sociology of Knowledge Security in the Digital Educational", **Vestnik Universiteta Journal**, Cilt.1, Sayı.3, 2020, ss.154-159

ZHANG, Han ve diğerleri; "Big Data Analysis and Prediction of Electromagnetic Spectrum Resources: A Graph Approach", **Mdpi Journal Sustainability**, Cilt.15, Sayı.1, 2022, ss. 2-17

ZHAROVSKA, Iryna ve Nataliya Ortinska; "The Information War as A Modern Globalization Phenomenon", https://www.researchgate.net/publication/345734928 , (Erişim Tarihi: 19.05.2021).

ZOU, Qi ve diğerleri; "Vision and Reality of E-Government for Governence Improvement: Evidence From Global Cross-Country Panel Data", **Technological Forecasting & Social Change an Internatıonal Journal**, Cilt.1, Sayı.194, 2023, ss. 1-17