



**T.C.
GİRESUN ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
İŞLETME ANA BİLİM DALI**

**SOSYAL MÜHENDİSLİK BAĞLAMINDA
BİLGİ GÜVENLİĞİNİN ENDÜSTRİ 4.0 TABANLI
SİSTEMLERE UYARLANMASI**

Doktora Tezi

Cevdet ÖZMEN

172024003

Giresun 2020



**T.C.
GİRESUN ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
İŞLETME ANA BİLİM DALI**

**SOSYAL MÜHENDİSLİK BAĞLAMINDA
BİLGİ GÜVENLİĞİNİN ENDÜSTRİ 4.0 TABANLI
SİSTEMLERE UYARLANMASI**

Doktora Tezi

Cevdet ÖZMEN

172024003

Danışman: Prof. Dr. Bayram KAYA

Giresun 2020

JÜRİ ÜYELERİ ONAY SAYFASI

Giresun Üniversitesi Sosyal Bilimler Enstitüsü'nün 16 Eylül 2020 tarihli toplantısında oluşturulan jüri, Sosyal Bilimler Enstitüsü İşletme Ana Bilim Dalı Doktora öğrencisi Cevdet ÖZMEN'in “**SOSYAL MÜHENDİSLİK BAĞLAMINDA BİLGİ GÜVENLİĞİNİN ENDÜSTRİ 4.0 TABANLI SİSTEMLERE UYARLANMASI**” başlıklı tezini incelemiş olup, aday 02 Ekim 2020 tarihinde, saat 14:00’da jüri önünde tez savunmasına alınmıştır.

Aday çalışma, sınav sonucunda başarılı bulunarak jürimiz tarafından oy birliği / oy çokluğu ile Doktora Tezi olarak kabul edilmiştir.

Sınav Jürisi	Unvanı, Adı Soyadı	İmzası
Üye (Başkan)	Prof. Dr. Bahtışen KAVAK	
Üye	Prof. Dr. Leyla ÖZER	
Üye	Prof. Dr. Bayram KAYA (Danışman)	
Üye	Doç. Dr. Kurtuluş Yılmaz GENÇ	
Üye	Doç. Dr. Eren BAŞ	

ONAY

...../...../2020

Prof. Dr. Enver SARI
Enstitü Müdürü

YEMİN METNİ

Doktora tezi olarak sunduğum “**Sosyal Mühendislik Bağlamında Bilgi Güvenliğinin Endüstri 4.0 Tabanlı Sistemlere Uyarlanması**” adlı çalışmamın, tarafımdan bilimsel ahlak ve geleneklere aykırı düşecek bir yardıma başvurmaksızın yazıldığını ve yararlandığım kaynakların kaynakçada gösterilenlerden oluştuğunu, bunlara atıf yapılarak yararlanılmış olduğunu belirtir ve bunu onurumla doğrularım.

...../...../2020

Cevdet ÖZMEN

imza

ÖNSÖZ

İçinde bulunduğumuz yüzyılın teknolojik hızına ve karmaşıklığına ayak uydurabilmek ne bireyler ne de kurumlar açısından kolay gözükmemektedir. Yenilikçi teknolojilerin insanlığa ayak bağı olması yerine faydalı araçlara dönüşebilmesi için mevcut durumu kavrayabilmek, belki bir parça da olsa yakın geleceği öngörebilmek ve hatta tasarlamak açısından oldukça önemli ve gerekli gözükmemektedir. Bu çalışmanın temel amacı, yukarıda bahsedilen süreçlere olan farkındalığın ortaya çıkartılması ve daha kolay yönetilebilmeleri açısından, öne çıkan üç ana kavram olan; Sosyal Mühendislik, Bilgi Güvenliği ve Endüstri 4.0'ın ayrı ayrı açıklanmasının yanı sıra, bu kavramların ilişkisel ve bütüncü (holistik) olarak yorumlanmalarıdır. Bütüncü yaklaşımın öneminden hareketle, kavramların birbirleriyle ilişkilendirilmesi *sistem yaklaşımı* ve *kaos teorisi* ve kaos teorisi içerisinde yer alan *kelebek etkisi* gözetilerek kurgulanıp, insan merkezi sinir sisteminde (beyin ve omurilik) yer alan nörolojik yapıya analogi yapılarak geliştirilen bir model üzerinden açıklanmaya çalışılmıştır.

Bu çalışmamda bana yol gösteren ve her aşamasında rehberlik eden İşletme Ana Bilim Dalı'ndan hocam ve Tez Danışmanım Prof. Dr. Bayram KAYA başta olmak üzere, çeşitli öneri ve yönlendirmeleriyle katkıda bulunan İşletme Ana Bilim Dalı Başkanı ve hocam Doç. Dr. Kurtuluş Yılmaz GENÇ'e, İstatistik Ana Bilim Dalı Başkanı ve hocam Prof. Dr. Erol EĞRİOĞLU'na ve hocam Doç. Dr. Eren BAŞ'a, Sosyoloji Ana Bilim Dalı'ndan Dr. Öğr. Üyesi Nezihe Başak ERGİN ve Dr. Öğr. Üyesi Emine ERDOĞAN ÇİNAZ'a, Gazi Üniversitesi'nden Prof. Dr. Rüya ÖZMEN'e, yurt dışı alan araştırması sürecinde randevu alımlarında ve sahaya erişimde önemli katkıları olan Ruhi ÖZMEN ve Tony BOYLAN'a, İngilizce ses kayıtlarının bilgisayar ortamında yazıya aktarılmasında Ruben ÖZMEN'e teşekkür ederim.

Saygılarımla,
Cevdet ÖZMEN
Giresun 2020

ÖZET

**SOSYAL MÜHENDİSLİK BAĞLAMINDA BİLGİ GÜVENLİĞİNİN
ENDÜSTRİ 4.0 TABANLI SİSTEMLERE UYARLANMASI**

Medeniyetlerin yükseliş ya da çöküşleri, karşılaşabilecekleri kırılma anlarının öngörülüp yönetilebilmeleri ya da anlaşılamamalarıyla doğrudan ilintilidir. Bu manada, doğru zamanlamayla küçük de olsa anlamlı öngörü ve önlemlerin, geç kalınmış maliyetli yatırımlardan çok daha fazla fayda sağlayacağı açıktır. Günümüzdeki teknolojik büyüme ve iletişim hızındaki artış, süreç döngülerini hem karmaşık hem de kontrolü zor bir duruma sokabilmektedir. Parçaların her birinin öneminin göz ardı edilemeyeceği fakat esas olanın büyük resmi görebilmek olduğu gözden kaçırılmamalıdır. Bu çalışma özellikle içinde bulunduğumuz ve yakın gelecek zaman diliminde yaşamı daha fazla kuşatacak olan bir sürecin yapı taşlarını oluşturan Sosyal Mühendislik, Bilgi Güvenliği ve Endüstri 4.0'ın ilişkisinin ortaya konulması amaçlanarak yapılmıştır. Bu kavramların bütüncü (holistik) olarak yorumlanmaları da oldukça önemlidir. İlişkilendirme süreci *sistem yaklaşımı*, *kaos teorisi* ve *kaos teorisi* içerisinde yer alan *kelebek etkisi*'ne dayandırılmıştır. Bu sürecin işleyişi ise insan merkezi sinir sisteminde yer alan nörolojik yapıyla benzeşim (analoji) yapılarak kurgulanan bir model üzerinden açıklanmaya çalışılmıştır. Literatür araştırması sonucunda elde edilen bulgular, yurt içi ve yurt dışında bulunan ve ağırlıklı olarak bilgi teknolojileri alanında önde gelen kurum ve kuruluşlarda görev yapan, bilgi teknolojisi yöneticisi ve benzer pozisyonlarda bulunan yöneticiler ile yapılan yarı yapılandırılmış görüşmeler neticesinde elde edilen veriler doğrultusunda yorumlanmıştır. Çalışmada yer alan üç ana kavram için şu ana kadar ilişkisel ve bütüncü bir yaklaşım içeren bir çalışmanın yapılmadığı, bu bağlamda organizasyonlarda güvenlik ve yapısal açıkların varlığının yeterince ortaya konulmadığı, ayrıca bu yöndeki risklerin katlanarak arttığı görülmüştür. Siber dünyadaki gelişmelerin ve yapay zekâ alanındaki çalışmaların işletme, kurum, kuruluş ve devletlere karşı olumsuz yönde daha yoğun ve daha tehlikeli boyutlarda kullanılmaya başlamasından önce, gerekli önlemlerin mümkün olan en kısa süre içerisinde alınması gerektiği sonucuna ulaşılmıştır. Teknoloji okuryazarı olan, çeşitli eğitimlerle desteklenmiş donanımlı insan kaynağının oluşturulması, sızma testlerinin

(penetration testing) yapılması ve risklere yönelik farkındalık yaratmanın en ekonomik ve en hızlı alınabilecek önlemlerin başında yer aldığı tespit edilmiştir. Basit ama etkili olan bu önlemler sayesinde risklerin büyük oranda engellenebileceği düşünülmektedir.

Yenilikçi teknolojiler çatısı altında sektörel kavramların bütüncü bir yaklaşımla değerlendirilmesi işletmelerde nihai amaç olan karlılığın artırılmasının yanı sıra verimliliğin optimizasyonuna, hizmetin hızlı ve kesintisiz sunulabilmesine, işletme güvenilirliğinin korunmasına, değişken piyasa koşulları ve rekabetçi ekosistem içerisinde işletme varlıklarının artırılmasına önemli katkılar sunacaktır. Günümüz işletmelerinin “varlık” olarak gördükleri veri’nin korunmasına ve Endüstri 4.0 çatısı altında güvenli bir geleceğin inşasına çeşitli katkılar sunacağını düşündüğümüz bu çalışmanın ayrıca, yönetici kadrolarına da farklı bakış açıları kazandırabileceği düşünülmektedir.

Anahtar Kelimeler: Sosyal Mühendislik, Bilgi Güvenliği, Endüstri 4.0, Sistem Yaklaşımı, Kaos Teorisi

ABSTRACT**THE ADAPTATION OF INFORMATION SECURITY TO INDUSTRY 4.0
BASED SYSTEMS IN THE CONTEXT OF SOCIAL ENGINEERING**

Rises or collapses of civilizations are directly related to the ability to predict and manage the moments of breaking that they may encounter. In this sense, it is clear that meaningful forecasts and measures, albeit small, with the right timing, will benefit much more than late-cost investments. Today's technological growth and increase in communication speed can put the process cycles in a complex and difficult state to control. It should not be overlooked that the importance of each piece cannot be ignored, but the main thing is to see the big picture. This study was carried out with the aim of revealing the relationship between Social Engineering, Information Security and Industry 4.0, which are the building blocks of a process that we are in and will encompass life more in the near future. It is also very important that these concepts are interpreted as holistic. The relationship between the concepts is explained by a model developed by analogy with the neurological structure in the human central nervous system by considering the *system approach*, *chaos theory* and the *butterfly effect* within *the chaos theory*. The findings obtained in this study have been interpreted based on the conceptual framework which is drawn through literature review, these findings are obtained as a result of semi-structured interviews conducted with information technology managers or managers in similar positions, mainly in leading institutions and organizations in the field of information technologies. It has been observed that a relational approach has not been adequately perceived and applied in the three main concepts Social Engineering, Information Security and Industry 4.0, and therefore, structural deficits have emerged in organizations and the existing risks have increased exponentially. It was concluded that the necessary measures should be taken as soon as possible before the developments in the cyber world and the works in the field of artificial intelligence are started to be used in a more intensive and more dangerous manner negatively against the enterprises, institutions and organizations and even the states. It is determined that the creation of well-equipped human resources, which are technology literate, supported by various trainings, conducting penetration tests and

raising awareness for risks are at the top of the most economical and fastest measures to be taken. It is predicted that risks can be prevented to a great extent thanks to these simple but effective initiatives.

Evaluating sectoral concepts with a holistic approach under the roof of innovative technologies will contribute to the optimization of efficiency, rapid and uninterrupted service delivery, preservation of business reliability, and increasing business assets in a competitive ecosystem, as well as increasing profitability, which is the ultimate goal in enterprises. It is thought that this study, which we think will contribute to the protection of the data that today's businesses see as "assets" and to the construction of a secure future under the umbrella of Industry 4.0, can also bring different perspectives to the executive staff.

Keywords: Social Engineering, Information Security, Industry 4.0, System Approach, Chaos Theory.

İÇİNDEKİLER

ÖNSÖZ.....	I
ÖZET.....	II
ABSTRACT	IV
KISALTMALAR	XII
TABLolar LİSTESİ.....	XIV
ŞEKİLLER LİSTESİ.....	XVI
GİRİŞ	1
BİRİNCİ BÖLÜM.....	7
1. SOSYAL MÜHENDİSLİK	7
1.1 Tanımı.....	9
1.2 Tarihi Süreç	18
1.3 Sosyal Mühendislikle Etkileşimli Kavramlar	20
1.3.1 Algı ve Gerçeklik Kavramı	21
1.3.2 Algı Yönetimi	22
1.3.3 Sosyal Algı	24
1.3.4 Stratejik Algı Yönetimi	26
1.3.5 Gündem Belirleme ve Propaganda.....	27
1.3.6 Geleceği Şekillendirme	28
1.3.7 Sosyal Kanıt	29
1.3.8 Toplum Mühendisliği.....	30
1.3.9 Çerçeveleme Etkisi (<i>Framing Effect</i>)	31
1.3.10 Manipülasyon.....	33
1.3.11 Nöro Linguistik Programlama (NLP)	35
1.3.12 Sevgi ve İtaat.....	36
1.3.13 Teknoloji Okuryazarlığı	37
1.3.14 Medya Okuryazarlığı	38
1.3.15 Mahremiyet (<i>Privacy</i>)	39
1.3.16 Heuristics	42
1.3.17 Etik	42

1.4 Sosyal Mühendislik ve Sektörel İlişkiler	44
1.4.1 Sosyal Mühendislik ve (Sosyal) Medya.....	44
1.4.2 Sosyal Mühendislik ve Politika.....	48
1.4.3 Sosyal Mühendislik ve Pazarlama	50
1.4.4 Sosyal Mühendislik ve Sağlık	51
1.4.5 Sosyal Mühendislik ve Teknoloji	51
1.5 Sosyal Mühendislik Araçları ve Çıktıları.....	52
1.6 Sosyal Mühendislikte Genel Saldırı Teknikleri.....	63
1.6.1 Sosyal Mühendislik Alanında Bilinen (En Çok Tercih Edilen) Saldırı Teknikleri.....	67
1.6.1.1 Bahane Üretme (<i>Pretexting</i>)	68
1.6.1.2 Kimlik Avı / Oltalama (<i>Phishing</i>)	68
1.6.1.3 Subaşı (<i>Water-Holing</i>).....	68
1.6.1.4 Taviz (<i>Quid Pro Quo</i>).....	69
1.6.1.5 Balküpu Tuzağı (<i>Honeytrap</i>).....	69
1.6.1.6 Yanlış Yönlendirme (<i>Diversion Theft</i>)	69
1.6.1.7 Zıpkınla Avlama (<i>Spear Phishing</i>).....	69
1.6.1.8 Yemleme (<i>Baiting</i>)	69
1.6.1.9 Kuyrukçuluk (<i>Tailgating</i>).....	70
1.6.1.10 Hile (<i>Rogue</i>).....	70
1.6.1.11 Sesli Kimlik Avı (<i>Vishing</i>)	70
1.6.1.12 Korkutma (<i>Scareware</i>)	70
1.6.1.13 Omuz Sörfü (<i>Shoulder Surfing</i>).....	71
1.6.1.14 Çöp Karıştırma (<i>Dumpster Diving, Skipping</i>)	71
1.6.2 Sosyal Mühendislik Saldırı Vektörleri.....	74
1.6.3 Sosyal Mühendislik Saldırı Döngüsü.....	74
1.6.3.1 Bilgi Toplama	75
1.6.3.2 İlişki Kurma ve Raporlama.....	75
1.6.3.3 İstismar (Faydalanma)	76
1.6.3.4 Sonuçlandırma (İcra, Uygulama).....	76
1.6.4 Sosyal Mühendislik Yaşam Döngüsü	76
1.6.4.1 İz Sürme (<i>Footprinting</i>).....	77

1.6.4.2	Güven İnşası (<i>Establishing Trust</i>)	77
1.6.4.3	Psikolojik Manipülasyon (<i>Psychological Manipulation</i>)	78
1.6.4.4	Çıkış/Sonlandırma (<i>The Exit</i>)	78
1.6.5	Sosyal Mühendislik Atak Güzergâhı	79
1.7	Sosyal Ağlarda Tersine Sosyal Mühendislik.....	80
1.8	Sosyal Mühendisliğin Tehlikeleri ve Tehditleri.....	82
1.9	Sosyal Mühendislik Saldırılarından Korunma Yöntemleri	87
1.9.1	Güvenlik Politikası.....	106
1.9.2	Eğitim ve Öğretim.....	106
1.9.3	Ağ Yönergesi	106
1.9.4	Denetimler ve Uyum	106
1.9.5	Teknik Prosedürler	106
1.9.6	Fiziksel Erişim Yönergesi.....	106
1.10	Sosyal Mühendislik Örnekleri.....	109
İKİNCİ BÖLÜM		112
2.	BİLGİ GÜVENLİĞİ	112
2.1	Tanımı.....	117
2.2	Tarihi Süreç	120
2.3	Bilgi Toplama Yöntemleri	122
2.4	Bilgi Yönetimi	123
2.5	Bilgi Güvenliğine Yönelik Saldırı ve Önlemler	125
2.5.1	Güvenlik Yönetimi (<i>Security Management</i>)	128
2.5.2	Ağ Güvenliği (<i>Network Security</i>).....	129
2.5.3	Sosyal Ağlarda Güvenlik (<i>Security in Social Networks</i>)	131
2.5.4	Uç/Son Nokta Kullanıcı Güvenliği (<i>Endpoint Security</i>).....	131
2.5.5	Veri Güvenliği (<i>Data Security</i>).....	132
2.5.6	Uygulama Güvenliği (<i>Application Security</i>).....	133
2.5.7	Kimlik ve Erişim Yönetimi (<i>Identity and Access Management</i>)	134
2.5.8	Sanallaştırma ve Bulut (<i>Virtualization and Cloud</i>).....	134
2.5.9	İki Faktörlü Kimlik Doğrulama (<i>Two-Factor Authentication - 2FA</i>).....	135
2.5.10	Fiziksel Güvenlik (<i>Physical Security</i>).....	137
2.5.11	Personel Güvenliği (<i>Personnel Security</i>).....	139

2.5.12	Siber Saldırlara Karşı Güvenlik (<i>Security Against Cyber Attacks</i>)...	140
2.5.12.1	Bilgi Güvenliği Yönetim Sistemleri (<i>Information Security Management Systems - ISMS</i>).....	141
2.5.12.2	Saldırı Tespit/Önleme Sistemleri (<i>Intrusion Dedection System - IDS, Intrusion Prevention System - IPS</i>).....	142
2.5.13	Felaketten Kurtarma (<i>Disaster Recovery</i>).....	143
2.6	Hukuksal Düzenleme ve Sorumluluklar	144
2.6.1	Kişisel Verilerin Korunması Kanunu (6698)	145
2.6.2	Elektronik İmza Kanunu	146
2.6.3	Türk Ceza Kanunda Yer Alan İlgili Maddeler.....	146
2.6.4	5651 Sayılı Kanun.....	147
2.6.5	Siber Olaylara Müdahale Ekipleri (SOME).....	148
2.6.6	Güvenli Veri Akışı Yaklaşımı (<i>Data Free Flow With Trust</i>)	148
2.6.7	Avrupa Birliği Genel Veri Koruma Yönetmeliği (<i>EU General Data Protection Regulation - GDPR</i>).....	149
2.7	Bilgi Güvenliği ve ISO Standartları.....	150
2.7.1	TS ISO/IEC 17799 Bilgi Teknoloji - Bilgi Güvenliği Standardı.....	151
2.7.2	BS7799, BS7799-1, BS7799-2	151
2.7.3	ISO ve IEC	151
2.7.3.1	ISO/IEC 27000-27001-27002-27005	152
2.8	Veri İhlali İstatistikleri	154
ÜÇÜNCÜ BÖLÜM	161	
3. ENDÜSTRİ 4.0.....	161	
3.1 Tanımı.....	165	
3.2 Endüstri 4.0'ın Bileşenleri	167	
3.2.1	Büyük Veri (<i>Big Data</i>) ve Analitiği (<i>Analytics</i>)	169
3.2.2	Bulut Bilişim (<i>Cloud Computing</i>).....	177
3.2.3	Yapay Zekâ (<i>Artificial Intelligence - AI</i>)	179
3.2.4	Bulanık Mantık (<i>Fuzzy Logic</i>)	182
3.2.5	Nesnelerin İnterneti (<i>Internet of Things - IoT</i>).....	184
3.2.6	Siber Güvenlik (<i>Cyber Security</i>).....	192
3.2.7	Siber Fiziksel Sistemler (<i>Cyber Physical Systems</i>).....	196

3.2.8	Otonom Robotlar (<i>Autonomous Robots</i>).....	198
3.2.9	Artırılmış Gerçeklik (<i>Augmented Reality - AR</i>).....	202
3.2.10	Akıllı Bina ve Şehirler (<i>Smart Buildings and Cities</i>)	205
3.2.11	Üç Boyutlu (3B) Yazıcılar (<i>3D Printers</i>).....	208
3.2.12	Proaktif Önlemler (<i>Proactive Prevention</i>)	210
3.3	İşletmelerin Endüstri 4.0'a Adaptasyonu	211
3.4	Endüstri 4.0'ın Önündeki Engeller.....	216
DÖRDÜNCÜ BÖLÜM		221
4. SOSYAL MÜHENDİSLİK, BİLGİ GÜVENLİĞİ VE ENDÜSTRİ 4.0		
KAVRAMLARINA İLİŞKİSEL VE BÜTÜNCÜ BİR YAKLAŞIM.....		221
4.1	Araştırmanın Yöntemi	239
4.1.1	Araştırma Yaklaşımının Doğası.....	239
4.1.2	Araştırma Modeli (Deseni)	240
4.1.3	Çalışma Grubu (Örneklem).....	241
4.1.4	Sahaya Erişim.....	242
4.1.5	Veri Toplama Teknikleri.....	242
4.1.6	Veri Toplama Süreci (Alan Araştırması)	244
4.1.7	Pilot Uygulama	244
4.1.8	Mülakat Görüşmeleri	245
4.1.9	Verilerin Analizi.....	245
4.1.10	Etik.....	250
4.2	Bulgular	250
4.2.1	Demografik Verilere Ait Bulgular	252
4.2.2	Literatür Araştırması Sonucunda Elde Edilen Sosyal Mühendislik, Bilgi Güvenliği ve Endüstri 4.0'ın Kesişme Alanlarına Ait Bileşenlerin Katılımcılara Göre Önem Sıralaması.....	254
4.2.3	Katılımcılar Tarafından Önerilen Bileşenler.....	258
4.2.4	Sorun Analizine Yönelik Bulgular.....	259
4.2.5	Katılımcıların Sosyal Mühendislik, Bilgi Güvenliği ve Endüstri 4.0'ın İlişkilendirilmesine Yönelik Düşüncelerine Ait Bulgular	268
4.2.6	Katılımcıların Endüstri 4.0 Bağlamında Yenilikçi Teknolojilere Yönelik Olumlu ve Olumsuz Görüşlerine Ait Bulgular	270

4.2.7	Kodlama, Kategori ve Temalar	272
4.2.8	Kodlama Kelime Frekans Dağılımları	283
4.3	Yorum.....	285
SONUÇ VE ÖNERİLER.....		292
KAYNAKÇA		302
EKLER.....		323
ÖZGEÇMİŞ.....		334



KISALTMALAR

2FA (*Two-Factor Authentication*): İki Faktörlü Kimlik Doğrulama

3B Yazıcılar: Üç Boyutlu Yazıcılar

B2B (*Business to Business*): İşletmeden İşletmeye

B2C (*Business to Consumer*): İşletmeden Tüketicie

BG: Bilgi Güvenliği

BI (*Business Intelligence*): İş Zekâsı

BİT: Bilgi ve İletişim Teknolojileri

BT (Bilgi Teknolojileri / IT: *Information Technology*): Bilgisayar (yazılım ve donanım) ve iletişim teknolojilerinin (veri, ses iletişimi, ağlar vb.) bileşimi

C2 (*Command and Control*): Komuta ve Kontrol

C2C (*Consumer to Consumer*): Tüketiciden Tüketicie

CPS (*Cyber Physical Systems*): Siber Fiziksel Sistemler

DNS (*Domain Name System*): Alan Adı Sistemi

E 4.0: Endüstri 4.0

EPC (*Electronic Product Code*): Elektronik Ürün Kodu

ERP (*Enterprise Resource Planning*): Kurumsal Kaynak Planlaması

E-TAG (*Electronic Tag*): Elektronik Etiket

GPS (*Global Positioning Systems*): Küresel Yer Belirleme Sistemleri

GSM (*Global System for Mobile Communications / Groupe Spécial Mobile*): Mobil İletişimler İçin Küresel Sistem Standardı

HQ (*Headquarter*): Genel Merkez

HVAC (*Heating Ventilating and Air Conditioning*): Isıtma, Havalandırma ve Klima

IDS (*Intrusion Detection System*): Saldırı Tespit Sistemi

IIoT (*Industrial Internet of Things*): Endüstriyel Nesnelerin İnterneti

INFOSEC (*Information Security*): Bilgi Güvenliği

IoT (*Internet of Things*): Nesnelerin İnterneti

IT (*Information Technology*): BT (Bilgi Teknolojileri)

JIT (*Just in Time*): Tam Zamanında (üretim)

M2M (*Machine to Machine*): Makineden Makine'ye (İletişim)

NFC (*Near Field Communication*): Yakın Alan İletişimi

NLP (*Neuro Linguistic Programming*): Nöro Linguistik Programlama

OTA (*Over The Air*): Havadan

PIN (*Personal Identification Number*): Kişisel Kimlik Doğrulama Numarası

QR Code (*Quick Response Code*): Kare Kod

RFI (*Radio Frequency Interference*): Radyo Frekans Paraziti

RFID (*Radio Frequency Identification*): Radyo Dalgası Kullanarak
Kimliklendirme/Tanımlama

SIP (*Session Initiation Protocol*): Oturum Başlatma Protokolü

SM: Sosyal Mühendislik

SSL (*Secure Sockets Layer*): İnternet üzerindeki bilgi akışı sırasında güvenlik ve gizliliğin gerçekleştirilmesi amacıyla geliştirilmiş bir güvenlik protokolü

TEMPEST (*Transient Electromagnetic Pulse Emanation Standard*):
Elektromanyetik Sızıntılardan Korunma Standardı

TT (*Touchless Technologies*): Temassız Teknolojiler

URL (*Uniform Resource Locator*): Standart Kaynak Bulucu, web site adresi

USB (*Universal Serial Bus*): Evrensel Seri (bağlantı) Veriyolu

VoIP (*Voice Over Internet Protocol*): İnternet Üzerinden Ses Protokolü

VPN (*Virtual Private Network*) Sanal Özel Ağ

TABLÖLAR LİSTESİ

Tablo 1. Sosyal Mühendislik Tanımlarının Yöntem/Hedef/Amaç Sınıflandırması-I	15
Tablo 2. Sosyal Mühendislik Tanımlarının Yöntem/Hedef/Amaç Sınıflandırması-II	16
Tablo 3. Sosyal Mühendislik Kısaca Nedir, Nasıl Kullanılmaktadır ve Nasıl Korunulur?	17
Tablo 4. Sosyal Mühendislik Araçları ve Çıktıları	62
Tablo 5. Sosyal Mühendislik'in Karakteristik Yapısı	63
Tablo 6. Bazı Sosyal Mühendislik Ataklarından Korunma Yöntemleri ve Önlemler	91
Tablo 7. Sosyal Mühendislik Taktikleri, Zafiyetler (Güvenlik Açıkları) ve Azaltıcı (Hafifletici) Önlemler	102
Tablo 8. Güvenlik Ataklarının Sektörel Dağılımı (Olay Sayısına Göre)	158
Tablo 9. Çalışma Grubuna Ait Demografik Veriler	252
Tablo 10. Yaş Grubuna Ait Tanımlayıcı İstatistikler	253
Tablo 11. Meslek/Eğitim Çapraz Tablolama	253
Tablo 12. Sosyal Mühendislik, Bilgi Güvenliği ve Endüstri 4.0'ın Kesişme Alanlarına Ait Bileşenlerin Katılımcılara Göre Önem Sıralaması	254
Tablo 13. Katılımcılar Tarafından Önerilen Diğer Bileşenler	258
Tablo 14. Literatür Araştırması Sonucunda Oluşturulan Sorun Analizi'nde (Şekil 61) Yer Alan Tespitlere Yönelik Olarak Katılımcıların Söylemlerinden Elde Edilen Destekleyici Bulgular	261
Tablo 15. Literatür Araştırması Sonucunda Oluşturulan Sorun Analizi'nde (Şekil 61) Yer Almayan Fakat Alan Araştırması Sonucunda Sorun Analizine Eklenen Tespitlere (Şekil 62) Yönelik Olarak Katılımcıların Söylemlerinden Elde Edilen Bulgular	267
Tablo 16. Katılımcıların Sosyal Mühendislik, Bilgi Güvenliği ve Endüstri 4.0'ın İlişkilendirilmesine Yönelik Düşünceleri – I	269
Tablo 17. Katılımcıların Sosyal Mühendislik, Bilgi Güvenliği ve Endüstri 4.0'ın İlişkilendirilmesine Yönelik Düşünceleri – II	270
Tablo 18. Katılımcıların Endüstri 4.0 Bağlamında Yenilikçi Teknolojilere Yönelik Olumlu ve Olumsuz Görüşleri	271

Tablo 19. Kodlama ve Kategorilerin Oluřturulması	273
Tablo 20. Důğüm Özeti Raporu (<i>Node Summary Report</i>) (NVivo 10 Uygulaması)	282



ŞEKİLLER LİSTESİ

Şekil 1. Çerçeveleme Etkisi-I	32
Şekil 2. Çerçeveleme Etkisi-II	32
Şekil 3. Sevgi ve İtaat (“Evet Deme”) İlişkisi	37
Şekil 4. Tehlike İçerikli E-Posta Saldırılarının Haftanın Günlerine Göre Dağılımı..	47
Şekil 5. Tehlike İçerikli E-Posta Saldırılarının Günün Saatlerine Göre Dağılımı	47
Şekil 6. Tehlike İçerikli Sosyal Medya Saldırılarının Günün Saatlerine Göre Dağılımı	48
Şekil 7. Tim Roth’un “ <i>Lie To Me</i> ” İsimli Dizide Cal Lightman Rolünde Göstermiş Olduğu Mikro-İfadeler.	58
Şekil 8. Project Hostile Intent (Tehdit Algılama)	59
Şekil 9. Sosyal Mühendislik Saldırısının Ontolojik Bir Modeli	66
Şekil 10. Sosyal Mühendislik Saldırı Teknikleri	67
Şekil 11. İkiz Görünümlü Web Siteleri (Arayüzleri) - Google.....	73
Şekil 12. İkiz Görünümlü Web Siteleri (Arayüzleri) - Facebook.....	73
Şekil 13. En Temel Sosyal Mühendislik Saldırı Döngüsü.....	75
Şekil 14. Sosyal Mühendislik Yaşam Döngüsü-I	77
Şekil 15. Sosyal Mühendislik Yaşam Döngüsü-II.....	78
Şekil 16. Sosyal Mühendislik Atak Güzergâhı	80
Şekil 17. Tersine Sosyal Mühendislik	82
Şekil 18. Sosyal Mühendisliğin Kırmızı Bayrakları (Belirtileri).....	93
Şekil 19. Sosyal Mühendisliğe Karşı Önleyici Stratejiler	102
Şekil 20. Bilgi Güvenliği Yapbozu’nun Unsurları	116
Şekil 21. Bilgi Güvenliği Üçgeni (AIC Triangle).....	118
Şekil 22. Bilgi Güvenliğinin (Temel) Prensipleri	119
Şekil 23. Bilgi Güvenliği Alt Başlıkları.....	128
Şekil 24. STS’nin Ağda Konumlandırılması	142
Şekil 25. SÖS’ün Ağda Konumlandırılması.....	143
Şekil 26. Veri İhlalleri Kaynak Dağılımı	155
Şekil 27. Sosyal Taktiklerin Kendi İçerisinde Dağılımı - 2010.....	155
Şekil 28. Sosyal Taktiklerin Kendi İçerisinde Dağılımı - 2011.....	156
Şekil 29. Bir Veri İhlalinin Ortaya Çıkışı ve Rotası	159

Şekil 30. Endüstri 4.0 Prensipleri	166
Şekil 31. Endüstri 4.0'ın Temel Bileşenleri.....	168
Şekil 32. Büyük Veri'nin Bileşenleri.....	170
Şekil 33. Data Never Sleeps 6.0 Raporu.....	172
Şekil 34. Büyük Veri ve Kritik İş Birimleri.....	176
Şekil 35. Bulut Bilişim'in Avantaj ve Dezavantajları	178
Şekil 36. Enformasyon Değer Döngüsü.....	188
Şekil 37. Nesnelerin İnterneti (IoT) ve Sektörler.....	190
Şekil 38. Küresel Çapta Siber Suçların Sektör Bazında Yıllık Ortalama Maliyetleri	196
Şekil 39. Otonom Robotlar	201
Şekil 40. Yıllara Göre Kalite Yaklaşımları.....	204
Şekil 41. Artırılmış Gerçeklik.....	204
Şekil 42. Akıllı Binalar	207
Şekil 43. Akıllı Şehirler	207
Şekil 44. Üç Boyutlu (3B) Yazıcılar - Örnek I	209
Şekil 45. Üç Boyutlu (3B) Yazıcılar - Örnek II.....	209
Şekil 46. İşletmelerde Dijital Kültür Özellikleri.....	215
Şekil 47. Sosyal Mühendislik ve Bilgi Teknolojileri Güvenlik Testleri.....	226
Şekil 48. Sosyal Mühendislik, Bilgi Güvenliği ve Endüstri 4.0'ın Kesişme Alanları	227
Şekil 49. Sosyal Mühendislik, Bilgi Güvenliği ve Endüstri 4.0'ın Kesişme Alanlarına Ait Bileşenler	228
Şekil 50. Sinir Hücresi (Nöron) Yapısı ve Bağlantıları	234
Şekil 51. Multipl Skleroz (MS) Hastalığı	235
Şekil 52. Merkezi Sinir Sistemi	235
Şekil 53. Sosyal Mühendislik, Bilgi Güvenliği ve Endüstri 4.0'ın İlişkisel Tasarım Modellemesi	237
Şekil 54. Veri Çözümlemesinin Bileşenleri: Etkileşimli Model.....	247
Şekil 55. Nitel Veri Analizi Süreci	247
Şekil 56. En Önemli (İlk) Üç Bileşen	255
Şekil 57. En Az Önemli (Son) Üç Bileşen.....	255

Şekil 58. Sosyal Mühendislik, Bilgi Güvenliği ve Endüstri 4.0'ın Kesişme Alanlarına Ait Bileşenlerin Katılımcılara Göre Önem Sıralaması-I.....	256
Şekil 59. Sosyal Mühendislik, Bilgi Güvenliği ve Endüstri 4.0'ın Kesişme Alanlarına Ait Bileşenlerin Katılımcılara Göre Önem Sıralaması-II.....	257
Şekil 60. Sosyal Mühendislik, Bilgi Güvenliği ve Endüstri 4.0'ın Kesişme Alanlarına Ait Tüm Bileşenler ve Önem Sıralaması	258
Şekil 61. Sorun Analizi-I (Literatür Araştırması Sonucuna Göre)	260
Şekil 62. Sorun Analizi-II (Alan Araştırması Sonucunda Eklenenler).....	266
Şekil 63. Sosyal Mühendislik, Bilgi Güvenliği ve Endüstri 4.0 Temalarına Ait Kategoriler.....	273
Şekil 64. Kodlama Sonucu Elde Edilen Kavramların Kaynaklarla Olan İlişkisi	283
Şekil 65. Kodlama Yapılarak Kategorilerin Oluşturulmasında En Sık Kullanılan 100 Kelime (Frekans Yüksekliğine Göre) (NVivo 10 Uygulaması)	284
Şekil 66. Frekansı En Yüksek 100 Kelime İçin Ekran Sorgulama Görüntüsü (NVivo 10 Uygulaması)	284

GİRİŞ

Yüzyılın teknolojik hızına ve karmaşıklığına ayak uydurarak ondan mümkün olduğunca en üst düzeyde faydalanabilmek ancak bu alanla ilgili kavramların neler olduğunun bilinmesi, yönetilebilmesi, ilişkisel ve bütüncü yaklaşımlar sayesinde doğru çıkarımların yapılabilmesiyle mümkün gözükmektedir. Yenilikçi teknolojilerin insanlığa ayak bağı olması yerine faydalı araçlara dönüşebilmesi ancak ilgili teknoloji ve kavramların bir bütünlük içerisinde ele alınmasıyla mümkündür. Bu çalışmanın merkezi, yukarıda bahsedilen süreçlere yönelik farkındalığın ortaya konulması ve daha kolay yönetilebilmeleri açısından, öne çıkan üç ana unsur olan; Sosyal Mühendislik (SM), Bilgi Güvenliği (BG) ve Endüstri 4.0 (E 4.0)'ın ayrı ayrı açıklanmasının yanı sıra, ilişkisel ve bütüncü (holistik) olarak yorumlanmalarının daha önemli olduğu düşüncesi üzerine kuruludur.

SM başlığı altında algı, algı yönetimi, yönlendirme ve manipülasyon, sosyal mühendislik saldırı teknikleri; BG başlığı altında mahremiyet, kişisel ve kurumsal veri güvenliği ile iletişim teknolojileri üzerinde gerçekleştirilen veri akışı ve içerik güvenliği, siber güvenlik; E 4.0 başlığı altında ise daha çok, otomasyon, robotik ve yapay zekâya dayalı algoritmalar ile Nesnelerin İnterneti (Internet of Things-IoT), M2M, akıllı fabrikalar ve akıllı şehirler yer almaktadır.

SM ve BG çok yeni konular olmamakla birlikte, henüz birkaç yıldır konuşulan E 4.0 ile olan sıkı bağlantıları ve yakın gelecek olarak kabul edebileceğimiz önümüzdeki on beş yirmi yıl sürecinde teknolojik gelişme ve ilerlemenin ağırlıklı olarak bu platform üzerinde cereyan edeceği öngörüsünden hareketle, bu üç kavramın etkileşim, kesişme ve etki alanlarının önemi ve genişliği, bu kavramların birlikte ele alınması zorunluluğunu doğurmaktadır.

Araştırmanın Amacı ve Problem Cümleleri: Bu çalışmada sosyal mühendislik bağlamında bilgi güvenliğinin endüstri 4.0 tabanlı sistemlere uyarlanmasıyla ülkemizde ve yurt dışında bu alanlara yönelik ne tür girişimlerin bulunduğu, farkındalık, genel eksikliklerin neler olduğu, konunun işletmeler ve kurumlar açısından ne tür riskler doğurduğu/doğurabileceği, bu risklerin maddi ve manevi boyutları, kişiler (müşteriler, kullanıcılar, çalışanlar) ve yönetimlerin konunun içeriği ve önemi hakkında ne düzeyde bilgi sahibi olduğu ve genel yaklaşımları

araştırılmıştır. Bununla birlikte E 4.0'ın neleri kapsayacağı ve nelerden etkileneceğine dair güncel ve yakın gelecekteki çalışmalar ve içerikleri hakkında bilgilerin ve verilerin ortaya konularak, konuyla ilgili paydaşların bilinçlendirilmesi ve çeşitli tutumlar geliştirebilmeleri ve ön alıcı çalışmalar yapabilmelerine yönelik stratejik katkılar sunmak amaçlanmıştır. SM, BG ve E 4.0 konularının ilişkisel düzeyde ele alınarak ortak yanlarının ortaya çıkartılması ve bu yönde var olan farkındalığın ne düzeyde olduğunun belirlenmesinin de hedeflendiği bu araştırmada yer alan genel amaç ve alt amaçlar (problem cümleleri) şu şekilde belirlenmiştir:

Genel Amaç: Bilgi İşlem Teknolojileri ve yakın alanlarda faaliyet gösteren kurum ve kuruluşlarda Bilgi Teknolojileri Yöneticisi ya da benzer pozisyonda görev yapan kişilerin SM, BG ve E 4.0'ın birbirleriyle olan ilişki ve örtüşmeleri hakkındaki farkındalıklarını, yaptıkları çalışmaları, karşılaştıkları/karşılaşabilecekleri riskleri, aldıkları önlemleri ortaya çıkartarak, bu ilişki ve örtüşmenin öneminin bilinmesinin kişilere/kurumlara olası getirilerini tespit etmek ve (bulgulara dayalı) öneriler sunmaktır. Bu genel amaç çerçevesinde şu sorulara da yanıt aranmıştır:

Alt Amaçlar: Yöneticilerin SM, BG ve E 4.0'ın birbiriyle olan ilişkileri hakkında;

- Yaptıkları çalışmalar nelerdir
- Ne tür eğitimler söz konusudur
- Bu çalışmaların getirileri hakkındaki düşünceleri nelerdir
- Karşılaştıkları/karşılaşabilecekleri riskler nelerdir
- Bu risklere karşı almış oldukları önlemler nelerdir
- SM, BG ve E 4.0 kavramlarının ilişkilendirilmesine yönelik ne tür girişimleri bulunmakta ve diğer kurumlara verebilecekleri öneriler nelerdir

Eğitim, bilgilendirme, teknik ve ekonomik desteklerin yanı sıra teknolojik, bilişim ve hukuksal alt yapıların oluşturulması, mevcut durum ve bakış açılarının iyileştirilmesi, çağdaş misyon ve vizyonların tanımlanarak, stratejik hedefler ile politikaların belirlenmesi, SM, BG ve E 4.0 kavramları ve kesişme noktaları için kısa, orta ve uzun vadeli yol haritalarının çıkartılmasına katkılar sunmak ve ayrıca

kavramlara ilişkin ilişkisel farkındalık yaratmak bu çalışmanın diğer amaçlarını oluşturmaktadır.

Araştırmanın Önemi: İnsan yaşamının ayrılmaz bir parçası olan teknoloji, özellikle hızlı/anlık bilgi paylaşımı ve küresel ekonomiler herkesi birbirine yakınlaştırmış, hatta bağlamıştır. Neredeyse tüm iş süreçlerinin dijital ortamlara taşındığı düşünülecek olursa, özel yaşama dair bilgilerden, şirket proje içeriklerine kadar her türlü bilginin internet ortamında (izinli/izinsiz) paylaşıldığına ve manipüle edilebildiğine şahit olmaktayız. Dolaşıma giren bu (doğru/yanlış/müdahale edilmiş) bilgiler bir taraftan kişilerin yaşamlarını, öte yandan kurumların iş dünyasını menfi ya da müspet yönde etkileyebilmektedir. Örneğin; kişisel verilerin ya da silah sanayisindeki bir firmanın çok önemli bilgilerinin bilinçli ya da sehven ifşa edilmesine değin birçok verinin kötü niyetli kişiler tarafından çalınarak ya da manipüle edilerek yayımlanması çok ciddi hasarlara sebebiyet verebilmektedir. Bilinen konvansiyonel savaşların yerini artık dijital platformlar üzerinde gerçekleştirilen ekonomi ve bilgi şekillendirmeli sosyal mühendislik müdahaleleri, bilgi temelli rekabetler, siber saldırılar vb. almaktadır. Yakın gelecekte bu tür girişimlerin E 4.0 olarak adlandırılan yapı üzerinde salınacağını düşünecek olursak, çalışma konumuz olan bu üç ana kavramın (SM, BG, ve E 4.0) yollarının kesişmesi kaçınılmaz gözükmemektedir. Bu durumun önemini fark ederek sosyo-ekonomik ve teknolojik yapıyı kontrol edebilen ve yönetebilenlerin hep bir adım önde olacağını söylemek mümkündür. Alt bileşenlerinin de yardımı ile burada bahsedilen kavramların kesişme noktaları açıklanırken ne tür stratejilerin izleneceğinin açıkça ortaya konulması ve yalın örneklerle anlatılmasının yanı sıra, konunun uzmanı kişilerle yapılan görüşme ve değerlendirmeler ışığında doğru perspektiflerin çizilebilmesi için önümüzde uzanan dijital dünyanın ve sanayinin yapısının anlaşılabilmesinin de oldukça önemli olduğunu düşünmekteyiz.

Literatüre bakıldığında yukarıda bahsedilen bu kavramların ayrı ayrı ele alındığını (Kurzweil, 2019; Kahneman, 2018; Albert, 2018; Apak, 2018; Awad, 2018; Banger, 2018; Biswas, 2018; Bostrom, 2018; Cialdini, 2018; Çavuş, 2018; Çoban, 2018; Furnell, 2018; Harari, 2018; Løkke, 2018; Hadnagy, 2017; Aslanbakan, 2017; Kaku, 2017; Davenport, 2014; Ok, 2013; Quiel, 2013; Bölükbaşı, 2012; Abuşka, 2010; Mann, 2008; Mitnick ve Simon, 2001) ancak birbirleri ile olan

ilişkileri bağlamında (ikili ya da üçlü bağlantılar şeklinde) yeterince irdelenmedikleri görülmektedir. Bu çalışmada, SM, BG ve E 4.0 kavramlarının birlikte ele alınarak aralarındaki ilişkilerin çeşitli açılardan ortaya konulmasının literatüre önemli katkılar sunacağı düşünülmektedir.

Bilişim teknolojilerinin işletmelere genel olarak sağlamış olduğu şu faydalardan yola çıkacak olursak;

- Bilgiye hızlı erişimi mümkün kılması
- İşletme verimliliğini artırması
- Kurum hafızası, müşteri portföyü ve güvenli arşivlemeyi mümkün kılması
- Üretim maliyetlerinin azaltılmasına katkı sağlaması
- Sıfır hataya yaklaşarak üretimde verimliliği artırması
- Küresel rekabette avantajlar sağlaması

ve benzeri alanlara yönelik güncel yaklaşımların E 4.0 platformundan bağımsız olamayacağı düşünülmektedir. Öte yandan, teknolojilerden faydalanmanın yanı sıra, getirebileceği risklerin neler olduğu ve korunma yollarının da bilinmesi gerekmektedir. Bu tutum; risk ve maliyetleri azaltma, her türlü güvenlik önlemlerinin alınması, verimlilik, iş süreçlerinin devamlılığı gibi birçok alanda işletme, kurum ve devlet yönetimlerine katkı sağlayabilecektir. Bu çalışmada elde edilecek bulgular sayesinde sistematik ve stratejik yapılanmalara yönelik pratik çözümlerin üretilebileceği düşünülmektedir.

Araştırmanın Kapsamı ve Sınırlılıkları: Araştırma, SM, BG ve E 4.0'ın yanı sıra bu kavramlara ait (alt) bileşenlerin de büyük bir kısmını kapsamaktadır. Çalışmada yer alan veriler, çeşitli rapor ve doküman incelemesi, gözlem ve görüşme teknikleri yoluyla elde edilmiştir. Araştırmaya dâhil edilen rapor, makale, internet kaynakları ve kitaplardan elde edilen teorik verilerin yanı sıra yapılan görüşmelerden elde edilen verilerin çalışmada yer alan kavramların açıklanabilmesi ve anlaşılabilmesine önemli katkılar sunacağı düşünülmektedir.

Görüşmeye katılanlardan görüşme sorularına içtenlikle cevap vermeleri için kısa ön sohbetler gerçekleştirilerek, araştırmaya yönelik çeşitli konularda bilgilendirmeler yapılmıştır. Geliştirilen “görüşme formunun”, cevap aranan sorulara yönelik yeterli içeriğe sahip olduğu düşünülmektedir. Bunu desteklemek için

gerçekleştirilen pilot uygulama çalışmasının verileri, uzman kişilerin gözetiminde tartışıldıktan sonra esas uygulamaya geçilmiştir.

Nitel araştırma yöntemlerinden yarı yapılandırılmış görüşme tekniği kullanılarak yurtiçi ve yurt dışında (Türkiye ve İrlanda) toplam on farklı kurum ile yapılan araştırmada elde edilen veriler içerik analizi ve betimsel analiz kullanılarak yorumlanmıştır. Alan araştırması için seçilen kurumların araştırmaya katkı sunabilecek kurumlar olmasına özen gösterilmiştir. Sayının on kurum ile sınırlı tutulması, yeterli verilerin elde edilebileceği varsayımının yanı sıra, araştırmanın bütçesi ve alan çalışması için ayrılan sürenin dikkate alınmasıyla da ilişkilidir.

Bu çalışma dört bölümden oluşmaktadır:

Birinci, ikinci ve üçüncü bölümlerde; sırasıyla SM, BG ve E 4.0 konuları ele alınarak, tanımlar, kavramlar, literatür ve güncel yaklaşımlar çeşitli kaynaklardan faydalanılarak açıklanmış, yalın bir anlatımla konuya en yabancı olanların dahi bilgi sahibi olabilmelerine çalışılmıştır. SM başlığı altında; kapsadığı alan, tarihsel süreç ve günümüzdeki kullanım alanları, etkileri ve korunma yöntemlerinden bahsedilmiş, BG başlığı altında; veri-enformasyon-bilgi-bilgelik süreçlerinden bahsedilerek, BG'nin ne anlama geldiği ve önemi (bilgi, bilişim ve iletişim teknolojileri de dâhil olmak üzere) alt bileşenleriyle açıklanmıştır. E 4.0 başlığı altında ise E 4.0'ın nasıl ortaya çıktığı, neden kabul gördüğü, etki alanları ve ülkelerin bu yöndeki hazırlıkları ve hangi aşamalarda oldukları ortaya konulmuştur. E 4.0'a bağlı olarak Nesnelerin İnterneti, artırılmış gerçeklik, makine öğrenmesi, yapay sinir ağları, bulanık mantık, yapay zekâ, 3B yazıcılar, robotik, dijital güvenlik, *blockchain* platformu (kripto paralar, akıllı kontratlar, paylaşım ekonomisi) ve benzeri konular alt başlıklar halinde açıklanmıştır.

Dördüncü bölümde; yukarıda verilen üç ana kavram (özellikle kesişme noktaları dikkate alınarak) ilişkisel ve bütüncü (holistik) bir yaklaşımla değerlendirilmiştir. Bu kavramların kesişme noktaları Venn şeması görseli ile açıklanarak, aralarındaki ilişki çeşitli yönleriyle ortaya konulmuştur. SM, BG ve E 4.0 kavramların birbirleriyle ilişkilendirilmesi *sistem yaklaşımı* ve *kaos teorisi* ve kaos teorisi içerisinde yer alan *kelebek etkisi* gözetilerek kurgulanıp, insan merkezi sinir sisteminde (beyin ve omurilik) yer alan nörolojik yapıyla analogi yapılarak geliştirilen bir model üzerinden açıklanmıştır. Küçük bir SM (müdahalesi) ile BG

tehlikeye girerek E 4.0 tabanlı ve bağılı tüm katmanlar bu durumdan olumsuz etkilenebilecektir. Tıpkı post modern yönetim kuramlarından biri olan *düzensizlik içerisinde düzeni* tarif eden, evrenin doğrusal olmayan (non-linear) yönlerini açıklamaya çalışan *kaos ve karmaşıklık teorisi* ve onun içerisinde yer alan Edward Lorenz'in *kelebek etkisi teorisi*'nde (1972) olduğu gibi. Yine benzer şekilde, ilişkiler, Mayo, Barnard ve Bartalanfy'ın (1937) ve Norbert Wiener'in (1948) olay ve birimlerin birbirleri ile olan ilişkisini dış çevre şartları ile ilişkili olarak da incelediği *sistem yaklaşımı*'ndan hareketle açıklanmaya çalışılmıştır. Sorun analizinde ise *mantıksal çerçeve yaklaşımı* (logical framework approach) kullanılmıştır. Mantıksal Çerçeve Yaklaşımı; “1970’lerde araştırmanın tasarımının niteliğini ve açıklığını iyileştirmek üzere geliştirilmiş bir yaklaşımdır. Düşünmeye yardımcı bir araç olarak düşünülmelidir. Bilginin analiz edilmesi ve yapısal olarak düzenlenmesine olanak sağlamaktadır” (ibb.gov.tr, 2018). Dördüncü bölümün devamında araştırmanın yöntemi, bulgular ve yorumlar kısmı yer almaktadır. Son olarak, sonuç ve önerilere yer verilmiştir.

BİRİNCİ BÖLÜM

1. SOSYAL MÜHENDİSLİK

Bu bölümde, sosyal mühendislik (SM), SM ile etkileşimli kavramlar, SM ve sektörel ilişkiler, SM araçları ve çıktıları, SM’de genel saldırı teknikleri, SM döngüsü, sosyal ağlarda tersine SM, SM’nin başlıca tehlikeleri ve tehditleri ve son olarak SM saldırılarından korunma yöntemleri açıklanacaktır. Ayrıca fikir oluşturma açısından, SM örneklerine de yer verilecektir.

Bu bölümde ele alınacak olan SM’nin, benzer alandaki araştırmalardan temel farkı; insanların büyük bir kısmının SM’nin ne olduğunu tam olarak bilmediği, SM’nin ilgisiz gibi gözüken başka konuların nasıl önemli bir parçası haline gelebildiğini fark etmediği, ne tür zararların oluşabileceği ve hangi önlemlerin alınabileceği hakkında kısmi bilgi sahibi olduğu gözleminden hareketle, SM’nin tüm yönleriyle açıklanarak, biraz bilgi ve dikkat sayesinde birçok SM saldırısından korunulabileceğini sade bir anlatımla ortaya koyabilmektir. Bu sayede kişiler, işletmeler ve kurumlar kendilerini önemli bir ölçüde koruma altına alabileceklerdir.

SM saldırısı yapanlar genel anlamda insanları aşamalı olarak kontrol eden üç farklı yola başvurmaktadır (Proofpoint, Inc., 2016). Bunlar:

- *Saldırganların (yazılım) kodlarının çalıştırılması:* Bu saldırılar genel olarak geniş gruplar halinde çalışan yüksek hacimli kurumlara yönelik girişimlerden oluşmaktadır. Teknik algılamadan (tespitten) kaçınmak için çeşitli yollar kullanılır ve insanları güvenliği devre dışı bırakmaya ya da yok saymaya, bağlantıları tıklamaya, belgeleri açmaya ya da dizüstü bilgisayarlara, tabletlere ve akıllı telefonlara kötü amaçlı yazılım yükleyen dosyaları indirmeye ikna ederler.
- *Saldırganlara kimlik bilgilerinin verilmesi/ifşası:* Bu saldırılar, orta hacimli kurumlarda sıklıkla ortaya çıkmaktadır. Kullanıcı adları ve şifreler gibi önemli kimlik bilgilerine sahip “anahtar” insanlar hedef alınır. Sistemleri veya kritik hizmetleri, “kale anahtarlarını” üzerlerine devralmaları için kandırırlar.
- *Saldırganlar için doğrudan çalışılması ve onlara paraların aktarılması:* Bu saldırılar daha dar kapsamlıdır ama hedefleri büyüktür. Kilit kişiler ve önemli

görevler için yetkileri bulunan kullanıcıların doğrudan saldırganlar adına hareket etmeleri amaçlanır. Bu kişiler, üst düzey yönetimden gelen emirleri takip ettiklerini düşünerek, çoğu zaman sahte banka hesaplarına banka havalesi dahi yapabilmektedir.

Tüm bu saldırılar ölçek ve hacim bakımından farklılıklar içermektedir fakat hepsinin ortak bir amacı vardır: İnsanları belirli şeyleri yapmaya ikna etmek ve buna bağlı olarak çeşitli çıkarlar elde etmek.

Çalışanlar, birçok sebepten dolayı kolayca bilgi ifşa edebilmektedir. Çoğu durumda, insanlar sadece yardımcı olmak istemektedir. Başkalarıyla bu tür bilgileri paylaşmak (bazıları için) onların sıradan ve normal günlük işi olabilir ve bu norm haline gelebilir. Bazı durumlarda ise, kişi belki de sadece konuşkandır ve hangi bilgileri paylaştığından bağımsız olarak konuşmayı sürdürmekten hoşlanır ve bu gibi durumlarda hassas bilgi olarak kabul edilebilecek olanı ifşa etmelerinin istenmesi onlara sıra dışı görünmeyebilir. Özellikle bir meslektaşı, müşterisi ya da müşterisinin resmî bir temsilcisi ile ilgilendiklerini düşünüyorlarsa... İnsanlar ayrıca, otorite konumundaki bir kişinin bilgiye ihtiyaç duyduğuna veya üst yöneticinin isteğine uymadıkları için kınanabileceklerine inanmaya zorlanabildiklerinden ya da sadece sinir bozucu ve inatçı bir kişiyi telefonda (veya masalarından) uzaklaştırmak için bilgi ifşa edebilmektedir (Mimic Technologies, 2013, s.4).

Yüzde yüz güvenlik korumasının mümkün olmadığını -özellikle bilgi güvenliği söz konusu olduğunda- bu alanın uzmanları belirtmektedir. Fakat hiçbir önlem de almadan, bana ya da benim işletmeme/kurumuma bir şey olmaz yanılgısıyla hareket edildiğinde, birikimlerin, yani tüm emeklerin bir anda uçup gitmesine sebebiyet verilebilir. Bununla da kalmayıp -üçüncü şahıslara karşı- yasal sorumluluklar da (işin hukuksal boyutları, veri güvenliği, kişisel verilerin korunması, müşteri bilgi gizliliği vb.) söz konusu olabilmektedir.

Suçlular SM taktiklerini kullanırlar çünkü insanların doğal eğilimlerinden istifade etmek isterler. Ayrıca, SM uygulamaları genel olarak yazılımları hacklemenin yollarını bulmaktan daha kolaydır. Örneğin, bir kişinin size şifresini vermesi için kandırılması o kişinin hacklenmesinden çok daha kolaydır. Güvenlik, kime ve neye güvenileceğini bilmekle ilgilidir. İletişim kurduğunuz kişinin ne zaman

gerçek kişi olup olmadığını bilmek de önemlidir. Aynı şey çevrimiçi etkileşimler ve web sitesi kullanımı için de geçerlidir.

Herhangi bir güvenlik uzmanına sorduğunuzda, güvenlik zincirindeki en zayıf bağlantının, değerli olduğunu düşündüğü bir kişiyi veya senaryoyu kabul eden insan faktörü olduğunu söyleyecektir. Kapılarınız ve pencerelerinizde ne kadar kilit ve sürgünün olduğu veya bekçi köpekleriniz, alarm sistemleriniz, projektörler, dikenli tellerle çevrili çit ve silahlı güvenlik personelinizin olması fark etmez; kapıda pizza servis elemanı olduğunu söyleyen bir kişiye güvenerseniz ve onun gerçekten pizzacı olup olmadığını kontrol etmeden içeri girmesine izin vererseniz, getireceği riske maruz kalabileceğinizi göz önüne almalısınız. Verizon'un yıllık Veri İhlali Araştırma Raporu'na göre, başarılı veri ihlallerinin %43'ünden SM saldırılarının sorumlu olduğu görülmektedir (www.webroot.com). Bu yüksek oran her zaman ve her şartta gerçekleşebilecek sabit bir oranı ifade etmese de, özellikle veri ve bilgi güvenliği konularında SM'nin ne denli zararlı olabileceğini ve dikkate alınması gereken güvenlik konularının başında yer aldığını açıkça ortaya koymaktadır.

1.1 Tanımı

SM, insanların saflığından yararlanma, kandırma, aldatma, manipüle etme, istenilen yöne çekme, yönlendirme, kafa karıştırma, algı yaratma, algı oyunları, ön yükleme, suyu bulandırma ve durulaştırma, tereddüt yaratma gibi birçok kavramı içinde barındırmaktadır. Karşınızdakinin, onun iyiliğine çalıştığınızı ve zararsız olduğunuza inanmasını sağlamak gibi birçok farklı yöntemi içinde barındırır. Daha çok, yönlendirme, bilgi ve/ya maddi çıkar elde etme amaçlı kullanılmaktadır. Bireylere, işletmelere ya da kitlelere karşı olumlu ya da olumsuz yönde uygulanabilmektedir.

SM, zorlama veya aldatmayla mağdurlardan bilgi veya kaynak edinmek olarak tanımlanabilir. Bir SM saldırısı sırasında saldırganlar genellikle ağları taramaz, kaba kuvvet kullanarak şifreleri kırmaz veya yazılım açıklarından yararlanmazlar. Aksine, sosyal mühendisler sosyal dünyada insanların güvenliğini ve/ya saflığını manipüle ederek çalışırlar (Raman, Baumes, Beets ve Ness, 2002 Akt: Clark, 2017, s. 6).

Mann (2008, s. 11)'e göre SM, insanları aldatarak manipüle etmek, dışarı bilgi vermelerini ya da (istenilen yönde) aksiyon almalarını sağlamak, Ahmed

(2013)’e göre ise, SM, bilinenin aksine teknolojik hackleme değil, insan zafiyetinden yararlanmadır. Sosyal mühendisler, potansiyel kurbanları için “Rebecca” ve “Jessica” isim terminolojilerini kullanırlar. Sosyal mühendislerin hedefinde daha çok resepsiyon ve banka gibi yerlerde ön büro çalışanları, sekreterler, servis elemanları vb. bulunur. Hadnagy (2017) ise, güvenlik meraklılarına SM’nin ne olduğunu sorduğunda aldığı cevapların şunlar olduğunu ve bu cevapların kendisini çok şaşırttığını söylemektedir; “SM bilgi almak için insanlara yalan söylemektir”, “SM iyi bir aktör olmaktır”, “SM nasıl bedavaya bir şeyler alınacağını bilmektir” (s. 27). Oysa SM, bir saldırganın bir kuruluştaki insan unsuruna saldırarak teknik kontrolleri atlamasını sağlayan bir metodolojidir (Major, 2009, s. 40). SM, bireyin, grup üyelerinden birisinin veya bir grubun belirli bilgilere erişim sağlamak veya belirli bir davranışı gerçekleştirmek için manipüle edildiği bir dizi yöntemdir (Şerban ve Şerban, 2014). SM, insanları çeşitli eylemlerde bulunma ya da gizli bilgileri açığa çıkarma konusunda manipüle etme sanatıdır. Terim, tipik olarak bilgi toplama, dolandırıcılık, kimlik hırsızlığı veya bilgisayar sistem erişimidir. Kişilerarası etkileşimi içeren SM saldırıları doğrudan iletişim (şahsen veya telefonla olduğu gibi) veya elektronik yollarla aracılık edilen etkileşimdir (ör. elektronik medya, e-posta ve internet) (Kumar, Chaudhary ve Kumar, 2015, s. 15). SM, birini, bilgiyi ifşa etmeye yönlendirmek veya bu bilgilerin yayınlanmasına neden olabilecek eylemleri gerçekleştirmek için tasarlanmış aldatıcı tekniklerin kasıtlı olarak uygulanmasıdır. SM etkileşimi sırasında mağdur, davranışlarının zararlı olduğunu bilmemektedir. Sosyal mühendis hedefini suçluluk içgüdülerinden değil, masum içgüdülerinden dolayı kullanır (manipüle eder). Saldırganlar, mağdurları faydalı bilgileri açığa vurmaya veya bir bağlantıya (linke) tıklamaları gibi bir eylemde bulunmalarını sağlamak adına kandırma gibi çeşitli yöntemler kullanırlar. Doğrudan sömürü/ihlal teknikleri, SM kapsamında değildir. Bir SM saldırısı hedefe yönelik veya fırsatçı olabilmektedir. Hedefli saldırılar tipik olarak belirli bir kişiye odaklanırken, fırsatçı saldırılar belirli bir pozisyonadaki herhangi bir kişiden (yardım masası gibi) bilgi toplamaya yöneliktir (Samani ve McFarland, 2015, s. 6).

SM insan psikolojisini anlamak, gerektiğinde manipüle etmek, hedefte yer alan kişinin hassas ve kritik bilgiler vermesini sağlamak üzere kullanılan planlı bir yoldur. Öte yandan, SM iyi bir yalancı olmakla alakalı değildir; SM, en kısa zaman

diliminde ve yüksek risk almadan, bir sisteme erişim sağlayabilmek adına insanları yönlendirmenin çeşitli yollarını keşfedebilmekle ilgilidir (Tosun, 2015, s. 7). SM, herhangi bir sisteme erişim için yazılım veya donanım aracılığıyla uygulanan savunma güvenlik kontrolleri katmanlarına erişimden ziyade, insan hatası veya zayıflığını kullanır. Nihai güvenlik duvarı insandır ve eğer o kişi kandırılırsa/geçilirse, saldırganın kontrolü ele alması için kapılar tamamen açıktır.

Tüm SM girişimlerinin sınıflandırılabilceği başlıca iki ana kategori bulunmaktadır. Bunlar bilgisayar veya teknoloji temelli aldatma ve insan temelli aldatmadır; bilgisayar veya teknoloji-temelli yaklaşım, kullanıcının “gerçek” bilgisayar sistemiyle etkileşime girdiğine inanmasını ve gizli bilgiler vermesini sağlamakla, insan temelli yaklaşım ise, mağdurun bilgisizliğinden ve yardımcı olma içgüdüğü ve sevmeye olan doğal insan eğiliminden yararlanılarak aldatma yoluyla yapılır (Gulati, 2003, s. 1). İnsan kaynaklı saldırılar; saldırgan ile değerli bilgilere sahip olan mağdur arasındaki etkileşimlerdir. Buna karşılık, teknoloji tabanlı saldırılar ise; açılır pencereler, e-posta ekleri ve web siteleri gibi bilgisayar programları kullanarak gizli bilgilere erişme girişimleridir (Jain, Tailang, Goswami, Dutta, Sankhla ve Kumar, 2016, s. 95).

SM tekniklerini kullanan kişinin yani sosyal mühendisin amacını Hadnagy (2017, s. 180) şu şekilde tanımlamaktadır; “Bir sosyal mühendisin amacı bilgi toplamak, erişmemesi gereken bir yere ya da bir şeye erişmek ya da hedefin yapmaması gereken bir hareketi yapmasını sağlamaktır”.

Birleşik Krallık Ulusal Sistemleri Koruma Merkezi’nin raporunda ifade edildiği üzere SM psikolojik ve güvenlik çerçevesi içerisinde çeşitli şekillerde tanımlanabilmektedir. Ana tanımı ise, insanları kullanarak bir güvenlik katmanını geçmektir. FBI’ın bir dönem en çok arananlar listesinde adı bulunan bilgisayar korsanlarından Kevin Mitnick ise SM’yi “İnsanların saflığını kullanarak kişileri etkilemek, ikna etmek ve manipüle ederek kritik bilgilerin ele geçirilmesi” şeklinde tanımlamaktadır. En basit şekliyle ifade etmek gerekirse, insanların güvenini kazanarak onlara aslında istemedikleri (istediğini sandıkları) şeyleri yaptırmak olarak tanımlanabilir (Barışkan, 2017, s. 3). SM, kişisel bilgilere ve korunan sistemlere erişmek için insan zayıflıklarını kullanma eylemidir. SM, hedefteki kişinin hesabına girmek için bilgisayar sistemlerini kırmak yerine bireyleri manipüle etmeye dayanır.

SM, bir hedefin manipölasyon edilmesidir; bir kişinin kimliğini çalmaya veya bir kredi kartı veya banka hesabını ele geçirmeye ek olarak, bir şirketin ticari sırlarına erişmek veya ulusal güvenlikten faydalanmak için kullanılabilir (www.investopedia.com). Birleşik Devletler Ulusal İstihbarat Yönetim Ofisi ve İç Güvenlik Departmanı, 2017 Kamu-Özel Analitik Değişim Programı, *Fidye Yazılım ve Sosyal Mühendisliğin Geleceği* başlıklı çalışmasında SM'yi, hedefin eylemlerini etkilemek için aldatma ve ikna etme yoluyla (hedefi) psikolojik olarak manipüle etmek maksadıyla insan etkileşiminin kullanılması olarak tanımlamaktadır.

SM, büyük ölçüde insan etkileşimine dayanan ve çoğu zaman sistemlere, ağlara veya fiziksel konumlara veya finansal bilgilere erişmek için, normal güvenlik prosedürlerini ve en iyi uygulama duvarlarını geçebilmek adına insanları manipüle etmeyi içeren bir saldırı vektörüdür (Rouse, 2018a). Tehdit aktörleri, gerçek kimliklerini ve amaçlarını gizlemek ve kendilerini güvenilir bir birey veya bilgi kaynağıymış gibi sunmak üzere SM tekniklerini kullanırlar. Amaçları, kişileri veya kurum çalışanlarını, belirli bilgilere ulaşmak, belirli alanlara erişmek vb. faaliyetler için manipüle etmek veya kandırmaktır. SM, yalnızca bilgisayar korsanlarının kullandığı bir yöntem olmamakla birlikte, onlar için de oldukça popüler bir taktiktir, çünkü kullanıcıların zayıf yönlerinden yararlanmak genellikle bir ağ veya yazılım açığını bulmaktan daha kolaydır ve daha az çaba sarf etmeyi gerektirir. Saldırganlar, genellikle bir sisteme veya ağa sızmak ve hassas verileri çalmak veya kötü amaçlı yazılımları dağıtmak için ilk adım olarak SM taktiklerini kullanmayı tercih etmektedir.

SM'yi dar anlamda da geniş anlamda da ele almak mümkündür. Ama öyle gözüküyor ki dar anlamda ele alınsa bile SM'yi göz ardı etmemek gerekiyor. Zira, yakın gelecekte günlük yaşam akışı içerisinde çokça yer alacak (güvenlik, siber dünya, robotik, yapay zekâ, bulanık mantık, endüstri 4.0 vb.) kavramlarla etkileşimi her an her yerde hissedilebilecektir. Geniş anlamda SM'nin nerelere kadar uzanabileceğini biraz daha iyi anlamak için Hadnagy'nin (2017, s. 28-30) şu ifadelerine bakmak yeterli olacaktır; SM, günlük hayatta, çocukların ebeveynlerinden isteklerini yerine getirmede ve boyun eğdirmede (bunun tam tersi de geçerlidir), öğretmenlerin öğrencileriyle etkileşim biçimlerinde (güdüleme, yönlendirme ve yöneltme), doktor, avukat ya da psikologların hasta/müşteri/danışanlarından bilgi

almada, yasaların uygulanmasında ve hatta flört ederken dahi kullanılabilir. Yani kısaca bebeklerden politikacılara kadar uzanan geniş bir yelpazede kullanılabilir. Öyle ki Victor Lustig, SM sayesinde bazı insanları, onların Eiffel Kulesini satma haklarının olduğuna ikna edebilmiştir.

SM iyi ve kötü yönde kullanılabilirle birlikte daha çok negatif yönüyle gündeme gelmektedir. Teknolojik sızma (hackleme) SM ile eş anlamlı değildir. Fakat teknolojik sızmaya öncülük ve aracılık edebilen girişimleri bu kavrama dâhil etmek mümkündür. SM saldırıları, daha çok bir kimsenin ya da (çıkar) gurubunun, başkalarını veya diğer gurupları kendi çıkarları doğrultusunda ikna ederek bir hedefe ulaşma çabasını (manipülasyonu) ifade etmektedir.

Sosyal mühendis, insani zayıflıklardan ve bu zayıflıkların hemen herkes için benzer olabileceğinden hareketle, insanların bazı davranış ve tutumlarında stereotip (basmakalıp) bir tutum sergileyebileceklerini bilir ve bundan yararlanır. Türk Dil Kurumu (2018)'na göre stereotip, “sosyal bir grubun içinde olan ve içinde bulunduğu grubu en iyi temsil eden özellikleri taşıyan, örnek gösterilebilecek kişi veya basmakalıp (düşünce)” şeklinde açıklanmaktadır. “Pek çok araştırma insanların bir malzemenin kalitesinden emin olmadıklarında stereotip ilkesine başvurdıklarını göstermektedir” (Olson, 1977 Akt: Cialdini, 2018, s. 25). Yani bazı durumlarda insanlar, diğer çoğunluk tercih ediyor diye, çok fazla sebep aramadan kestirme bir yol/davranış olarak, en çok tercih edilen mücevher taşı rengini, tatil beldesini, havayolunu, X markasını (*klik-pırr*¹ tutumuyla) tercih edebilmektedir. Otomatik karar vermenin (kontrollü düşünmenin tersi) (örneğin: pahalı ürünler iyidir/kalitelidir) sonuçları her zaman kazançlı olmamakla birlikte genelde doğru çalışır ve insanları daha çok düşünme, analiz etme ve zaman ayırma yükünden korur. Karar vermek için kestirme bir yoldur. Hadnagy (2017, s. 74)'e göre insanların bilgi ifşa etmelerine sebebiyet veren şu özellikleri stereotip için örnek verilebilir:

- Birçok insan kibar olmak ister, özellikle de yabancılara, tanımadıklarına karşı.
- Profesyoneller (ya da öyle olduğunu düşünenler) bilgili ve zeki görünmek isterler.

¹ **Klik-pırr** (otomatik): Otomatik bir itaat tepkisi, bir bilgiye mekanik olarak tepki verme.

- İnsan beğenilmeyi sever, eğer övülürseniz, genellikle daha fazla konuşur ve daha fazla şey ifşa edersiniz.
- İnsan, uzman ve tecrübeli olduğu alanlarda konuşmayı daha çok tercih eder.
- İnsanları başarıları hakkında konuşturmak çok kolaydır.
- İnsanların birçoğu, kendileriyle ilgileniyor gibi görünen insanlara karşı nazik davranır.

Çok basit ve sıradan olduğu düşünülen kısa konuşmalar veya ayaküstü sohbetlerde sosyal mühendisler yeterli bilgiyi vermiş olabilirsiniz! Bir çocuğun ebeveynlerine istediği şeyi yaptırma aracı olarak kullandığı “ağlama” da bir tür SM’dir. Politikacıların düzenli aralıklarla kamuoyu anketleri yaptırarak birçok konuda (daha çok mevcut durumla ilgili) güncel düşünceleri öğrenmesi ve bunları yorumlaması da bir SM’dir. Bir psikoloğun, *danışanından* bazı davranışlarını değiştirmesi için onu ikna edebilmek adına anlattığı bazı gerçek ya da kurmaca hikâyeleri de bu kategoriye sokmak mümkündür. Yine aynı şekilde, bir satıcının elinde olan bir malı müşterisine kolayca satabilmek için, elinde olmayan bir malı kötülemeye çalışması da bir tür SM’dir. Flört ettiğiniz kişiyle yapılan sıradan konuşmalar içerisine yerleştirilebilecek “bilgi havuzu tuzakları” sayesinde birçok bilgi kolayca elde edilebilir ve bunlar daha sonra niyetinize göre (iyi ya da kötü) kullanılabilir. Buradaki en önemli zafiyet; kişiyi yakinen tanıyarak olmak, ona güven duymak, zaten birçok şeyi paylaşıyor olmak, yaklaşma duygusu, karşı cinsin çekiciliği gibi insani özelliklerden kaynaklıdır. Bu tür davranışlar casusların da kullanmayı sıkça tercih ettikleri yöntemlerin başında gelmektedir. “Tüm dünyada casuslar tarafından kullanıldığı için birçok hükümet, çalışanlarını bilgi ifşa ettirmeye karşı eğitmekte ve uyarmaktadır” (Hadrnagy, 2017, s. 74). Elde edilen bilgileri şantaj olarak kullanmayı kısmen de olsa SM’nin dışında değerlendirmek doğru olacaktır. SM’yi sahtekârlıktan ayıran ince çizgi, birincisinde (iyi niyetle) olumlu yönlendirmeler de yapılabilirken ikincisinde yalnızca olumsuzluk ve aldatma söz konusudur.

SM’ye yönelik olarak yukarıda verilen çeşitli tanımlardan hareketle; yöntem/araç, hedef ve amaç sınıflandırması yapılarak oluşturulan ve aşağıda Tablo 1 ve Tablo 2’de ifade edilen veriler ışığında, SM’nin operasyonel (işlevsel) tanımını şu şekilde yapmayı uygun buluyoruz: “SM, insanların bilgisizliğinden, insani

zayıflıklarından ve zafiyetlerinden yararlanarak; aldatma, ikna, zorlama, güvenini kazanma, yönlendirme ve/ya teknik/teknolojik ataklar vasıtasıyla; kişisel, kurumsal, değerli ve kritik bilgiler elde ederek; maddi kazanç elde etme, güvenli alanlara erişme ve insanların istenilen yönde aksiyon almalarını sağlamaktır.”

Tablo 1. Sosyal Mühendislik Tanımlarının Yöntem/Hedef/Amaç Sınıflandırması-I

Kaynak	Yöntem / Araçlar	Hedef	Amaç
Raman, Baumes, Beets ve Ness, 2002 Akt: Clark, 2017, s. 6	Zorlama, aldatma, insanların güven ve sağlığından yararlanma	Herkes	Bilgi ve kaynak edinme
Mann, 2008, s.11	İnsanları aldatarak manipüle etmek	Herkes	Bilgi almak, istenilen yönde aksiyon göstermelerini sağlamak
Ahmed, 2013	İnsan zafiyetinden yararlanma	Resepsiyon ve banka gibi yerlerde ön büro çalışanları, sekreterler, servis elemanları	Bilgi elde etme ve yönlendirme
Major, 2009, s. 40	İnsan unsurlarına saldırmak	Kuruluşlardaki insanlar	Teknik kontrolleri atlamak
Şerban ve Şerban, 2014	Manipülasyon	Birey, grup ya da grup üyelerinden biri	Bilgiye ulaşma ya da belirli davranışların gerçekleştirilmesini sağlamak
Kumar, Chaudhary ve Kumar, 2015, s. 15	Manipülasyon	Kişiler arası ya da gruplar	Bilgi toplama, dolandırıcılık, kimlik hırsızlığı, bilgisayar sistemlerine erişim, gizli bilgileri açığa çıkarma ya da belirli davranışların gerçekleştirilmesini sağlamak
Samani ve McFarland, 2015, s. 6	Yönlendirme, aldatıcı teknikler kullanma	Kişilere ya da belirli pozisyonundaki kişilere	Bilgi ifşası veya bilgi elde etmek için yönlendirme
Tosun, 2015, s. 7	İnsan psikolojisi ve manipülasyon	İnsanlar	Hassas ve kritik bilgiler elde etmek. Güvenli sistemlere erişmek
Gulati, 2003, s. 1	Bilgisizlik, insanların yardım iç güdüsüyle hareket etmesi ve sevilme içgüdüğü	İnsanlar	Gizli bilgilere ve sistemlere erişmek
Jain, Tailang, Goswami, Dutta, Sankhla, Kumar, 2016, s. 95	İnsan zafiyeti ve teknik ataklar	Kişiler	Değerli bilgilere erişmek
Birleşik Krallık Ulusal Sistemleri Koruma Merkezi	Psikoloji ve teknoloji	İnsanlar	Kurum güvenliğini kırmak
Mitnick ve Simon, 2001	İnsanların sağlığı, ikna etme ve manipülasyon	İnsanlar	Kritik bilgilerin ele geçirilmesi
Barışkan, 2017, s. 3	Güven kazanmak	İnsanlar	İstemedikleri şeyleri yaptırmak
Investopedia.com	İnsan zayıflıkları, manipülasyon	İnsanlar	Kişisel bilgilere ve korunan sistemlere ulaşmak. Kimlik, kredi kartı ya da banka bilgilerine ulaşmak
Birleşik Devletler Ulusal İstihbarat Yönetim Ofisi ve İç Güvenlik Departmanı	Aldatma ve ikna	İnsanlar, kurumlar	Hedefin eylemlerini etkilemek, psikolojik manipülasyon
Rouse, 2018	Manipülasyon	İnsanlar	Sistemlere, ağlara, fiziksel konumlara ve finansal bilgilere ulaşmak

Tablo 2. Sosyal Mühendislik Tanımlarının Yöntem/Hedef/Amaç Sınıflandırması-II

Yöntem / Araçlar	Hedef	Amaç
Aldatma	Bireyler	Bilgi edinme/toplama
İkna	Grup üyeleri	Gizli bilgilere erişme
Zorlama	Grubun tamamı	Değerli bilgilere erişme
Manipülasyon	İşletmeler	Kritik bilgilere erişme
Yönlendirme	Kurumlar	Kişisel bilgilere erişme
Güven kazanma	Toplumlar	Kaynak edinme
Teknik ataklar	Devletler	Finansal bilgilere erişme
Teknoloji		Dolandırıcılık
Zafiyetler		Kimlik hırsızlığı
Bilgisizlik		Güvenli sistemlere/alanlara erişme
İnsani unsurlar		Teknik kontrolleri geçme
İnsan psikolojisi		Sistemlere erişim
İnsanlık iç güdüsü		Fiziki alanlara erişme
Saflıktan yararlanma		İstenilen yönde aksiyon aldırma
Güvenden yararlanma		Eylemleri etkileme
Zafiyetten yararlanma		Psikolojik manipülasyon
İnsan zayıflıkları		

Bünyesinde barındırdığı birçok SM uzmanı ile tanınan social-engineer.org sitesi ise SM için şunları ifade etmektedir: “SM, bilim, psikoloji ve sanatın bir karışımıdır. İlginç ve karmaşık oluşunun yanı sıra aynı zamanda çok da basittir. Birisini, ilgi ya da ilgi alanı dışındaki bir yöne doğru etkileme işidir. SM, ebeveynler, terapistler, çocuklar, eşler ve başkalarıyla nasıl iletişim kurulabileceğini de kapsadığından onun her zaman olumsuz bir şey olmadığını düşünüyor ve bu yüzden onu daha geniş ve genel ifadelerle tanımlamayı uygun buluyoruz. Yine de, işin daha çok kötü yanıyla ve bundan (sizi ve şirketinizi veriden, bilgiden, paradan ve daha fazlasından ayırmak için genellikle kötü niyetli dolandırıcı ve sosyal mühendisler’den) sizi nasıl koruyacağımızla ilgileniyoruz”. Aynı internet sitesi SM’nin ne olduğuna ve nasıl kullanıldığına dair Tablo 3’de yer alan şu özet bilgileri de (başlık olarak) paylaşmakta ve ardından, ancak eğitim ve bilgi yoluyla korunulabileceğini ifade etmektedir.

Tablo 3. Sosyal Mühendislik Kısaca Nedir, Nasıl Kullanılmaktadır ve Nasıl Korunulur?

Sosyal Mühendislik Nedir?	Nasıl ya da Nerede Kullanılır?	Kendinizi Nasıl Korursunuz?
- Etki, ikna (<i>Influence</i>) - Yönlendirme (<i>Manupulation</i>) - İfşa ettirme (<i>Elicitation</i>) - Bilgi toplama (<i>Info gathering</i>) - Psikoloji (<i>Psychology</i>) - Bilim (<i>Science</i>) - Profil çıkartma (<i>Profiling</i>) - İletişim (<i>Communication</i>) - Modelleme (<i>Modeling</i>) - Yüz ifadesi: jest ve mimik (<i>Facial expressions</i>) - Vücut dili (<i>Body language</i>) - Sanat (<i>Art</i>) - Yanlış yönlendirme (<i>Misdirection</i>) - Bahane üretme (<i>Pretexting</i>) - Duygusal sömürü (<i>Emotional hijacking</i>) - Raporlama (<i>Rapport</i>)	- Aileniz, patronunuz, eşiniz ve arkadaşlarınızla iletişim kurarken (<i>Communication with your family, boss, spouse and friends</i>) - Şirket ihlallerinde (<i>Breaches companies</i>) - Veri hırsızlığında (<i>Stealing data</i>) - Siber suçlarda (<i>Cyber crime</i>) - Siber savaşlarda (<i>Cyber warfare</i>)	Eğitim (<i>Education</i>)

Kaynak: <https://www.social-engineer.org/about/> 'dan uyarlanmıştır, Erişim: 23.11.2018

SM büyük ölçüde psikolojiye dayanmaktadır. Sosyal mühendislerin insanları harekete geçmeye ikna etmelerine yardım eden, insanların duyarlı olduğu, çeşitli teşvik ve motivasyon türleri vardır. Örneğin, Dr. Robert Cialdini, *Etkileme: İknanın Psikolojisi* (Influence: The Psychology of Persuasion) adlı kitabında temel altı motive edici güçten bahsetmektedir (Shackleford, 2018):

- Karşılık verme/mukabele (*Reciprocation*): Size yapılan bir şeyler karşılığında, birine borçlu hissetmek.
- Sosyal kanıt (*Social proof*): Nasıl davranılması gerektiği konusunda diğerlerine bakmak/izlemek/kopyalamak.
- Bağlılık/Tutarlılık (*Commitment/Consistency*): Davranış kalıplarını geliştirmek ve alışkanlıklarından uzak tutmak.
- Beğenme (*Liking*): Sevdiğiniz biri tarafından ikna edilmek için “uyum sağlamak” istemek.
- Otorite (*Authority*): Otorite (yetkili) olarak kabul edilen makamlardan gelen talepleri kabul etme.
- Kıtlık/azlık (*Scarcity*): Bir şey çok sınırlı ve kaliteliyse, daha yüksek motivasyon hissi için onu takip etme/izleme/peşine düşme.

SM yakın gelecekte birçok yeni alanla da etkileşim içerisinde olacağından, her geçen gün SM'nin yeni tanımlarıyla karşılaşmak mümkün gözükmektedir.

1.2 Tarihi Süreç

SM'de kullanılan ilk yöntemlerin neler olduğu, kim ya da kimler tarafından kullanıldığı veya tarihi sürecin ne kadar geriye gittiği tam olarak bilinmemekle birlikte, MÖ 500'lerde yaşamış ünlü Çinli komutan, filozof ve askeri bilge olarak kabul edilen, savaş ve strateji uzmanı Sun Tzu'ya, belki daha da geriye götürmek mümkündür. SM saldırısı için bilinen daha eski bir örnek ise (MÖ 1184), Yunanlıların, korunaklı Truva (günümüzde Çanakkale şehri içerisinde yer almakta) şehrine girebilmeleri ve şehri içeriden işgal edebilmeleri için Truva Halkına, onlarda merak uyandırması için sunulan dev bir tahta at (Yunanlılar tarafından tahta bir at Truva şehri kale kapısı önüne bırakılır. Hediye olduğu düşünülen devasa tahta at Truvalılarca kale içerisine alınır. Atın gövdesine saklanan Yunan askerleri, gece yarısında, Truva askerleri uykuya daldıktan sonra, at içerisinden çıkarak kalenin

kapılarını dışarıda bekleyen Yunan askerlerine içeriden açarak şehre girmelerini ve şehri yağmalayarak teslim almalarını sağlar) sayesinde kazanılan Truva Savaşıdır.

Şerban ve Şerban (2014, s. 6)'a göre SM, tüm zamanların başından beri vardı. İlk iki kişinin (Adem ve Havva) "günaha düşmesi", yılan'ın ikna etme gücünü kullanmadan mümkün olamazdı. III. Amenhotep, Mısır'ın belki de en zengin dönemi boyunca, askeri güce ihtiyaç duymadan bugünün Suriye ve Filistin'ini güçlü kılmayı ve korumayı bir diplomat olarak edindiği becerilerle başarması da diğer bir örnektir. Daha yakın tarihli SM girişimleri için ise Rouse (2018a) şu bilgileri aktarmaktadır;

Frank Abagnale, SM tekniklerinde önde gelen uzmanlardan biri olarak kabul edilir. 1960'larda, bir havayolu pilotu, bir doktor ve bir avukat da dâhil olmak üzere en az sekiz kişiyi taklit etmek için çeşitli kılıklara girer. Abagnale, bu süre zarfında bir çek sahtekârıydı. Hapis sürecinden sonra kendi danışmanlık şirketini kurarak FBI için mali güvenlik danışmanı oldu. Yaşadığı deneyimleri anlattığı, en çok satanlar (best-seller) kitabı *Catch Me If You Can* (Yapabilirsen Yakala Beni) ve Oscar ödüllü yönetmen Steven Spielberg'in film uyarlaması ile ünlendi.

Başarılı bir SM saldırısına daha yakın bir örnek ise, güvenlik şirketi RSA'da 2011 yılında gerçekleştirilen veri ihlaliydi: Bu süreçte, bir saldırgan iki gün boyunca iki farklı kimlik avı e-postasını RSA çalışanlarının küçük bir gurubuna gönderir, gönderilen bu e-postalar "2011 İşe Alım Planı" konu satırına sahipti ve bir Excel belgesi eki içermektedir. Bu ekli dosya, Adobe Flash'ın arka planında çalışan ve "arka kapı" diye bilinen bir güvenlik açığı yaratacak kötü amaçlı bir kod içermektedir. Hangi bilgilerin tamamen çalındığı henüz netleşmemiş olsa da, RSA'nın SecureID adındaki iki faktörlü kimlik doğrulama (2FA) sistemi bu saldırıdan etkilenmişti ve şirket bu saldırıdan kurtulmak için yaklaşık 66 milyon dolar harcadı.

2013'te Suriye Elektronik Ordusu, kötü amaçlı bir bağlantı linki içeren kimlik avı e-postası aracılığıyla Associated Press'in Twitter hesabına erişti. E-posta, Associated Press'in kendi çalışanlarından birinden geliyormuş gibi yollandı. Saldırganlar, daha sonra Associated Press'in resmi hesabından sahte bir haber uydurarak bunu tweetlediler (yayınladılar). Haberde, Beyaz Saray'da iki patlamanın gerçekleştiğini ve ardından Başkan Barack Obama'nın yaralandığını duyurdular. Bu haber büyük bir reaksiyona yol açtı ve beş dakika gibi kısa bir süre içerisinde hisse senedi piyasasını 150 puan düşürdü.

2013 yılında gerçekleştirilen diğer bir kimlik avı saldırısı ise Target'a yönelikti ve bu büyük çaplı veri ihlallerine yol açan bir saldırıydı. Bir kimlik avı e-postası, Target'ın iş ortağı olan HVAC'a (ısıtma, havalandırma ve klima) gönderildi. E-posta, saldırganların, Target'ın satış noktası sistemlerine (POS) sızmalarını sağlayan Citadel Trojan yazılımını içeriyordu ve bu sayede 40 milyon müşterinin kredi ve banka kart bilgileri ele geçirildi. Aynı yıl, ABD Çalışma Dairesi bir water-holing (subaşı) saldırısı ile karşı karşıya kaldı ve internet siteleri bundan etkilendi. Internet Explorer'ın bir güvenlik açığından kaynaklanan ve uzaktan erişime izin veren kötü amaçlı bir yazılım bulaşmıştı.

Hacker'lar, 2015 yılında CIA'in direktörü John Brennan'ın kişisel AOL e-posta hesabına erişim sağladılar. Bilgisayar korsanlarından biri, medya kuruluşlarına, Verizon teknisyenlerinden biriymiş gibi davranarak sosyal mühendislik tekniklerini nasıl kullandığını ve Brennan'ın hesabı hakkında bilgileri nasıl elde ettiklerini açıkladı. Bilgisayar korsanları Brennan'ın Verizon hesap bilgilerini aldıktan sonra, AOL ile temasa geçerek Brennan'ın e-posta hesabının güvenlik sorularını doğru bir şekilde cevaplayarak e-posta hesabına erişebilmişlerdi.

1.3 Sosyal Mühendislikle Etkileşimli Kavramlar

SM ile iç içe geçmiş (transitif) ve etkileşimli (interaktif) birçok konu ve kavramdan söz etmek mümkündür. Bunlar içerisinde öne çıkan ve uygulamalarda yoğun olarak karşılaşılanlardan bazılarını açıklamamanın, konuyu birçok boyutuyla görebilmek açısından faydalı olacağı, zira SM'nin kapsadığı alanın genişliği ve diğer alanlarla kesişme noktalarının daha belirgin olarak anlaşılabilmesi açısından önemlidir.

SM tekniklerinin başarısı, sosyal mühendislerin hedeflerindeki kişileri belirli etkinliklere yönleltebilme veya onlardan özel bilgileri alabilme kabiliyetine bağlıdır. Günümüzde SM, kişiler ya da kuruluşlar açısından, karşı karşıya kaldıkları en büyük güvenlik tehditlerinden biri olarak bilinmektedir. SM, düşünülenin aksine büyük oranda teknik bir saldırı olmadığı ya da sistemlerin teknik istismarını gerektirmediği için bilinen siber saldırılarından farklıdır (Barışkan, 2017, s. 1).

İnsanlar insanları belirli bir şekilde davranmaya ikna etmek ister ve bunu yapmak için belirli sözcükleri, sesleri ve cümle kalıplarını akıllıca seçerek kullanırlar. Politikacılar vatandaşlardan oy istemek için konuşur, reklamcılar insanları bir ürünü ya da hizmeti almaya yönlendirirler. Kandırılmamak için, insanların amacının ne olduğunu anlamaya çalışmak gerekir. Bir başka deyişle *retoriği* anlamak gerekir. Retorik, dilin insanları ikna etmek veya etkilemek için kullanılmasıdır. Reklamlar insanları ikna etmeye çalışırken retorik özelliklerini çokça kullanır. Ürünü ya da hizmeti gerçekten cazip gösterecek sözcükler seçilir: Yeni, harika, değerli, lezzetli, güzel, özel, ekstra, çıtır çıtır, güvenli vb. (Crystal, 2018, s. 292). Sosyal mühendisler de sıkça retorik'i kullanırlar ve hedeflerindeki kişilerden sıkça şu cümleyi duymak isterler; “Birini ikna etmeyi biliyorsunuz...”

SM doğrudan kişiyi (kullanıcıyı, çalışanı, müşteriyi, yöneticiyi) ya da kurumu, işletmeyi, organizasyonu hedef alabilir. SM'nin uygulanmasında temel aracı faktör insandır. Buradan hareketle diyebiliriz ki, SM; sosyoloji, psikoloji, kültür,

çevre, dil, din vb. alanların belirli yönlerini kullanarak “insana erişim” sağlama odaklıdır. Aşağı kısımda çeşitli başlıklar altında (bu başlıklara elbette başka başlıklar ilave edilebilir) SM ile ilişkilendirilen kavramlara yer verilmiştir. SM’nin sanılandan çok daha geniş bir yelpazede varlık gösterdiğinin ve birçok alandan beslendiğinin anlaşılabilmesi açısından bu kavramların açıklanmasında fayda bulunmaktadır.

1.3.1 Algı ve Gerçeklik Kavramı

Algının sözlük anlamı, nesnel dünyayı duyular yoluyla öznel bilince aktarma olarak belirtilmektedir (Özer, 2012, s. 148). Türk Dil Kurumu (2019)’na göre ise algı, “bir şeye dikkati yönelterek o şeyin bilincine varma, idrak” olarak ifade edilmektedir.

Dünyayı algılama biçimi, yaşanan olaylara ilişkin olarak beş duyu organıyla bu olayların nasıl algılandığı ve yorumlandığı ile ilgilidir. Fakat çeşitli nedenlerle bu duyu organları bazen etkin bir şekilde kullanılamamaktadır. Bunun ana nedeni, algılama sürecini başkalarının düşünceleri, yaklaşımları ya da kişisel tecrübeleri veya kültür gibi çeşitli farklılıkların etkilemesidir. Bu durumda zahiri bir dünya, “gerçek” dünya olarak tanımlanabilir. Bu manada, dünyada var olan renkler, görüntüler, sesler, söylemler, insanlar ve yaşamlar, algı çemberine paralel daraltılarak, eğilip bükülür, ideolojilere uygun kalıplara sokulur ve algı sonucu ortaya çıkan gerçek ile nesnel gerçek arasındaki farkın ayırt edilebilmesi oldukça zorlaşır; zihinlerde oluşan algıya dayalı bu gerçek esas gerçekmiş gibi değerlendirilir (Apak, 2018).

Algı, çevreden alınan duyu uyarılarının zihinde anlamlı deneyime çevrilme sürecidir. Algı, basit öğelerden çağrışım yoluyla oluşturulan karmaşık bir deneyim sürecidir. Öğrenme ve bilişe açılan yoldur. Algı, çevredeki nesneleri, olayları, ilişkileri duyu organları yoluyla anlamak, anlamlandırmak sürecidir (Ertan, 2016, s. 2). Aynı olgu için algı kişiye göre farklılık gösterebilmektedir çünkü dışsal etmenler ve veriler kişinin kendi bakış açısına (bilgi düzeyi, duyguları, yaşama dair deneyimleri) ve çerçevesine göre yorumlanıp değerlendirilmektedir.

Her birimiz gerçekliği biraz farklı görürüz. Örneğin Dr. Eagleman şuna işaret ediyor: “Kadınların en az %15’i, onlara fazladan (dördüncü) bir fotoreseptör veren bir mutasyonla doğar, bu da üç farklı tip fotoreseptör bulunduran ve çoğunluğu oluşturan insanlara aynı gibi görünen iki farklı rengi birbirinden ayırt edebilmelerini sağlar” (Kaku, 2017, s. 47). Kişiler dış çevreden gelen her türlü veri, enformasyon ve

bilgiyi kendi geçmiş ve deneyimlerinin ışığında ve mümkün olduğunca kendi yargı çerçevesinde değerlendirerek bir çıktı elde etmekte ve kararlarını bu doğrultuda vermektedir. Algı yönetimi, bu süreç içerisinde daha çok dışsal etkenler (external factors) ile ilgilidir. Ağırlıklı olarak veri, enformasyon ve bilgi üçgenini içeren bu dışsal çerçeve dilsel kavrayış ile kişinin zihninde oluşan resme, yani algıya dönüşmektedir, bu algı bir anlamda subjektif değerleri içermektedir. Gerçeklik kavramı ise kişiye göre değişmeyen nesnel çıkarımlardır. Bu anlamda gerçeklik kavramı reel durum (un algılanması) olarak adlandırılabilir.

Kitle iletişim ve sosyal medya araçlarının algılama sürecine etki etmesi sonucunda, gerçeklik algısının değişebildiği görülmektedir. Bu araçlarda yer alan haberlerin başlıca kaynağı olma gücünü elinde bulunduran iktidarlar (bazen kişi ya da kurumlar) propaganda ve algı yönetimi çalışmalarıyla mesajlarını hedef kitleye iletebilmekte, amaca yönelik olarak hedef kitlenin algısını da etkileyebilmektedir (Apak, 2018). Teorik açıdan algılama süreci aşamaları ise; duyum süreci, simge süreci ve duygu süreci aşamalarından oluşmaktadır. Duyum süreci, kişilerin dış dünyadaki her türlü uyarana verdiği bilinçli tepkilerden; simge süreci, kişilerin daha önce anlamlandırdıkları nesneleri daha kolay ve kısa sürede algılamalarından; duygu süreci ise, kişinin geçmiş dönemdeki deneyimlerinin yanı sıra algılama sırasında duygusal kararlarının etkilerinden oluşmaktadır (Özarslan, 2014, s. 7).

Kişilerin algılamaları, tutum ve davranışlarını doğrudan etkilemekte, değiştirmekte ve biçimlendirmektedir. Sosyal yaşamlarında kişiler, isteyerek ya da istemeyerek, bilinçli veya bilinçsiz şekilde birçok etmenden etkilenerek oluşturdukları bu algılamalara göre tutum ve davranış geliştirmektedirler. Bununla birlikte, algılama süreci geçmiş deneyimlerin etkisiyle otomatikleşmiş (klik-pırr) olduğundan kişiler özel durumlar haricinde algılama sırasında çok fazla zaman harcamaz ve algıladıkları konu üzerine detaylı düşünme gereği hissetmezler, çünkü algılama içsel bir durumdur (Özarslan, 2014, s. 13-14).

1.3.2 Algı Yönetimi

Algı yönetimi aslında bilinçli veya bilinçsiz şekilde günlük yaşantımızda dahi sıkça başvurulan bir husus olmakla birlikte, bilinçli ve sistemli şekliyle ilk defa Amerika Birleşik Devletleri Savunma Bakanlığı tarafından tanımlanmıştır. Buna göre algı yönetimi, "Kitlelerin duygu, düşünce, amaç, mantık, istihbarat sistemleri ve

liderlerini etkileyerek seçili bilgilerin yayılması ve/veya durdurulması; bunun sonucunda hedef davranış ve düşüncelerinin hedefleyenin istekleri doğrultusunda yönlendirilmesidir. Diğer deyişle algı yönetimi gerçekler, yansıtma, yanıltma ve psikolojik operasyonların bir bütünüdür” (Ersaydı, 2011, Akt. Özarslan, 2014, s. 30-31). Kişinin, yüklenen algıyı kendi gerçeği olarak alması tamamen “algı gerçektir” kavramıyla ilgili bir tutum geliştirmedir ve algıya dair üzerinde en çok tartışılan kısım ise tam da burasıdır. Algı yönetimi bu boşluktan yararlanarak ortaya koyduğu söylemi ve çıkarsamaları destekleyecek (gerçek ya da sözde) kanıtlar ile pekiştirme yoluyla stratejisini daha da güçlendirmektedir.

Tüketici davranışlarını etkileyen unsurlardan biri olan algı, yönetilebilen bir kavram olarak günümüz iş dünyasında ele alınmaktadır. Algı yönetimi ile istenilen davranışlar zor kullanılmadan tüketici üzerinde (çeşitli yöntem ve teknikler kullanılarak) oluşturulmaya çalışılır. Bu şekliyle çok ciddi bir güç olan algı yönetimi kavramı *yumuşak güç* tanımlaması ile ifade edilmektedir (Ertan, 2016). Algı yönetimi, hedef kitleyi (hedefte olan grubu) istenilen yönde etkileyebilmek için icra edilen her türlü faaliyeti kapsamaktadır. Bunların içerisine çeşitli stratejiler, politikalar, manipülasyonlar gibi birçok alan girmektedir. Kişiler, askerler, ordular, devletler, hükümetler gibi birçok uygulayıcısı bulunabilmektedir. Hedef, yalnızca bir kişi, bir grup ya da bir ülke olabilmektedir. Örgütlü algı yönetimi ise büyük gruplar (bunlar çıkar grupları olabileceği gibi politik amaçlara hizmet eden gruplar vb. de olabilir) tarafından çeşitli araçlar (basın, sosyal medya, eğitim, din, mevki vb.) kullanılarak yapılmakta, daha uzun bir süreç ve geniş bir etki alanı içerebilmektedir.

İnsanlık tarihinin her döneminde çeşitli şekillerde uygulanan algı yönetimi uygulamaları, teknolojinin gelişmesiyle birlikte kitlelerin oldukça rağbet gösterdiği sosyal medya alanına kaymıştır (Özarslan, 2014, s. 3) bu şekilde sosyal medya araçlarının gücünü de yanına alan algı yönetimi eskisine nazaran daha kısa zamanda ve daha geniş kitlelere ışık hızıyla ulaşabilmektedir. Kötü niyetli kişi veya yönetimlerin elinde yıkıcı etkiler yaratabilen algı yönetimi, SM süreçlerinde olduğu gibi dikkatle izlenmesi gereken (saldırgan) bir yapıya sahiptir. *Doğrulayıcı kaynakların* ya da kaynak doğrulayıcılarının önemi burada da karşımıza çıkmaktadır.

Algı yönetimine maruz kalan kitleler, sergiledikleri davranışların kendi kararları olduğuna ne kadar inanırlarsa ve neye maruz kaldıklarının farkında

olmazlarsa algı yönetimi o kadar başarılı olmaktadır. Bu sebeple algı yönetimi uygulamaları, uygulayıcı için çok sabır ve dikkatle uygulanması gereken faaliyetlerdir. Algı yönetimi uygulamaları açıktan yapılmadığı için, kaynağı ve amacı ilk etapta anlaşılamamaktadır (Özarslan, 2014, s. 2). Bu şekliyle yapboz'un parçaları (her ne kadar bütünün alt parçaları olsa da) "büyük resim" in içerisinde gizlenmekte ve zamanından önce onu ele vermemektedir ve genellikle büyük resim kitlelerce algılanmaya/anlaşılmaya başladığında ise süreç muhtemelen çoktan tamamlanmıştır. İster yapıcı ister yıkıcı amaçlar doğrultusunda kullanılsın, algı yönetiminin çeşitli aşamaları mevcuttur. Özer (2012, s. 177) algı yönetimini uygulama bakımından toplamda on bir temel kural altında toplandığını ifade etmektedir. Bunlar; hedef kitlenin değerleriyle uyum, hedef kitlenin kültürüyle uyum, beklentilerin üzerinde yaklaşım sergilemek, yalın olmak, sonuca odaklanmak, ölçümlemek, gerçeklere dayanmak, tekrar etmek, farklılaşmak, görselliği doğru yönetmek, düşüncelerden çok duygulara hitap etmek.

Medya ve iletişim araçlarının, bilginin manipüle edilmesi, şekillendirilmesi, çarpıtılması ve belli amaçlar için ön plana çıkarılması olarak tarif edilebilecek algı yönetimi günümüzde reklam sektöründen siyasete kadar her alanda kullanılmaktadır. Algı yönetimi *bilgi alanının* insan boyutunu hedef alarak gelecek politikalar ve anlaşmazlıklar için şekillendirilmesidir. Böylece algı yönetimi, savaş, anlaşmazlıklar, terör ve yumuşak politikalar çerçevesinde, süreç öncesinde, süreç sırasında ve süreç sonrasında kullanılan bir mekanizma haline dönüşmektedir (Ertan, 2016, s. 7). Tıpkı SM ataklarının öncelikli hedefinde (zayıf halka olan) insan unsurunun bulunması gibi, algı yönetimi ve SM'nin ortak hedefi de insan ve insan algısıdır.

1.3.3 Sosyal Algı

Sosyal algı kendimizin ve diğer insanların davranışlarını nasıl algıladığımıza dair bir bilişsel süreçtir. Sosyal algı temel algı ilkelerine bağlı olarak işlemektedir. Önceden sahip olduğumuz bilgiler sadece yeni gelen uyarıcıyı yorumlamamız için temel teşkil etmekle kalmaz, aynı zamanda hangi bilgiyi seçeceğimize, hangisine dikkat edeceğimize ve bilgiyi nasıl organize edeceğimize de rehberlik ederler. Sosyal algı, nesne algısından çeşitli açılardan farklılaşmaktadır. Zira bir kişiyi (bazen olay ve olguları da) nasıl algıladığımız ve onunla nasıl bir etkileşime girdiğimiz, kısmen onun bizi nasıl algıladığı ve bizimle nasıl bir etkileşime girdiğine de bağlıdır

(Yıldırım, 2018). Sosyal algı, yalnızca algılanan tarafından oluşturulabilecek bir durum değildir ve algılayanın beklenti, motivasyon, ihtiyaç, beğeni, deneyimleri ile diğerlerinin aktardıklarından etkilenmektedir (Özarslan, 2014, s. 19). Nesneler ile kişilerin algılanmasında ilişki ve etki bakımından farklılıklar bulunmaktadır. Bu sebeple kişilerin algılanmasının söz konusu olduğu sosyal algı, nesne algılamalarına göre daha karmaşık bir süreci de beraberinde getirmektedir. Çünkü nesnelerin hareket ve durum değişiklikleri hakkında mantıksal çıkarımları yapmak ve çözüm yolları bulmak daha kolay ve anlaşılabilirken, insan davranışları ve bunlardan meydana gelen olay ve durumların anlaşılması biraz daha karmaşık ve çok fazla değişkenden etkilenebilen bir süreçtir (Güney, 2012, s. 118, Akt. Özarslan, 2014, s. 19).

Kötü kokuğumuzu öğrenene kadar ne gargaraya ne de deodoranta ihtiyacımız bulunuyordu, ta ki çekici ve güvenli olma isteğimiz üzerinden bizleri etkileyen reklam ajansları kendi doğal kokumuzun çevremize rahatsızlık verdiğine dair bizi ikna edene kadar. Bugün, kendimiz gibi kokmamamız gerektiği artık bir gerçeğe dönüşmüş bulunmaktadır ve şimdi her gün iyi kokmak, güzel görünmek ve bu sayede de iyi hissetmekle ilgili mesaj bombardımanına tutuluyoruz, savaştan farksız bir şey bu (Frey, 2016, s. 53).

Yazılı malzeme piyasasının önümüzdeki yıllarda gittikçe küçüleceği, kitle tüketim piyasalarının onlarca *uzun kuyruk*² piyasa (long tail marketing) parçalarına ayrılması, Google-AdWords-AdSense ve Analytics gibi karmaşık araçlar sayesinde çevrimiçi mecraların popülerleştirilmesi, YouTube’de en çok izlenen videoların 30 saniye ve daha kısa süren videolar olması, dikkat süresinin azalmasından dolayı kısa süreler içerisinde mesajlar taşıyacak grafik, video ve animasyonların bir araya getirilmesi (ve gösterilme frekansının arttırılması) (Frey, 2016, s. 58-72), hızlı eğitim araçlarının kullanılmaya başlanması yakın gelecekte sosyal algının nasıl yaratılacağı ve şekillendirileceği konusunda bizlere önemli ipuçları vermektedir. Ayrı bir başlığın konusu olan “sadeleştirme” ve “hız” konularının da sosyal algı yönetiminde çokça tercih edilecek yöntem ve parametrelerden olacağı kaçınılmaz gözükmemektedir. Ne anlatmak (aktarmak) istiyorsanız en fazla “10 saniyeniz var” mottosu geleceğin

² **Uzun Kuyruk** (Long Tail): Çok çeşitli ürünlerin toplam satışının tercih edilen (popüler) bir ürünün satışından daha fazla olmasını ifade etmektedir ve ilk olarak Chris Anderson tarafından Wired Dergisine yazılan makalede Netflix ve Amazon.com benzeri iş ve ekonomik modelleri tarif etmek için kullanılmıştır.

iletişim ve algı sürecini yönetmedeki ortalama zaman süresini tanımlamaya esas oluşturmaktadır. Bu sayede, hızla *kritik kitle*³ noktasına erişmek mümkün olabilecektir.

İnsanların davranış şekillerini bilmek onların gelecekteki davranışlarını şekillendirmek için önemli bir bilgi kaynağıdır. SM çatısı altında sosyal algının yaratılabilmesi açısından bu tür bilgi araçlarına ihtiyaç vardır. Örneğin yukarıdaki paragrafta bahsedilen “hız” konusunda Frey (2016, s. 74-75)’in vermiş olduğu şu bilgiler (geleceği mevcut bilgilerden hareketle şekillendirme ve istenirse bu doğrultuda sosyal algı yaratabilme açısından) oldukça önemlidir; National Eating Trend’e göre öğle yemeklerinin %34’ü ayakta yeniliyor ve bu durum 112 milyar dolarlık bir ABD fast-food sektörüyle karşılanan bir trenddir. İnsanların %66’sı aynı zamanda hem internette geziniyor, hem televizyon izliyor. Reuters tarafından yapılan bir araştırmaya göre insanların %49’u enformasyon akışını takip edemediklerini düşünüyor. Tüm bu bilgiler ışığında zaman baskısını anlamak, gelecekteki tüketici davranışlarını anlamak/yorumlamak ve yönlendirmek açısından önemli verilerdir.

1.3.4 Stratejik Algı Yönetimi

Stratejik algı yönetimi bugüne kadar politika, askeri, diplomasi, soğuk-sıcak savaş dönemleri ve diğer birçok alanda kullanılmıştır. İşletmecilik açısından ise son zamanlarda yeni kalıplara bürünen stratejik algı yönetimi daha çok müşteri odaklı ve bireysel hedeflere yönelik yapılmaktadır. Yapılan çeşitli araştırmalar göstermektedir ki, kaybedilen bir müşterinin yerine yeni bir müşteri kazanmak (eldeki müşteriye tutma maliyetine göre) yedi kat civarında daha fazla bir maliyete sebep olmaktadır. Bu nedenle stratejik algı yönetimi müşteri kazanımı öncesi, müşteri devamlılığı sürecinde ve müşteri kaybı sonrası (olmak üzere üç farklı süreçte de) dikkatlice yönetilmesi gereken bir olgu olarak karşımıza çıkmaktadır.

Algı Yönetimi’nin siyasi, askeri, sosyal ve iş yaşamında uygulama alanı bulunduğunu biliyoruz. İş dünyasında ise bu yönelimin stratejik olarak ele alınması iş dünyasının rekabet koşullarının gereği olarak karşımıza çıkmaktadır. Stratejik Algı Yönetimi iş dünyasında müşteri merkezli bir yaklaşımdır. Müşteriyi sürdürülebilirliğin ve kârın odak noktası olarak tanımlar ve müşteri memnuniyetinin önemi üzerinde durur. İş dünyasından müşteri algılamalarının en kolay tespit

³ **Kritik Kitle Noktası:** Belli bir toplumsal dönüşümün başlaması için gerekli görülen asgari toplumsal birliktelik (Frey, 2016, s.72).

edilebildiği alan ise müşteri deneyimlerinin ölçümlendiği çalışmalardır (Ertan, 2016, s. 1). Müşteri (kullanıcı, hasta, seçmen, üye vb.) deneyimleri algılama ölçümleri daha çok yüz yüze yapılan görüşmeler, elektronik ortamda yapılan anketler ve sosyal medya üzerinden yapılan geri bildirimlerin yorumlanmasıyla elde edilebilmektedir. Bu şekilde elde edilen veriler, mevcut duruma göre değerlendirilip, istenilen hedefe ulaşma yolunda stratejik algı yönetimi sayesinde geliştirilebilmektedir. Burada kastedilen stratejik algı yönetimi süreci; yönetenin niyetine göre yalnızca kendi çıkarlarını gözeten faaliyetleri ya da daha gerçekçi kararlarla fiili durumu tespit edip eksikliklerin giderilmesi ve her iki taraf için de fayda sağlayacak stratejiler olarak ortaya konulabilmesini ifade etmektedir.

1.3.5 Gündem Belirleme ve Propaganda

1960'lı yıllarda karşımıza çıkan Gündem Belirleme Modeli, McCombe, Shaw ve diğerleri tarafından geliştirilmiştir. Bu görüşe göre, kitle iletişim araçları halkı “ne hakkında düşüneceklerini” anlatmada çok maharetlidir. Başka bir deyişle, kitle iletişim araçları dünyayı bizim için inşa etme yeteneğine sahiptir ve bu yönde çalışırlar (Çoban, 2018, s.16). Medyanın bu gücü politikacıların ilgisini doğal olarak çekmektedir ve böylece medya da politika yapmaya başlamaktadır. Çoban (2018)'a göre, “medya haberler sayesinde gerçeklik ile bağlarımızı koparmakta ya da yeniden düzenlemektedir. Bu anlamda egemen ideolojinin medya yoluyla bize kendi gerçekliğini dayatması ve bunun tek gerçeklik olduğunu söylemesi kabul edilemez” (s. 16). Propaganda ise, kişilerin ya da grupların (bu bazen toplumu kapsayacak şekilde de icra edilmeye çalışılmaktadır) bir başka kişi ya da grup tarafından kontrol altına alınmaya çalışılmasıdır. Bu şekilde, düşünceler toplu olarak (doğru-yanlış, olumlu-olumsuz) yönlendirilebilmektedir. Genel kanaat odur ki, propaganda daha çok, negatiflik içermektedir. Gerçeklik çerçevesini kendi ufkuna göre belirlemektedir. İkinci Dünya Savaşında, Nazi Almanyası'nın da yaptığı böyle bir şeydi. “Medya Yönlendirmesi” açısından modern yüzyılda listenin en başında ise hiç şüphesiz ABD yer almaktadır. Deniz aşırı yayın yapan televizyon kanalları, dünya genelinde tanınan ünlülerin konuk olarak yer aldığı programlar, açık oturum ya da talk-show'lar, “dünya dili” olarak kullanılan İngilizce, propagandanın gücünü arttırmaktadır. Propagandalarda tanınmış yüzlerin, otoritelerin, bilim insanlarının, elit (olduğu düşünülen) kişilerin kullanılması daha geniş bir etki yaratmaktadır.

Chomsk'ye göre devlet propagandası, eğitimli sınıflar tarafından desteklendiği ve hiçbir sapmaya izin verilmeden yapıldığı zaman büyük bir etki yaratabiliyor (Chomsky, 1995 Akt: Çoban, 2018, s. 26). Propagandanın diğer temel özellikleri ise; içeriğinin basit olması, herkesin anlayabileceği bir dilin kullanılması, sürekli tekrarlanması adımlarından oluşmaktadır. Medyada haber sunulurken, “yöneten ideolojiye” hizmet olarak, yöneten ideolojinin önemsemiş olduğu (ve mutlaka toplumla paylaşılması gereken!) enformasyon, devletin ideolojik araçlarından biri (medya) kullanılarak hayata geçirilmektedir.

1.3.6 Geleceği Şekillendirme

Şimdiki zamanın/düşüncelerin/uygulamaların geleceği şekillendirmede çok önemli roller oynadığına hiç şüphe yok. Peki, gelecek şimdiyi şekillendirebilir mi? Evet, geleceğe dair vizyon oluşturulursa bu şekilde gelecek de şimdiden şimdiki zamanı şekillendirmiş olacaktır. Frey (2016, s. 9-25) bu düşüncüyü şu şekilde açıklıyor; “Geleceği kontrol edebiliyorsanız neden ona dair tahminler yürütmekle uğraşasınız ki? (...) Eğer insanların gelecek vizyonlarını değiştirecek, karar alma şekillerini de (yani şimdiki zamanı da) değiştirmiş oluruz”. Geleceğin aslında çok karmaşık ve rastgele olaylar kümesinden oluştuğunu düşünmeye meyilliyizdir. Frey (2016) birçok insanın geleceğin rastlantısal ve tahmin edilemez bir olaylar kümesinden ibaret olduğuna inandıklarını, oysaki gelecekteki birçok şeyin yüksek bir olasılık derecesiyle tahmin edilebildiğini söylüyor. Buna örnek olarak (küçük yanlışlar payları olmakla birlikte); iyi oyunculardan kurulu bir takımın maçı kazanacak olması, başarılı öğrencinin sınavda yüksek puan alacağı, hava tahmini raporları vs. verilebilir. Bir martının kanat çırpmasının hava değişimine etki edebileceğini öngören meteoroloji uzmanı Dr. Edward Lorenz bunu daha sonra *kelebek etkisi* teorisine dönüştürerek gelecek ve şimdiki zaman arasında sıkı bir bağ olduğunu açıklamayı başarmıştır.

Geleceği şekillendirmek için *şimdiki anı* şekillendirmek, bilinen bir kavram olmasına rağmen, etkilerinin boyutları ve gücü biraz gözden kaçmaktadır. Kısa zaman içerisinde gerçekleşecekler daha çok ilgi çekmekte ve takip edilebilmekte (algılanabilmekte) iken, orta ve uzun vadede gerçekleşecekler ise biraz kenara itilebilmektedir ve böylece *büyük resim* kendi oluşumu için görünmezlik pelerinin altında kendisini korumaya alabilmektedir. “*Ağaç yaşken eğilir*”, “*çocuklar*

geleceğimizdir” kavramlarının altında da benzer düşünceler yer almaktadır. SM içerisinde yer alan birçok kavram şimdiki zaman için uygulamaya konuluyor olsa da, aslında öte yandan geleceği de şekillendirmektedir.

1.3.7 Sosyal Kanıt

Sosyal kanıt, genel olarak, grup, kalabalık ya da toplum içerisinde insanların nasıl davranacağını bilmediği, kararsız kaldığı ya da bilgisiz olduğu konularda geriye kalan büyük çoğunluğun davrandığı gibi davranmasıdır. Bu davranış biçimi her zaman doğru bir davranış biçimi olmasa da, birçok kişinin benzer davranışı sergilemesinden dolayı bu durum bir tür savunma mekanizması oluşturabilmekte, davranışı sergileyen açısından hafifletici sebep gibi görülebilmektedir. Hadnagy (2017, s. 228)’e göre bu tür davranışlar daha çok, insanların aşına olmadıkları bir durumda kaldıklarında ve bunun yanı sıra bu durumla nasıl başa çıkacaklarına dair alabilecekleri bir referans noktası bulamadıklarında ortaya çıkmaktadır ve bu durum onları daha bilgili olduğunu düşündüğü kişileri örnek almaya yöneltebilmektedir.

Sosyal kanıt, sosyal etki ve taklit etme kavramları ile de iç içedir. Kişi ve grupları yönlendirmede oldukça etkili bir SM aracı ve yöntemidir. Bu nedenle tanınmış ve ünlü kişiler reklam filmlerinde oynatılmaktadır. Başarıları ya da fiziksel çekicilik gibi özellikleri ile ön plana çıkan bu kişileri insanlar daha kolay takip ve taklit etmek istemektedir. Bir kalp pili markasının tanıtımında ünlü bir kalp cerrahının kullanılması (bu durum tanıtımı yapılan kalp pilinin kaliteli olduğu anlamına gelmese de) satışları olumlu yönde etkileyecektir. Çevrimiçi alışveriş yaparken, satın almak istediğiniz ürünle ilgili yapılmış olan (olumlu-olumsuz) geri bildirimler bireylerin tercihlerini etkileyecektir. Bilgi yarışmalarında yarışmacının, izleyici joker hakkını kullanmasında da benzer etkiler görülmektedir; yarışmacı kendi tahminini açıklarsa izleyiciler bundan (kısmen de olsa) etkilenecek oylama yapacak ama esas etki izleyicilerin “ortak” kararının yarışmacıyı etkilemesi yönünde olacaktır. Yarışmacı, seyirciden gelen cevabı dikkate alarak soruyu doğru cevaplayamamış olsa bile, kendine sosyal bir kanıt bulduğundan, olumsuz etkiler daha hafif atlatılabilecektir. Toplumsal kabuller de benzer şekilde işlemektedir; yaşanılan bölgedeki insanlar gibi davranmak doğal bir kabul görme ile ödüllendirilirken, “aksi yönde” bir davranış tercihinde bulunmak ise (doğru bir tercih olsa dahi) dışlanacaktır. Sosyal baskı, toplumsal baskı vb. baskılarda da benzer

durumları görmek mümkündür. Radyo ve TV programlarında (daha çok komedi ve sitcom) kullanılan toplu alkış, kahkaha efektleri de yine sosyal kanıt sunmanın bir çabasıdır.

1.3.8 Toplum Mühendisliği

Toplum mühendisliği kavramı, devlet iktidarlarının veya özel gruplarca toplumun geniş bir bölümünün tavır ve sosyal davranışlarına doğrudan ve ya dolaylı etki sağlayacak çabalar için siyaset biliminde geçen bir kavramdır (toplummuhendisligi.com). Yönetenler ve yönetilenler ayrımından kaynaklı ve çeşitli ideolojik düşüncelerin örüntüleriyle kaplı karar verici mekanizmaların kim ya da kimler tarafından kontrol edilmesi gerektiği tarih boyunca süregelen bir mevzudur. Seçme ve seçilme, grup lideri, sözcü, vekil, temsilci, başkan, devlet başkanı, dini lider vb. başlıklar ve kavramlar altında vücut bulmuş yönetme ve yönlendirme çabaları birçok dönemde “karar alıcıların” diğerleri adına (halk, toplum, avam, tebaa) “işleri yürütme” şeklinde uygulanması ile sürdürülmüştür. Yönetim şekli ne olursa olsun (demokrasiler de dâhil) hep bir karar verici var olmuştur. Toplumlar genel olarak, yönetilmeye ve yön verilmeye muhtaç kalabalıklar olarak görülmüş, gerek katı kast sisteminin uygulandığı dönemlerde, gerek askeri yönetimlerde gerekse modern yönetimlerde bu düşünce hep var olmuştur. Tüm gerçeklerin çıplaklığı ve açıklığı ile toplum tarafından bilinmesi ve yorumlanması ise pek istenmemiş, aksine bunun onlar için zaman kaybı, can sıkıcı ve faydasız işler olacağı görüşü ağır basmış ve böylece yönlendirilmesi mübah olan “tüketim toplumu” ve buna uygun bir kamuoyu oluşturma çabası süregelenmiştir hep.

Kıta Avrupası, İngiltere ve ABD’de sanayi devrimi sosyal bir değişim yaratmıştır. Bu değişim 19. yüzyıl sonlarında, kitle hareketleri ve toplumsal olaylardan duyulan endişenin artmasına neden olmuştur. İşçi hareketlerinin yoğunlaşmasının da katkısıyla, toplumun büyük bir kısmını oluşturan kalabalıkların, rasyonel akılla değil de hayvansal içgüdü ve şehvetle hareket ettiği şeklindeki görüşler, kitlelerin düzene karşı ciddi bir tehlike olarak görülmeye başlanmasına neden olmuştur (Abuşka, 2010, s. 5). Kalabalıkların us ile hareket etmediği, edemediği düşüncesinin Türkiye’deki yansımaları ise yakın geçmişte, “*memleketi başlar değil ayaklar mı yönetsin?*”, “*profesör ile dağdaki çobanın oyu bir olur mu?*”

şeklinde vukuu bulmuş ve tartışılmıştır. Devletin ideolojik araçları ise bu tartışmalara yön vermek için güncelliğini hep korumuştur.

“Açığa vurma (publicity)” ve reform anlayışlarının, farkında olmadan otoriteye saygı göstermeyen bir toplum yarattığına inanan ABD’li Walter Lippmann, I. Dünya Savaşı’ndan sonra ABD’nin dünyaya demokrasiyi ihraç etmesi görüşünü desteklemekle birlikte, cahil bir güruh olan kitlelerin gerçek demokrasi içindeki rolünden endişe etmiş ve Le Bon’un savunduğu kitle kontrolünü benimsemiştir. Açığa vurma şeklindeki yayıncılığın irrasyonel halkı kontrol için kullanılması gerektiğini düşünen Lippmann’ın; “halka gerçeklerin (factual truth) sunulması halinde, toplumun bekası için önemli konuları bilgisiz güruhlara tartışacağı bir ortam yaratılacağı”nı savunmuştur. Böylece “irrasyonel tepkilere açık halkın önemli konularda varacağı kanaatlerin, rasyonel olması gereken liderlerin önüne köstek olarak çıkacağı” şeklindeki görüşü, günümüz toplum mühendisliği anlayışına yön vermiştir (Abuşka, 2010, s. 2-3).

Kitle iletişim araçlarının yaygınlaşmasıyla, toplum mühendisliği altın çağını yaşamaya başlamış ve hiçbir dönemde olmadığı kadar kamuoyu “doğrularla” bilgilendirilebilmiştir. Bu süreç daha sonraları basının karşımıza yasama, yürütme ve yargı güçlerinden sonra “dördüncü güç” olarak çıkmasıyla zirve yapmıştır. Günümüzde ise medya, üzerine “sosyal medya zırhını” da giyerek birçok resmi otoritenin, kurumların, başbakanların, cumhurbaşkanlarının ve devlet başkanlarının resmî duyuru/ilan/fikir beyanı ve “en doğrusunu açıklama” platformuna dönüşmüştür.

1.3.9 Çerçeveleme Etkisi (*Framing Effect*)

Çerçeveleme etkisi, SM’de olduğu gibi, bilgi sunarken, kişilerin sizin istediğiniz yönde düşünmesine yardımcı olacak şekilde sunulmasıdır. Bunun farklı kullanım teknikleri vardır; bir bilginin tamamını değil istenilen kısmının öne çıkartılması, bir fotoğrafın (tamamına bakıldığında farklı bir bilgi ya da durumun söz konusu olabileceği) yalnızca bir parçasının gösterilmesi, cümlede belirli bir kelimenin altının çizilmesi, cümlenin tersten söylenmesi, sayı ve rakamların (istatistik içeren bilgilerde daha çok kullanılmaktadır) tersten söylenmesi ya da yorumlanması gibi. Örneğin; bir ülkede meydana gelen trafik kazaların oranını küçük göstermek istiyorsanız, bilgi (ya da haber) şu şekilde düzenlenebilir; bu yılki

trafik kaza oranlarında geçen yılki oranlara göre hiçbir artış yaşanmadı (aslında bu yıl da, geçen yıl da yaşanan kaza oranları çok yüksek olabilir). Diğer bir örnek; ebola virüsünden Güney Afrika’da ölenlerin sayısı elli bin kişi demek yerine, sayıyı önemsiz gibi göstermek için, ülke nüfusunun on binde birinden az şeklinde çerçevelenebilir. “İnsanların yarısı hastalıklı” ifadesi ile “insanların yarısı sağlıklı” ifadeleri aynı şeyler olsa da kişilerde yarattığı etkiler farklı olabilmektedir. Şekil 1 ve Şekil 2’de çerçeveleme etkisine yönelik iki farklı örnek verilmiştir.

Şekil 1. Çerçeveleme Etkisi-I



Şekil 2. Çerçeveleme Etkisi-II



Kaynak: <https://unsplash.com/photos/SeTgyZSgj4Y>, Erişim: 11.03.2020
(çerçeve ve yazı araştırmacı tarafından fotoğrafa eklenip, uyarlanmıştır)

Haberde sansür mekanizmasının uygulanmaması halinde, kelimelerin tam anlamıyla propaganda olarak işlev görmesi mümkün değildir. Bir propagandanın hedefine ulaşması için halk ile olay arasında bir bariyer oluşturulmalıdır. Herhangi bir insan için arzu edilir bir sahte ortam yaratmadan önce gerçek ortama erişim sınırlandırılmalıdır (Lippmann, 1922, s. 42-43, Akt. Abuşka, 2010, s. 26). Bu sayede çerçeveleme etkisi görevini daha etkin bir şekilde yerine getirebilecektir. Propaganda, çerçeveleme etkisinin kullanımında sosyolojinin de yardımı ile (bütünleşik bir) kaldıraç etkisi görebilmekte ve bu özelliğinden dolayı yaygın olarak kullanılmaktadır. Propaganda, modern dünyada en güçlü araçlardan biri olarak ortaya çıkmıştır. Kitleleri önemli semboller, hikâyeler, rivayetler, raporlar, resimler ve diğer sosyal iletişim şekillerinin bilinçli manipülasyonu ile kontrol altına alma çabası rutin hale gelmiştir (Lasswell, 1927, s. 220-221, Akt. Abuşka, 2010, s. 39).

Çerçevelemenin kullanımının arkasında yatan niyete dair karşıt görüşler bulunmaktadır. Lilleker'e (2013, s. 114) göre, çerçevelerin, bilginin izleyiciler (kişiler) tarafından algılanmasını sağlayan deneyimsel ve bilişsel kısa yollar görevini üstlendiği savunmasına karşın, bilginin aşırı basitleştirildiği ve halkın önemli meselelerden uzaklaştırıldığına dair karşıt görüşler yer almaktadır. Sonuca ilişkin çerçeveleme yöntemi ise taraflılık içerdiğinden dolayı eleştirilere hedef olmaktadır. Örneğin, Avrupa Para Birliği ya da Avrupa Anayasası hakkında yapılan karşıt yayınlar, Avrupa Birliği'nin bizzat kendisi hakkında çeşitli olumsuz algılamalara neden olabilmektedir.

1.3.10 Manipülasyon

Manipülasyon daha çok, kişilerin bazı yetileri ve araçları kullanarak, kendi çıkarları doğrultusunda hedefteki kişi ya da kişileri etkilemek ve kontrol altına almak olarak bilinmektedir. Manipülasyon, gerçeği ya da gerçek olmayanı, doğru ya da yanlış bükerek, olduğundan daha farklı bir şekilde (kendi çıkarları doğrultusunda) sunmak ve/ya kullanmaktır.

İnsanlar kendi hayallerini cesaretlendiren, başarısızlıklarını haklı çıkartan, korkularını hafifleten, şüphelerini doğrulayan ve düşmanlarını kötülemeye yardım edenler için her şeyi (her türlü yardımı) yapar (Şerban ve Şerban, 2014, s. 7). Manipülasyon sanatı olarak da görülen ikna (kabiliyeti) ise bu manevranın en güçlü araçlarından biridir. Hadnagy (2017)'e göre manipülasyon, insanları sizin gibi

düşünmeye sevk etmek ve kendilerini iyi hissetmelerini sağlamaktan çok sizin istediğinizi yapmaya zorlamakla alakalıdır. Manipülasyon ve zorlama, hedefin ideolojisini, inançlarını, tutumlarını ve davranışlarını değiştirmek için daha çok psikolojik güçten yararlanmak, hedefin kendi özgür iradesini ve eleştirel düşünmesini kırmak, değiştirmektir (s. 251-266). Ulaşmak istenilen nokta, nesnel ve mantıksal çıkarımlar yapmasını engelleyerek (istenilen yönde) belirli bir kalıp içerisinde hareket etmesini sağlamaktır. Hedefin koruma kalkanı kırıldıktan sonra beslenme/bilgi kaynağı artık sosyal mühendisin hizmetinde olacaktır.

Hadnagy (2017, s. 252)'e göre manipülasyonda tutum, ister beyin yıkama şeklinde isterse daha az sinsi bir girişim şeklinde olsun, uygulaması altı farklı şekilde cereyan etmektedir. Bunlar;

- Hedefin telkine açıklığını arttırmak
- Hedefin çevresini kontrol altına almak
- Şüphe uyandırmak
- Güçsüzlük hissi yaratmak
- Hedefte güçlü duygusal tepkiler yaratmak
- Kuvvetli gözdağı vermek

Hadnagy'nin önerdiği bu başlıklara şunları da eklemek uygundur;

- Bir amacı ya da çıkarı, hedef ya da referans göstererek, kişiyi bu yönde aşılama
- Hedefi, övgülerle (daha çok gerçek olmayan övgülerle) güdülemek
- Çeşitli şekillerde hedefin kaygılarını arttırmak ya da azaltmak
- Yanıltıcı ya da gerçek bilgiler kullanarak telkinde bulunmak
- Şartlandırmak
- Ödül ve teşvikler

İşletmecilik açısından da manipülasyonun uygulama alanı oldukça yaygın ve geniştir; pazarlamada, satışta, medyada, gömülü reklamlarda ve benzerlerinde. Örneğin mağaza ve marketlerde rafların belirli aralıklarla yerleştirilmesi, ürün-renk kombinasyonları, üst raflara (göz hizasına) daha çok satılan ürünlerin yerleştirilmesi, müşterilerin ilk girişte mağazayı daha çok sağdan başlayarak gezdikleri bilindiği için

çarpıcı ürünlerin o alana yerleştirilmesi, rahatlatıcı müzik yayınlama, havaya sıkılan güzel koku gibi birçok yöntem ve uygulama bulunmaktadır.

1.3.11 Nöro Linguistik Programlama (NLP)

Nöro Linguistik Programlama (Neuro Linguistic Programming [NLP]), insanların üzerinde hiç düşünmeden hızlıca otomatik bir şekilde gerçekleştirmiş olduğu düşünme ve davranış biçimlerini bilinçli bir duruma taşıma metodudur. İnsanların duyu organları aracılığı ile edinmiş olduğu yaşam tecrübelerini ve bu tecrübelerle dilin etkilerini, dil aracılığı ile kodlanması (mesaj) vasıtası ile duygu, düşünce ve davranış biçimlerinin yeniden formüle edilmesi, düzenlenmesi, yönetilmesi olarak bilinmektedir. Bostrom (2018), bir beyindeki düşüncelerin diğer beyin tarafından anlaşılabilmesi için, düşüncelerin ortak bir uzlaşım uyarınca parçalara ayrılıp semboller halinde paketlenmesi gerektiğini, ancak bu şekilde sembollerin alıcı beyin tarafından doğru bir şekilde yorumlanabileceğini, dil'in işinin de bu olduğunu (s. 66) ifade etmektedir. NLP; yaratıcılık, reklam, yaşam koçluğu, sağlık, eğitim, psikolojik yardım, psikoterapi, insan kaynakları ve SM gibi birçok alanda kullanılmaktadır.

NLP tekniğinde sosyal mühendis, manipüle etmeye çalıştığı kişiye bilinçaltı mesajlar vermek için beden dilini ve dikkatli bir sözcük seçimi kullanmanın yollarını arar. Sosyal mühendis, işe beden dilini hedefin/kurbanın beden dili ile eşleştirerek başlar. Ayrıca nefes oranı, ses seviyesi, aksan ve kelime hazinesiyle eşleşme sağlar. Bunu yaparak, bilinçaltı bir seviyede ilişki kurmaya çalışır. Daha sonra beden dilini değiştirerek, hedefin omuzlarına veya kollarına hafifçe dokunarak olumlu düşünceleri, duyguları ve imgeleri ifade eden kelimeleri kullanarak başka bilinçaltı mesajları da verebilir. Tüm bu dokunsal, görsel ve sözlü eylemler hedefteki kişinin sosyal mühendis ile etkileşim kurmasını sağlar. Bu noktadan sonra sosyal mühendis, kişisel bilgiler, bir şirketin sırları, gizli veya kritik bilgileri hakkında bilgi toplamak gibi maksatlarla (her neyin peşinde ise) iletişimi devam ettirir (Tosun, 2015, s. 14). NLP, 1970'li yıllarda Gregory Bateson'un öncülüğünde Richard Bandler ve John Grinder tarafından geliştirilmiştir (social-engineer.org). Neden bu kadar başarılı olduklarını anlamak için zamanın en başarılı terapistleri (Fritz Perls, Virginia Satir ve Milton Erickson) ile çalışarak, bu çalışmanın sonucunda NLP'nin "kod" kavramlarını geliştirdiler. Bu ilk (öncül) araştırma, değişimi etkileyecek dil

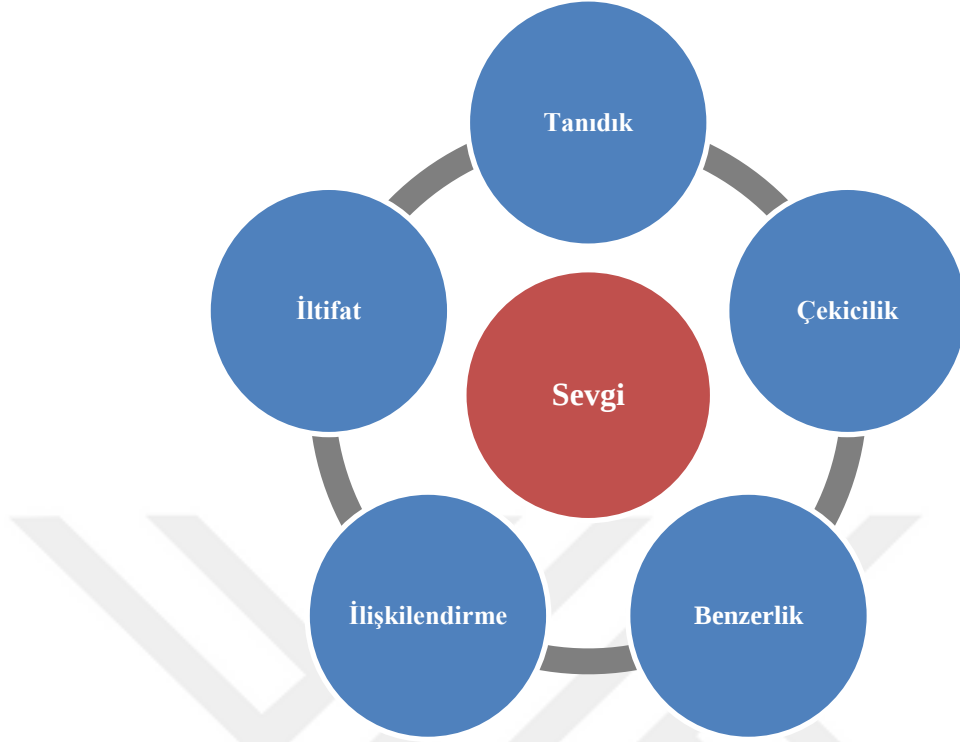
kalıplarının nasıl kullanılacağını tanımlayan bir meta modelin (dili daha etkin kullanabilme, iletişimde avantaj yaratma) geliştirilmesini sağlamıştır. NLP kullanımı, diğerlerini kontrol etmek, yakalanmadan yalan söylemek ya da insanların tüm ruhsal sorunlarını çözmek maksadıyla, 1900-2000’li yıllarda çok popüler hale geldi. NLP bilimsel olarak kanıtlanmamış olsa da kullanılmaktadır. NLP, sosyal mühendislerin hedeflerindeki kişilerin istenilen davranışları sergilemeleri, yönlendirmelere olumlu tepki vermeleri için sesin, dilin ve kelime seçiminin nasıl kullanılacağıyla ilgilidir; bazı durumlarda ne söylediğiniz değil onu nasıl söylediğiniz daha önemlidir, sesteki titreme, vurgunun gücü (cümle içindeki bir kelime üzerinde yoğunlaşabilir), sesin tonu, devrik cümle kurma vb.

NLP, insanlara danışmanlık ve yardım için güçlü bir araçtır, ancak, SM bağlamında, birisini tanımak ve daha sonra onlar üzerinde etki kazanmak için basit bir teknikler seti olarak daha sınırlı bir şekilde kullanılır. NLP, karşınızdaki kişinin dikkatli bir şekilde dinlenmesini tavsiye eder. Kişiler kendilerini ifade ederken; “ben” mi “biz” mi diyor? “düşünmek” mi “hissetmek” mi kelimesini kullanıyor, “ne demek istediğini görebiliyorum” ya da “onu duyabiliyorum” mu diyorlar (görme duyusunu mu yoksa duyma yetisini mi ön plana çıkardığı anlaşılıyor). Kişi, belirleyici mi (kendinden emin) yoksa tereddütlü mü görünüyor? NLP, hedefin birçok özelliğini ortaya çıkartmaya (anlamaya) ve bunun üzerinden hızlı bir şekilde sempati geliştirerek kişiler üzerinde etkili olabilecek bir pozisyona erişmeyi sağlamaktadır (Barrett, 2003, s. 63).

1.3.12 Sevgi ve İtaat

Cialdini (2018) sevgi ve itaat (evet deme) konularını ilişkilendirmektedir. İnsanların bildikleri, sevdikleri ve çekici buldukları kişilere evet demeyi tercih ettiklerini, itaat profesyonellerinin (bir anlamda sosyal mühendislerin) bu durumu lehlerine kullandıklarını belirtmektedir. Sevilen, bilenen, güvenilen, hayır denilmesi zor olan kişilerin bazı işlerin yaptırılmasında aracı olarak kullanılması ihtiyacının da benzer kaynaklı olduğunu söylemek mümkündür. Cialdini’nin sevgi ve itaat ilişkisini Şekil 3’de görülen beşli ile özetlemek mümkündür:

Şekil 3. Sevgi ve İtaat (“Evet Deme”) İlişkisi



Kaynak: Cialdini, 2018’den uyarlanmıştır

- Çekiciliğin sosyal etkileşimde avantaj sağladığı düşünülen daha da fazladır.
- Bizim gibi olan insanları (benzerlerimizi) severiz.
- Çok abartılmadan (dozunda) yapılan iltifatlar sevgiyi, yani itaati pekiştirir.
- Tanındıklığı arttırmak (tekrar tekrar irtibatta olmak) sevgiyi oluşturur.
- Pozitif olaylarla ya da kişilerle ilişki kurmak (ilişkilendirmek) sevgi bağıını artırır.

1.3.13 Teknoloji Okuryazarlığı

Teknoloji okuryazarlığı en temel şekilde teknolojiyi kullanabilme, yönetebilme, değerlendirebilme ve anlayabilme yeteneği olarak tanımlanabilir (ITEA, 1996; Rose vd. 2004 Akt: Canbaz, 2010, s. 12). Teknoloji okuryazarlığı, bireylerin teknoloji ile kendileri ve toplum arasındaki ilişkinin anlaşılmasında gerekli olan entelektüel süreç, yeterlilik ve düzenin tümü olarak tanımlanabilir (Yawson, 2010 Akt: Bölükbaşı, 2012, s. 8). Kişilerin herhangi bir bilişimci kadar teknolojiden anlamalarını bekleyemeyiz fakat içinde bulunduğumuz çağda, özellikle yeni nesil dikkate alındığında, hemen hemen tüm iş ve işlemlerin dijital platformlar üzerinde

gerçekleştirildiği düşünülecek olursa, herkesin mümkün olduğunca teknoloji okuryazarı olması beklenmektedir. En azından temel bilgileri, teknolojik haberleri, güvenlikle ilgili bilgilendirme yazılarını okuyup anlama düzeyinde olsa da.

Tüm aile fotoğraflarını en tanıdık güvencik bir arkadaşın evinde bile saklamaktan (daha çok güvenlik ve dışsal, belki de üçüncü şahıslardan dolayı) imtina ederken, nasıl oluyor da hiç tanımadığımız kişilerin (şirketlerin) bilgisayarlarında saklanmasına kolayca razı olabiliyoruz? Kolumuzda taşıdığımız akıllı saatlere veya cep telefonlarına girmiş olduğumuz (artık veri girişlerini bile insanlar yapmıyor, sensörler bu verileri otomatik kayıt edebiliyorlar: Nabız, tansiyon, yürüme mesafesi, yürüyüş rotası, günlük rota, hafta sonu rotaları vb. onlarca veri) bilgilerin artık kişisel bilgiler olarak kalmadığını, cihazın GPS'i açıkken çekilen bir fotoğrafın internet üzerinden bir yere gönderildiğinde (gps sayesinde coğrafi konumları ve fotoğraf içine gömülü exif bilgileri sayesinde diğer bilgileri; tarih, saat, makinenin markası, açısı, eğim, vb.) aslında yalnızca fotoğrafı değil birçok bilgiyi de paylaşıyor olabileceğimizi kaçımız biliyor ya da önemsiyor? Teknoloji okuryazarlığı yalnızca burada bahsedilenlerle sınırlı olmasa da tek başına buradaki bilgiler dahi teknoloji okuryazarlığının önemini anlamak/anlatmak için yeterlidir.

1.3.14 Medya Okuryazarlığı

RTÜK (2016) medya okuryazarlığını şu şekilde tarif etmektedir; “medya okuryazarlığı; yaygın kabul gören tanımıyla, çeşitli türden (görsel, işitsel, basılı, vb.) medya mesajlarına erişebilme, erişilen medyaları eleştirel bakış açısıyla çözümleyip değerlendirebilme ve kendi medya iletilerini üretebilme becerisidir. Medya iletilerinin kendine özgü yapısının, dilinin ve uygulamalarının olduğu ve bunların sürekli değişmekte, gelişmekte olduğu da aşikârdır. Bireylerin bu mecraları daha verimli kullanmaları ve bunu yaparken maruz kalınabilecek bazı riskler karşısında farkındalık geliştirebilmeleri için, medya iletileri ve yöntemleri konusunda bilgi sahibi olmaları gerekmektedir.”

Bireylerin bu konularda daha iyi olmaları, teknolojiyi en azından ihtiyaçlarını giderecek düzeyde de olsa kullanabilmeleri, yaşam konforlarını arttırmaları ve ayrıca söylemleri çok fazla yanılgıya uğramadan ama kendi süzgecinden de geçirerek çözümlemeleri ile ilgili eğitimler “medya okuryazarlığı” eğitimi olarak adlandırılmaktadır.

Temel düzeyde de olsa medya okuryazarı olmak bireylerin hem güncel bilgi/haber akışını izleyebilmelerine hem zaman zaman bilgi/haber teyidi yapılması gerekebildiğini anlamalarına, yönlendirici bilgi/haber karşısında dikkatli ve bilinçli olunması gerektiğine, haber kaynaklarının çeşitliliğine ve bazen tutarlı bilgilendirmelerin yapıl(a)madığına, politik vb. manevralar için *çerçeveleme etkisi* vb. kavramların kullanılabildiğine dikkat etmeleri gerektiği konusunda faydalıdır ve katkı sağlayıcıdır. Hiç şüphesiz gündemin sürekli değiştiği ve bilgi akışının katlanarak arttığı günümüzde bu ve benzeri durumlar için bireylerin de kendi bilgi dağarcıklarını güncellemeleri ve yeni oluşumlara karşı yeni korunma yöntemleri geliştirmeleri gerekebilmektedir. Sonuç olarak denebilir ki, “her yaştaki bireyde sorgulama alışkanlığı oluşturmak, ifade biçimlerini geliştirmek ve eleştirel düşünürler, etkili iletişimciler ve günümüz dünyasında aktif vatandaşlar yetiştirmek medya okuryazarlığı ile geliştirilmek istenen davranış biçimleridir” (Avşar, 2014).

1.3.15 Mahremiyet (*Privacy*)

Küreselleşme, artık sadece yerel (ulusal) yasalara değil diğer taraftan uluslararası hukuk çerçevesinde, milletler arası sözleşmelere de bağlı kalınmasını istiyor. Entegrasyonun sağlanması açısından bu istek anlamlıdır. Be nedenle ilk bakılması gereken yerlerden biri Avrupa İnsan Hakları Sözleşmesi (AİHS) ve Avrupa İnsan Hakları Mahkemesi olmaktadır. Mahremiyet açısından AİHS’de yer alan 8. Madde’nin içeriğine bakılacak olursa (Løkke, 2018, s. 88);

Özel ve aile hayatına saygı hakkı:

- Herkes özel ve aile hayatına, meskenine ve yazışmalarına saygı gösterilmesi hakkına sahiptir.
- Bu hakkın kullanılmasına bir kamu makamının müdahalesi, ancak müdahalenin yasayla öngörülmüş olması ve demokratik bir toplumda ulusal güvenlik, kamu güvenliği, ülkenin ekonomik refahı, düzenin korunması, suçun önlenmesi, sağlığın ve ahlakın veya başkalarının hak ve özgürlüklerinin korunması için gerekli bir tedbir olması durumunda söz konusudur.

Tüm bunların yanı sıra birçok ulusal yasalarda yer alan konut dokunulmazlığı, iletişim hakkı, özel (kişisel) bilgilerin gizliliği yani kısaca mahremiyete ilişkin sayabileceğimiz birçok madde bulunmaktadır. Peki, gerçek

yaşamda bunlara ne denli uyuluyor diye baktığımızda durum çok da beklediğimiz ya da olmasını umut ettiğimiz şekilde yürümüyor. Sosyal medya devleri (özellikle yazılım firmaları) kullanım şartnamelerinde içerik analizi yapmadıklarını, kullanıcıların bu konuda rahat olmaları gerektiğini taahhüt ediyorlar, yalnızca üst veriye (meta data) baktıklarını söylüyorlar fakat *büyük veri* (big data) aracılığıyla üst veri izlemesi yapmak aslında içerik verisiyle izleme yapmaktan daha kabul edilebilir bir şey değildir keza belirli sayıdaki üst veri birleştirildiğinde içerik veri analizi yapmış sayılırsınız. Bu kitlesel olarak yapılırsa, mahremiyet hakkında daha çok bilgi demektir. Üst veriyi basit bir örnekle açıklayacak olursak, örneğin; e-postalarınızın konu (subject) kısmında yazarları bir üst veri olarak ele alabiliriz. Tek bir e-postadaki konu satırı karşı tarafa (e-postalarınızı takip eden organizasyonlar) bir şey ifade etmeyebilir ama örneğin son altı ay içerisinde göndermiş ve almış olduğunuz e-postaların sayısı kadar konu (subject) başlığını alt alta, yan yana getirdiğinizde hakkınızda tahminlerden çok daha fazla bilgi içerdiği görülebilecektir. Aynı şehirden gönderilen e-postaların yalnızca konu başlıklarına bakılarak o şehirde salgın hastalık, sel taşkınları, deprem ya da başka bir eylemin varlığını tahmin etmekse sanıldığından daha kolay hale gelmektedir. Bir şehirde grip salgının olduğunu ve sayısal tahmini e-posta ve hastane kayıtlarından öğrenen içerik sağlayıcıları (hosting ya da yazılım firmaları, dev şirketler) bu bilgiyi grip aşısı üreten bir firmaya para karşılığı satabilir. Bu aşamada özel hayata bir müdahale olmadığı düşünülüyor olabilir ama bireylerin yazışmalarından (yalnızca üst veri kullanılarak) bir veri, toplam yazışmalardan enformasyon ve enformasyon toplamlarından bir bilgiye (ör; şu şehirde 2.500 kişi gripten şikâyetçi gibi) ulaşıldığında aslında bilgi satışı gerçekleşmiş olmaktadır. İnsanların sağlık durumu başkaları tarafından işleniyor ve işleyenler açısından (haksız ve izinsiz) bir ekonomik değer elde edilebiliyor. Daha güncel bir örnek verecek olursak, akıllı cep telefonlarımıza sağlık bilgilerimiz (bizim isteğimizle fakat verilerin nerede kullanılacağından habersiz olarak) SM becerileriyle, sözde gönüllü olarak işleniyor. Bütünün bir parçası olarak (sistem yaklaşımına göre bütün, alt parçaların tamamından daha kıymetlidir) insanlar sistemin bir parçası haline getiriliyor ve mahrem bilgiler bu şekilde karşı tarafı ihya edebiliyor.

Günümüz cep telefonları pek çok yönden mükemmel birer “gözetleme aracı” ve 21. yüzyılda, hem vatandaşlar hem de toplum için bir takım büyük sorunlara yol

açmadan sistemden çıkmak zor gibi gözüküyor. Kişi, akıllı telefonsuz, internetsiz ya da banka kartsız yani tamamen analog bir hayat sürmeye kalkıştığında, bu tavır yöneticilerde kuşku uyandırıyor (Løkke, 2018, s. 11).

Kamusal güvenlik için otoriteler (devlet/hükümet), izlemenin gerekli olduğuna inanmak eğilimindedir fakat ne tür bilgilerin kamunun yararına olduğu konusunda açıklık ve fikir birliği bulunmamaktadır. Løkke (2018, s. 17), Alman Demokratik Cumhuriyeti (DDR) güvenlik ve istihbarat şefi Mielke'nin söylediklerinin izleme konusunda otoriter yönetimlerin yaklaşımını açıkça ortaya koyduğunu ifade etmektedir, şöyle ki: "Her şeyi anlayacaksak, her şeyi bilmeliyiz." Her şeyi bileceksek, doğal olarak herkesin, her zaman gözetlenmesi gerektiği sonucu ortaya çıkmaktadır. Yalnızca soğuk savaş döneminin değil günümüzde de dikkat çeken konuların başında yer almaktadır mahremiyet. Gelişen teknolojiler sayesinde, yalnızca otoriter ve sınırları yabancılara açmaktan pek hoşlanmayan ülkeler değil, gelişmiş ülkelerin de bu konuda iştahları kabarıktır. Dijital teknolojilerin izleme araçları daha da geliştikçe, yönetimler/devletler daha otoriterleşip, özel yaşamı ortadan kaldıracak müdahalelerle siyasi alternatiflerini yok mu edecekler sorusu akıllara gelmektedir. Özel hayatın içine (gelişmiş teknolojiler sayesinde kişisel bilgilere kolayca erişebilen) fütursuzca girecek yönetimler, sosyal medya araçları ve SM'nin gücünü de kullanarak topluma acaba şu şekilde mi seslenecek; "Sizin ihtiyacınızı, ne istediğinizi, hatta neyi istemediğinizi, nasıl düşünüp karar verdiğinizi biliyoruz, size bunları ancak biz verebiliriz!"

"Gizleyecek bir şeyiniz yoksa neden onları saklamaya gizlemeye çalışsınız ki!" ve benzeri yaklaşımlarla SM yönlendirmeleri yaparak insanları daha açık (hiç çekinmeden bilgilerini paylaşmaları gerektiği) hale getirmek isteyenlerin sayısı hiç de azımsanacak düzeyde gözüküyor. Løkke (2018, s. 22), Google'ın 2009 yılındaki patronu Eric Schmit'in, "Başkalarının bilmesini istemediğiniz bir şeyler yapıyorsanız, belki de her şeyden önce bunu hiç yapmamanız gerekmektedir" dediğini hatırlatarak, özel hayatın saklayacak bir şeyimizin olup olmamasıyla alakalı olmadığının iknasına çalışıldığını hatırlatıyor.

Başkalarının sizin hakkınızda neler bildiğini (dijital platform üzerinden elde edilenler için) bilme hakkı, kişisel verilerinizin nerede, ne için ve ne kadar süreyle kullanılacağını bilme hakkı, verilerin izinli kullanımdan sonra süresiz olarak

silineceğini talep etme hakkı, dolayısıyla mahremiyetin korunmasını talep etme hakkı, *özel hayatı koruma hukuku* başlığı altında düzenlenmeli ve dikkatli bir gözetim/denetim altında yönetilmelidir.

1.3.16 Heuristics

Genel istatistikleri göz önünde bulundurmadan, bize (çeşitli sebeplerden dolayı) daha doğruymuş gibi gelen/görünen yargılarda bulunma olarak tanımlayabileceğimiz *heuristics* Amos Tversky ve Daniel Kahneman tarafından öne sürülmüştür. Kısa yola dayanarak tahminlerde bulunma ya da karar verme olarak da tanımlayabileceğimiz *heuristics* her zaman doğru ya da optimum sonucu vermeyebilmektedir. Öğrenen algoritmalarda kullanılmasındaki gerekçe ise daha kısa zamanda sonuç elde edilebilmesindendir. SM açısından, daha hızlı bilgiye ulaşma ve aynı zamanda edinilen bilginin doğruluğunu sorgulama bakımından üzerinde durulması gereken bir nüanstır bu konu.

İnsanlar sorunların göreceli önemini hafızada ne kadar kolay erişilebildiklerine göre algılayıp değerlendirirler; bu durum genel olarak büyük ölçüde, medyada o konunun ne kadar yaygın olarak işlendiğiyle alakalıdır. Sık sık değinilen konular akılda kalırken, diğerleri dikkatlerden kaçmaktadır. Otoriter rejimlerin bağımsız medyaya ağır baskılar yapması da bu yüzden ileri gelmektedir. Dramatik olaylar ve ünlüler kamuoyunda kolayca ilgi uyandırdığından, medyanın kitlesel çılgınlıkları beslemesine sık rastlanmaktadır. Kişisel bağlamda ise, zor bir soru ile karşılaşıldığında, genellikle ikamenin farkına varmadan, onun yerine daha kolay bir soruyu yanıtlamak tercih edilir (Kahneman, 2018, s. 14-18). Sosyal mühendisler, esas elde etmek istedikleri bir sorunun cevabı için, daha zor ve karmaşık bir soru ilave ederek amaçlarına daha hızlı bir şekilde (bu yöntemi kullanarak) ulaşabilmektedir.

1.3.17 Etik

Etik, her disiplin ve alan için oldukça tartışmalı bir konu olsa da (neyin etik olup olmadığı) evrensel değerleri yaratmak ve korumak üzere çeşitli kuruluşlar bu yönde çalışmalar ve düzenlemeler yapmaktadır. Etik alanında çeşitli prensipler ortaya koyan iki kuruluş; ACM Konseyi (ACM Council – Association for Computing Machinery) ve IEEE Kurumu (The Institute of Electrical and Electronics

Engineers, Inc)’nun önermiş olduđu prensiplere bakmak hangi deđerlerin dikkate alındıđı (alınması gerektiđi) hakkında bilgi vermektedir:

ACM Etik Kuralları/Prensipieri (<https://www.acm.org/code-of-ethics>):

Genel etik kuralları;

- Tm insanların programlamada esas itibariyle paydař olduklarını kabul edip toplum ve insan refahına katkıda bulunulmalı.
- Zarar vermekten kaçınılmalı.
- Drst ve gvenilir olunmalı.
- Adil olunmalı ve ayrımcılık yapılmamalı.
- Yeni fikirler, icatlar, yaratıcı çalışmalar ve bilgi iřlem programları retmek iin yapılan alıřmalara (emeđe) saygı gsterilmeli.
- Gizliliđe (zele, zel yařama, kiřisel haklara) saygı gsterilmeli.
- İnsan onuruna zarar vermekten kaçınılmalı.

IEEE Etik Kuralları/Prensipieri ([https:// www.ieee.org/documents/ieee_policies.pdf](https://www.ieee.org/documents/ieee_policies.pdf)):

- Halkın gvenliđini, sađlıđını ve refahını en st dzeyde tutmak, ahlaki dzenleme ve srdrlebilir kalkınma uygulamalarına uymak iin aba sarf etmek, halkı veya evreyi tehlikeye sokabilecek faktrleri derhal ifřa etmek.
- Mmkn olduđuanda, gerek veya algılanan ıkar atıřmalarından kaçınmak, ıkar atıřmalarından etkilenen tarafları konu hakkında bilgilendirmek.
- Mevcut verilere dayanak teřkil edecek řekilde yapılan iddia ve tahminlerde drst ve gereki olmak.
- Rřveti her biimiyle reddetmek.
- Akıllı sistemler de dhil olmak zere geleneksel ve geliřmekte olan teknolojilerin yetenekleri (yetileri, kabiliyetleri) ve sosyal sonuları hakkında bireyleri ve toplumu bilgilendirmek ve konunun anlařılmasını sađlamak.
- Sadece eđitimli ve deneyim sahibi olduktan sonra teknik yeterliliđi(mizi) korumak ve geliřtirmek iin bařkaları iin teknolojik grevleri stlenmek.
- Hataları kabul etmek, dzeltmek ve bařkalarının katkılarını dzgn bir řekilde deđerlendirmek iin teknik alıřmaları arařtırmak, kabul etmek ve drst eleřtirilerde bulunmak.
- Herkese adil davranmak; ırk, din, cinsiyet, engellilik, yař, milliyet, cinsel ynelim, cinsiyet kimliđi veya cinsiyete dayalı ayrımcılık yapmamak.

- Başkalarının mülklerine, itibarlarına zarar gelmesine sebebiyet vermekten kaçınmak.
- Meslektaşlarına ve iş arkadaşlarına mesleki gelişimleri için yardımcı olmak ve bu etik kurallara uymalarını desteklemek.

1.4 Sosyal Mühendislik ve Sektörel İlişkiler

Bilgi, bilişim ve teknoloji çağında disiplinler artık tek başına değil, birlikte ele alınarak çözüm üretme çabası içerisine yönelmektedir. İlk başlarda multidisipliner, sonrasında interdisipliner ve son olarak da transdisipliner olarak bu süreç devam etmekte ve bütüncü bir yaklaşım çerçevesinde çalışılmaktadır. SM de hiç bir zaman kendi içerisinde ayrı bir alan olarak değil diğer alanlarla iç içe değerlendirilmekte ve uygulanmaktadır. İster yapıcı ister yıkıcı olarak ele alınması bu şekilde değerlendirilmesi ve uygulanmasında bir değişikliğe yol açmamaktadır. SM ağırlıklı olarak medya, politika, pazarlama, sağlık, teknoloji gibi alanlarla iç içe geçmekte ve kullanılmaktadır. SM'nin bu alanlarla olan ilişkisi başlıklar altında aşağıda ayrı ayrı açıklanmıştır. SM'nin etkileşim gösterdiği alanlar bunlarla sınırlı olmamakla ve her geçen gün yeni alanlar bu listeye eklenmekle birlikte, konunun genel çerçevesinden uzaklaşılmasından dolayı bazı başlıklara burada özellikle yer verilmemiştir.

1.4.1 Sosyal Mühendislik ve (Sosyal) Medya

Güvenlik uzmanları, sosyal medya kullanımının yaygınlaşmasıyla birlikte, ciddi *hackerların* hedeflerini çevrimiçi araştırdığını ve insanların kendileri, arkadaşları ve sosyal ağlar üzerinde paylaştığı kişisel bilgi birikimlerini kullandıklarını belirtiyor. Facebook, Twitter ve bilinen diğer sosyal medya araçlarının bilgisayar korsanları için ana kaynak haline geldiğini, biraz araştırma yapılarak, e-posta adresleri, telefon numaraları, iş yeri, sosyal çevreler, favori hobiler, etkileşim şekilleri ve diğer ilgi alanları gibi bilgilerin kolayca bulunabildiğini ifade etmekte (www.tsys.com). SM'nin “medya” içerisinde birçok kullanım şekli vardır; belirli eğilimlerin öne çıkartılması, birçok olumlu ya da olumsuz görüşün birlikte (art arda) sunulması, çerçeveleme etkisi, propaganda, yönlendirilmiş ve içeriği önceden oluşturulmuş açık oturum konuşmaları, sansür vb.

Reklamlarda kullanılan sosyal mühendislik ise başlı başına ayrı bir konudur; reklamlar, SM'ye ait birçok aracın eş zamanlı (iç içe geçmiş şekilde) sergilendiği bir

mecradır. Medya, sosyal medya ve SM'nin olanakları birlikte kullanıldığında ortaya çıkan etkiden kaçmak neredeyse imkânsız bir hal almaktadır.

Sansür ise diğer önemli bir konudur. Özellikle günümüzde, bilgi çağında, bilgiye erişimin engellenmesi, ilgili konu/olay/içerik hakkında yanlış yönlendirmelere, eğilimlerin belirli bir yöne doğru kaymasına, manipülasyona, gerçeği gizlemeye, daha da kötüsü insanların olgulardan bihaber yaşamalarına sebebiyet vermektedir. Sansür, ister bilinçli ister bilinçsiz kullanılsın, tarafsız olmayı ortadan kaldırmakta ve olayların görülmesi, bilinmesi istenilmeyen yönlerinin karanlıkta daha çok kalmasına yol açmaktadır (ayın karanlık yüzü ya da madalyonun öbür yüzü gibi). Sansürün diğer ilginç bir özelliği ise yasaklama olarak algılanıp, yasak olan şeylere karşı istek ve arzunun artmasını, yasağın daha çekici hale gelmesini körüklemesidir. “Neredeyse istisnasız, yasaklanan bilgiye karşı gösterdiğimiz tepki o bilgiyi yasaklamadan önce istediğimizden daha fazla bir arzuyla istememiz şeklinde ortaya çıkar” (Ashmore, Ramchandra ve Jones, 1971; Wicklund ve Brehm, 1974; Worchel ve Arnold, 1973; Worchel, Arnold ve Baker, 1975; Worchel, 1992 Akt: Caldini, 2018, s. 325) . Medya ve özellikle sosyal medya SM'nin en geniş ve en etkili şekilde uygulandığı alanların başında yer almaktadır. Hem ikna kabiliyeti hem ulaştığı insanların sayısı açısından bakılacak olursa medyanın gücü yadsınamayacak bir boyuta ulaşmaktadır. Dijital çağ insanların sosyal kişiliklerini değiştirmede, fakat iletişim biçimlerini değiştirdi. Sosyal medya kullanılarak milyonlarca insana anında erişim sağlanmakta ve yeni etkileşim yolları kullanılmaktadır. Ancak sosyal medyada güvenlik riskleri de bulunmaktadır; sosyal mühendis tarafından dolandırıcılık, işyerlerine ait bilgi toplama, hassas bilgileri çalma vb. sosyal medya üzerinden gerçekleştirilmektedir (Tayouri, 2015, s. 1096).

İnsanlar sosyal varlıklardır, insanlar arasındaki ilişkiler ve konuşmalar insan doğasının bir parçasıdır. İnsanlar her zaman gruplar halinde yaşar ve ateş etrafında, şehir pazarlarında, *pub* 'larda veya kafelerde iletişim kurarlar. Dijital çağ bunu değiştirmede ama iletişim biçimimizi değiştirdi. Bugün birçok dijital iletişim yöntemimiz var; Facebook arkadaşlarla ve ailelerle iletişim kurmak, resim ve link paylaşmak vb. için kullanılmakta. Mikro bloglar için Twitter, anında mesajlaşma için WhatsApp, fotoğraf paylaşmak için Instagram ve videolar için YouTube, iş sosyal ağları için ise LinkedIn kullanılmaktadır. Ayrıca, bazı özel ihtiyaçlar için ya da

belirli gruplar için başka birçok site bulunmaktadır (Tayouri, 2015, s. 1097). Artık neredeyse tüm iletişim (fiziksel iletişim dışarıda tutulabilir) dijital paylaşımlarla gerçekleştirilmekte. İletişim kurduğumuz kişinin bize olan mesafesi durumu değiştirmemekte, bazen aynı ev içerisinde bile (odadan odaya) sosyal medya/dijital platformlar kullanılmaktadır. Bu tutum ve davranışlarımız bize şunu gösteriyor ki, SM konularına ait tüm girişim ve uygulamalar da ağırlıklı olarak sosyal medya üzerinden gerçekleştiriliyor ve SM-Medya ilişkisi her geçen gün daha belirgin bir hal alıyor.

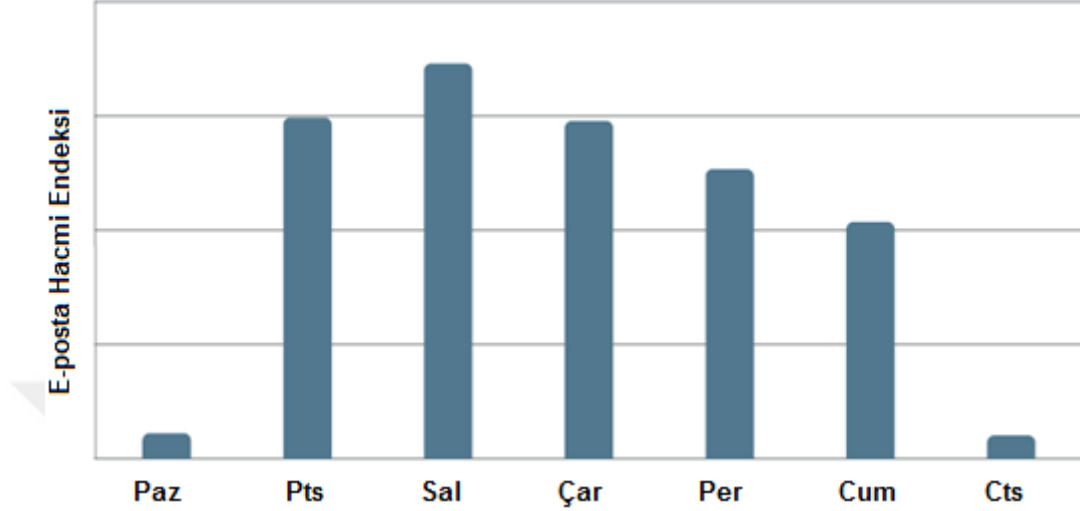
Brandtzaeg ve Heim (2009)'ın "Neden İnsanlar Sosyal Medya Sitelerini Kullanıyorlar" çalışmasına göre; sosyal medya kullanıcılarının %31'i yeni insanlarla iletişim kurmak, %21'i arkadaşlarıyla iletişimde kalmak ve %14'ü ise genel sebepleri olarak sosyalleşmeyi belirtiyor (Akt: Tayouri, 2015, s. 1097). %31 ile en büyük payı "yeni insanlarla iletişim kurmak" tercihi alıyor. Bu dikkat çekici bir yüzdendir (güncel yüzdenin daha da artmış olması muhtemeldir). İnsanlar artık yüz yüze değil sosyal medya aracılığıyla tanışmayı tercih etmektedir ve bu nedenle SM için sosyal medyanın ne kadar geniş, etkin ve (şimdilik) vazgeçilemez bir araç olduğu daha iyi anlaşılabilmektedir. Esas sorun ise sosyal medya üzerinden ne kadar çok kişisel, gizli, özel ve mahrem bilgilerimizin paylaşıldığının farkında olamayışımızdır. Diğer bir sorun ise paylaşmadığımızı sandığımız içerik ve bilgilerin aslında çevrimiçi ya da çevrimdışı ortamlarda ortalıkta dolaşıyor olmasıdır. Buna örnek olarak; kendimizin de içinde yer aldığı fotoğraflar, GPS koordinatları, bulut bilişimde tuttuğumuz (sakladığımızı sandığımız) veriler, ücretsiz depolama alanlarındaki dosyalarımız, e-posta içeriklerimiz, meta-datalar (üst-veriler), paylaşımların (sonradan üçüncü şahıslarla) paylaşılması, kişisel veriler, kalp atışımızın hızı, sağlıkla ilgili diğer veriler, yürüyüş rotamız, arabayı ne kadar hızlı/yavaş kullandığımız vb. veriler örnek olarak sıralanabilir.

The Human Factor Research Report (2016)'a göre 2015 yılında dünya genelinde yapılan araştırmalarda SM saldırılarına ilişkin bazı veriler şu şekildedir:

- Şekil 4'de tehlike içerikli e-posta saldırılarının haftanın günlerine göre dağılımı
- Şekil 5'de tehlike içerikli e-posta saldırılarının günün saatlerine göre dağılımı

- Şekil 6’da tehlike içerikli sosyal medya saldırılarının günün saatlerine göre dağılımı

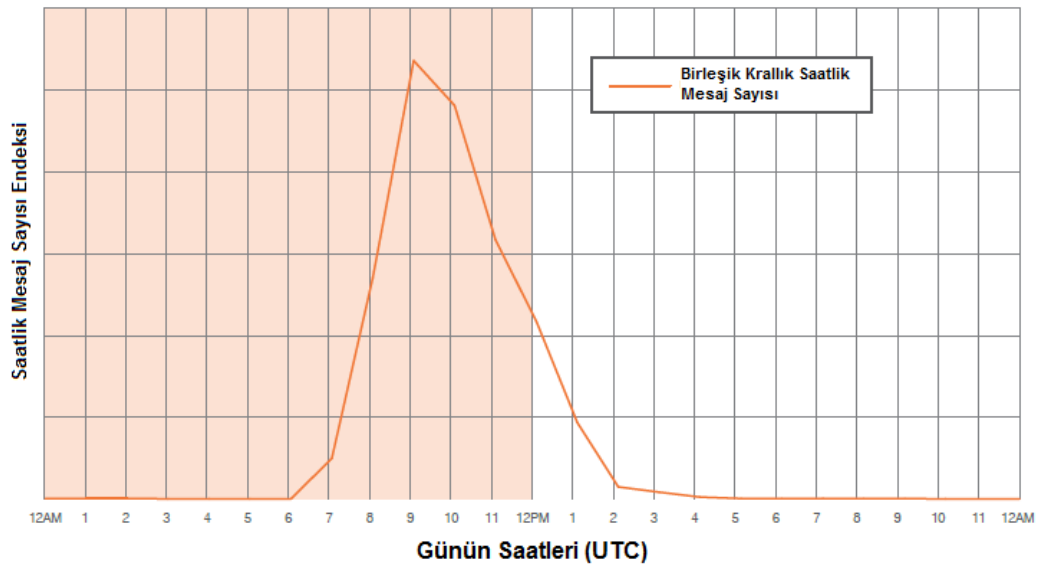
Şekil 4. Tehlike İçerikli E-Posta Saldırılarının Haftanın Günlerine Göre Dağılımı



Kaynak: The Human Factor (Research Report), 2016

2015 yılında yoğunluğun en çok haftanın ilk yarısında (Pazartesi'den Çarşambaya) yaşandığı, Salı günlerinde ise zirve yaptığı gözlemlenmiştir (2014 yılı için de benzer durum söz konusudur).

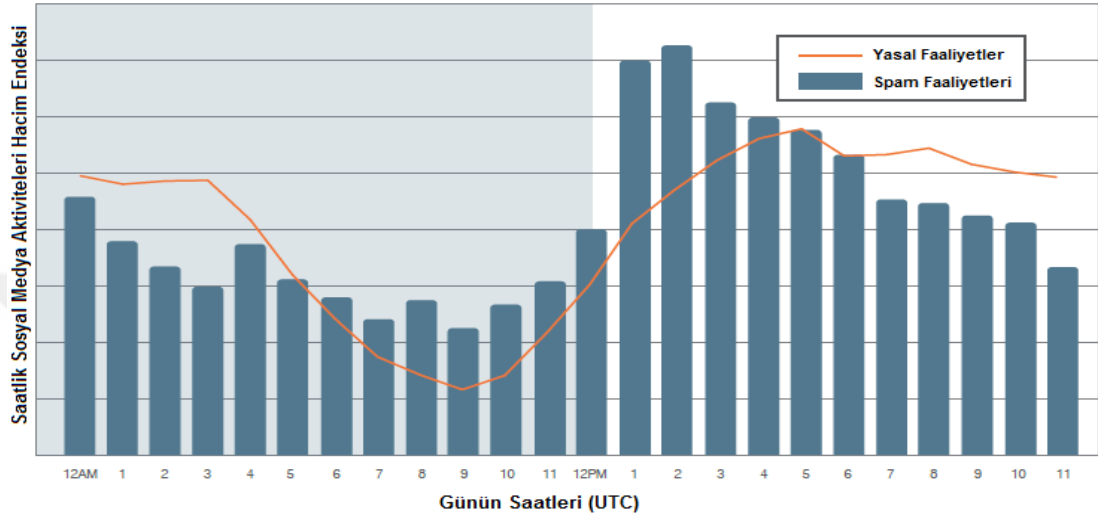
Şekil 5. Tehlike İçerikli E-Posta Saldırılarının Günün Saatlerine Göre Dağılımı



Kaynak: The Human Factor (Research Report), 2016

E-posta atakları yerel saatle özellikle günün erken saatlerini (09:00-10:00) hedeflemektedir. Buradaki amaçlardan bir tanesi de bilgi işlem çalışanlarının önleyici müdahale saatlerinden önce saldırı işleminin gerçekleştirilmek istenmesidir.

Şekil 6. Tehlike İçerikli Sosyal Medya Saldırılarının Günün Saatlerine Göre Dağılımı



Kaynak: The Human Factor (Research Report), 2016

Saldırganlar, etkinliklerini, hedeflenen mekânın en yoğun katılım saatlerine uyacak şekilde optimize etmektedirler. Organizasyonları hedef aldıklarında hem hedef kitleyi hem de saat dilimini dikkate almaktadırlar. Sosyal medya üzerinden gönderilen spamlarının/ataklarının en yoğun olduğu saatler sabah 08:00 civarında başlamakta ve öğleden sonra 2'ye kadar yaklaşık beş saat daha devam etmektedir. Bu durum, ABD'de iş günü boyunca giderek azalmaktadır. En yüksek aktivite süresi, insanların Facebook ve diğer sosyal medyada en aktif olduğu sabah saatinden öğle yemeğine kadar olan dilimde gerçekleşmektedir.

1.4.2 Sosyal Mühendislik ve Politika

Bir önceki başlık altında açıklanmaya çalışılan sansürün politikada kullanımı ise şu yönde cereyan edebilmektedir; uçlarda siyaset yapan siyasi grup üyeleri (politikacılar), en verimli strateji olarak popüler olmayan düşüncelerini propaganda etmek değil, bu düşünceleri sansürleyerek bu sansürü propaganda etmek yönünde kullanmayı tercih ederek (Cialdini, 2018, s. 326) *kendinden sansürü* çok etkili bir SM aracı olarak kullanabilmekteler.

SM-Medya, SM-Politika ilişkilerine kısaca göz attıktan sonra karşımıza “SM-Medya-Politika” üçlüsü çıkmaktadır. Çok sık karşılaştığımız bu üçlü, bireyleri ve toplulukları yönlendirme açısından oldukça etkili bir araç olarak sınırsızca hatta bazen fütursuzca kullanılabilir. Andrews (2017)’un *Engineering and Technology*’de yazmış olduğu yazıda bu konu şu şekilde ele alınmıştır: Bu Mayıs ayı başlarında, Facebook İngiltere’nin ulusal gazetelerinde ilanlar yayınlamaya okurlara sahte haberleri nasıl tespit edeceklerine dair bazı ipuçları verdi. Facebook daha önce bunun aynısını Fransa Cumhurbaşkanlığı seçimlerinde de yaptı. Fakat Facebook, ABD başkanlık seçimleri ve Avrupa Birliği’nin referandum oylamalarında aynı tavrı sergilemediğinden dolayı oldukça eleştiri aldı. Muhafazakâr Milletvekili Damian Collins, ABD seçimleri sırasında en iyi (doğru) 20 haber yerine 20 sahte haberin paylaşıldığını iddia etmektedir. Oxford İnternet Enstitüsü araştırmalarına göre Michigan eyaletinde çevrimiçi okunan haberlerin yaklaşık yarısı sahte haberlerden oluşmaktaydı. Onlarca sahte haber insanlara sunulmaktan çekinilmemişti. Bazen de yarısı doğru haber içerikleriyle de birçok konu ya da olay maskelenmişti. Beyaz Saray yarışı sırasında Hillary Clinton’ın DAES’e silah sattığı, Papa’nın ise Donald Trump’ı desteklediği yazılmıştı. AB referandumu sırasında ise İngilizlere, eğer AB’den ayrılırlarsa ülkelerinin 300 milyon Pound’luk bir tasarruf sağlayacakları söylenmişti.

Demokrasi, Abraham Lincoln’un “Tüm insanları bir süre kandırabilirsiniz, birtakım insanları sürekli kandırabilirsiniz, ama tüm insanları sürekli kandıramazsınız” prensibi üzerine kuruludur. Bir hükümet yozlaşmış ve insanların hayatını iyileştirmekten acizse, eninde sonunda yeterli sayıda vatandaş durumu idrak eder ve bu hükümetin yerine başkasını getirir. Ancak hükümetin medya üzerindeki kontrolü Lincoln’un mantığını boşa çıkarır, çünkü bu durum (hükümetin kontrolü) vatandaşların hakikatin farkına varmasını engeller. Medyayı tekeline alan oligarşi tüm başarısızlıklarını tekrar tekrar başkalarının üzerine atıp, dikkati hayali ya da gerçek dışı mihraklar üzerine çeker (Harari, 2018, s. 28-29) ve bu süreci mümkün olduğunca uzatıp durur, ancak ki başka bir sebepten dolayı işler çetrefilleşmeye başlayana değin.

Uygulamada, demokrasiler de SM kullanmaktadır. Buna karşın, demokratik bir hükümet, toplumda davranış için sınırlar oluşturmak için temsil ettikleri

insanların ortak ahlaklarını, değerlerini ve inançlarını yorumlamalı, mevzuat, iletişim ve sosyal pazarlama kampanyalarını kullanmalıdır. Toplumun değerleri ve inançlarının demokrasilerde ne anlama geldiği konusunda tartışmalar olduğu için, yasallaşma geliştikçe onlar da yavaş yavaş yerine oturur. Yazılı bir anayasa varsa, toplum bunu ortak inançları tartışmak ve kurmak ve mevzuat ihtiyacını belirlemek için bir referans noktası olarak kullanabilir (Emeraldinsight, 2015, s. 15).

1.4.3 Sosyal Mühendislik ve Pazarlama

Pazarlama sektöründe belirgin olarak karşımıza çıkma şekillerden bir tanesi “zaman ve sayı kısıtlaması”dır. Sınırlı sayıda olduğu ya da sınırlı bir süre içerisinde edinilebileceği/satın alınabileceği ileri sürülerek kullanılan bir taktiktir. Buradaki amaç, hedef/müşteri üzerinde psikolojik baskı yaratarak, hedefin belki de normal süreç içerisinde çok da istemeyebileceği (belki de hiç ihtiyacı olmayan) bir ürünü/hizmeti zaman ve sayı kısıtlaması baskısı altında kıymetli bir ürün/hizmet haline getirerek satışını gerçekleştirmektir. Mağaza vitrinlerinde zaman zaman gördüğümüz yazılar bu türdendir. Örneğin; “son 8 adet”, “son 3 gün”, “yarı fiyatına kampanyası için son hafta” vb. Bu taktiğin bir başka uygulama şekli de; “Müşterilere eğer hemen almak için karar vermezlerse, daha sonra aynı ürünü ya daha pahalıya almak zorunda kalacakları ya da hiç alamayacaklarının söylenmesi” (Cialdini, 2018, s. 315) şeklindedir.

SM özü itibariyle kötü değildir, ancak kötü amaçlı kullanımlara kolayca alet edilmektedir. Sosyal pazarlamanın SM tarafından kullanılan başka bir araç olduğu da iddia edilebilir. Bazı sosyal sorunların sistem genelinde müdahalelere ihtiyacı vardır. Pazarlamacılar, zaman zaman SM’ye el atarlar, ancak uygun bir etki düzeyinin ne kadar önemli olduğunu ve hangi sosyal pazarlamanın başarılabileceğini ve neyin başarılamayacağını bilmeleri gerekir. Kampanyalar ancak bu şekilde daha etkili hale gelebilmektedir. Halk, sosyal pazarlama ve SM arasındaki benzerlik ve farklılıkları net bir şekilde kavarsa, insanlar kendilerini etkileme girişimlerini daha iyi tanıyabilir ve davranışlarını şekillendirebilir. Pazarlamacılar sosyal pazarlamaya girdiklerinde, ait oldukları toplum üzerindeki etkisini göz önünde bulundurmaları gerekir. Kampanya o toplumun normlarına ve değerlerine uyuyor mu, yoksa toplumsal bir uyumu desteklemek ve propaganda yaratmak için mi hareket ediyorlar (Emeraldinsight, 2015, s. 16) bilmek gerekir.

1.4.4 Sosyal Mühendislik ve Sağlık

SM'ye etki eden medya okuryazarlığı ve teknoloji okuryazarlığı yanında bugünlerde sağlık okuryazarlığı gündemdedir. Sağlık okuryazarlığı hastalarla iletişimin daha güçlendirilmesi, hastaların sosyal medyayı sağlık hizmetleri açısından daha etkili kullanmasını ifade etmektedir. Bunun yanı sıra büyük ekonomik pazarlar oluşturan sağlık sektörü ve bu sektöre ilişkin alanlarda bireylere SM'nin çeşitli teknikleri kullanılarak çıkar elde amaçlı girişimlerde bulunmaktadır. Özellikle görsel basın ve sosyal medya üzerinden pazarlanmaya çalışılan çeşitli ürünler (spor malzemeleri, zayıflama ürünleri, çeşitli besin grupları, vitamin, bitkisel şifa adı altında satılmaya çalışılan onlarca ürün vb.) ortalıkta serbestçe dolaşmaktadır. Özellikle sağlık hizmeti veren kuruluşlara ulaşımın zor olduğu yaşam yerlerinde, entelektüel düzeyin daha alt seviyelerde olduğu kırsal kesimlerde (bu durum bazen entelektüel düzeyi yüksek olan insanların yaşadığı kent merkezleri için de geçerli olabilmektedir) ya da farklı farklı sebeplerden dolayı bu alana olan ilgiyi manipüle etmek isteyen ve SM tekniklerini çıkarları doğrultusunda acımasızca kullanan girişimlerin varlığının bilincinde olmak ve bu konularda kamuoyunu aydınlatmak gerekmektedir. Bu görev başta Sağlık Bakanlığı ve ilgili kuruluşlara düşmektedir. Ayrıca hastaya ait kişisel sağlık bilgilerinin korunması ve güvenli bir şekilde tutulması da çok önemlidir. Bu alan her ne kadar bir sonraki Bölümde anlatılacak olan BG'nin konusu olsa da, sağlık alanındaki bu kişisel bilgilere ulaşım ve onları farklı niyetlere aracılık etmesi için kullanma girişiminde bulunanların, SM tekniklerinden yararlandıklarının kamuoyuna hatırlatılmasında fayda bulunmaktadır.

1.4.5 Sosyal Mühendislik ve Teknoloji

Kamuya açıklanmış birçok siber saldırıdaki SM yaygınlığı, mağdurların kötü niyetli iletişimleri ayırt etme kabiliyetinde doğal bir zayıflık olduğunu ya da siber suçluların “insan duvarını” aşmak için daha karmaşık yöntemler kullandıklarını göstermektedir. Temel neden ne olursa olsun, ilk savunma hattının açıkça başarısız olduğunu görebiliyoruz. Daha da önemlisi, ihlalleri için kullanıcıları basitçe suçlamak tamamen adil değil. Açıkçası güvenli olmayan kullanıcı davranışının birçok örneği vardır; saldırganların genellikle hedeflerinin bilincini atladığını ve onları manipüle ettikleri görülmektedir (Samani ve McFarland, 2015, s. 5).

SM'nin teknoloji ile olan ilişkisi diğer alanlara göre oldukça belirgindir ve

daha öne çıkmaktadır. Bunun en önemli gerekçesi, her iki alanın da etkileşimli bir şekilde yoğun olarak kullanılıyor olmasıdır. SM çoğu zaman yalnızca insan faktörünü (ve zayıflığını) kullanarak ataklar yapsa da çoğu zaman bu ataklarda kullanılan araçlar teknolojinin çeşitli uzantılarından oluşmaktadır. Halen insandan insana ataklar ağırlıklı olsa da teknolojinin avantajları, zaman ve mekân konusunda çeşitli fırsatlar sağlaması ve hedef kitlenin dijital ortama yoğunlaşması (sosyal, ekonomik, kültürel, iletişim, seyahat vs.) ve benzeri nedenlerle SM uygulamaları bu platforma doğru kaymaktadır. Yoğunlaşmanın bu platformda gün geçtikçe daha fazla kümeleneyeceği şimdiden görülebilmektedir. Bu çalışmada “Sosyal Mühendislikle Etkileşimli Kavramlar” başlığı altında yer alan *teknoloji okuryazarlığı* konusu bu paragrafta açıklanmaya çalışılan sebeplerden dolayı da ayrıca önem arz etmektedir.

Siber saldırılara karşı yeni önlemler almak üzere çok büyük bütçeler ayrılarak yeni güvenlik yatırımları gerçekleştirilmektedir. Oysa insan faktörüne (insan kaynaklarına) aynı yatırım söz konusu değildir. Bu durumun farkına varan siber saldırganlar gözlerini SM alanına dikmiş durumdadır. Son zamanlarda basında yer alan bazı yazılarda bu duruma gönderme yapan “siber saldırganların yeni kısıkaçı sosyal mühendislik” (<https://www.dunya.com>) vb. başlıklara sıkça rastlanılmaktadır.

1.5 Sosyal Mühendislik Araçları ve Çıktıları

SM atakları bilişim teknolojileri (daha ziyade yazılım tabanlı) ve psikolojik (duygu-his-davranış) tabanlı olmak üzere iki farklı şekilde uygulanmaktadır. Bazı durumlarda (SM’nin daha etkin kullanımı için) her iki yöntem birlikte kullanılabilir. Bu bölümde her iki alandan da bahsedilerek örneklerle açıklanmaya çalışılacaktır.

Her suçta olduğu gibi, SM gibi bir anti-sosyal davranış için altta yatan bazı nedenler vardır. Bu sebeplerden bazıları şunlardır (Okeyni ve Owens, 2007, s. 3):

- **Finansal Kazanç:** Pek çok nedenden dolayı, bir kişi SM ile uğraşması için finansal olarak baskı altında olabilir. Örneğin, arkadaş ya da aile baskısı.
- **İntikam:** Kişisel nedenlerden dolayı, bir birey, bir arkadaşını, meslektaşını, bir kurumu, eski işvereni bencil arzularını yerine getirmek için hedef almaya karar verebilir.

- **Kişisel Sebepler:** Bir birey, kişisel kazanç kayıtlarını değiştirmek veya bir arkadaşının, ailesinin veya iş arkadaşının taleplerinden dolayı SM faaliyetleriyle bir sisteme veya bilgiye erişmek isteyebilir.

SM’de kullanılan araçlar sonsuz sayıda olmasa da sanılanın aksine oldukça geniştir. Hedefteki kişinin güvenini kazanmaktan onu korkutmaya, manipüle etmeye kadar birçok yöntemi içerebilmektedir. Bu araçlardan bir kısmı Tablo 2’de verilmiştir. SM kullanımında psikoloji, psikiyatri, antropoloji, sosyoloji, işletme, iktisat gibi birçok disiplinin gerçekleştirmiş olduğu çalışmalardan yararlanılmaktadır. Örneğin, iktisat biliminde *az bulunurluğu* (zaman ve mekâna göre değişiklik gösterebilmektedir) ifade eden *kıtlık prensibi* (scarcity) -sınırlı talebe karşı kaynakların sınırlı kalması-, “insanlara ihtiyaç duydukları veya istedikleri bir şeyin sınırlı miktarda olduğu ve onu elde etmek için belirli bir tutum ya da eyleme riayet etmeleri söylendiği zamanki durum” (Hadrnagy, 2017, s.33) karşısında, insanları belirli bir davranışı göstermesi/sergilemesi için yönlendirme yapmada güçlü bir araç olarak kullanılabilmektedir. İnsanların kıt olan bir şeyi talep etmeleri/istemeleri/arzulamaları çok rastlanan bir durumdur. Bu durumu bilen politikacılar, satış elemanları, pazarlamacılar, mücevher satıcıları da bunun gücünden sık sık yararlanmaktadır.

SM’de başlangıç noktası hedef kişi ya da kurum hakkında her türlü veri/enformasyon/bilgiyi toplamak, onları sınıflandırmak, portföy oluşturmak, boşlukları doldurmak, ilişkilendirmek ve raporlamakla başlar ve bu süreç kurgu ve atakla devam eder. Bilgi toplama çok geniş bir alandır; bunun içerisine ayaküstü sohbetten aile fotoğraflarına bakmaya, sosyal medya hesaplarını kontrol etmekten çöpleri karıştırmaya, yayımlanmış açık raporları okumaya kadar uzanan geniş bir yelpaze söz konusudur (kişiler ya da kurumlar hakkında küçük veriler büyük verilere bu şekilde dönüşebilmektedir). Bilgi toplamada gözlem gücünü kullanmak çok önemlidir (bu sayede ilişkilendirme ve büyük resim kurgulanabilmektedir), aslında dedektiflerin de yaptıkları budur. Kişi ya da kurumlar hakkındaki (ilk başta bize çok basit ve önemsiz gibi gözükebilen) gözlemler bir araya getirildiğinde inanılmaz derecede geniş bir bilgi havuzu oluşturulabilmektedir. Örneğin, hedefin sigara içip içmediği, kurumda sigara içmek için bir bölümün ayrılıp ayrılmadığı, girişlerde şifre/parmak izi/kartlı geçiş teknolojilerinin hangisinden yararlanıldığı, misafirlerin

herhangi bir yaka (ziyaretçi) kartına ihtiyaç duyup duymadığı, kargo teslimatlarının direk kişiye yapılıp yapılamadığı, güvenlik kameralarının olup olmadığı, varsa yerlerinin tespiti, çöplere (çöp kutularına, bidonlara) erişimin olup olmadığı, ne tür bilgilerin (evrak, CD, dosya, kartvizit, mektup, fatura vb.) çöpe atıldığı, evrak imha cihazının kullanılıp kullanılmadığı, kullanılıyor ise bunun yalnızca dikey kesim yapan (basit, sıradan) bir cihaz mı (bu şekilde biraz vakit harcayarak çok kıymetli evraklar tekrardan okunabilir hale kolayca getirilebilmektedir) yoksa daha gelişmiş bir cihazla mı yapıldığının tespiti, temizlik elemanlarının içeriden mi yoksa dışarıdan bir şirketten mi kiralandığı, bu kişilerle temasın zorluk düzeyi ve onların erişim gücü. Örneğin otellerdeki temizlikçilerde her kapıyı açan bir anahtarın (golden key) bulunması vb. Bunlar arasında “çöp karıştırıcılığı”na bir başlık açmakta fayda vardır:

Çöp Karıştırıcılığı: İnsanlar ya da kurumlar hiç de azımsanmayacak kadar bir bilgiyi çöp kutularına atmaktadır. Bunlar, gerektiği gibi imha edilmezlerse (bazen imha edildiği düşünülen belge, CD, usb bellek, harddisk’ler bile basit müdahalelerle geri kazanılabilmektedir) soysal mühendislere, ya da çok daha kötü niyetli olan saldırganlara büyük fırsatlar yaratılmış olur. Bir kişinin çöp kutusundan elde edilecek şeyler, o kişi hakkında ne kadar bilgi toplanabileceği hakkında şaşırtıcı düzeyde veriden, hatta direk bilginin kendisinden oluşabilmektedir. Yiyecek, yemek, mutfak atıkları, poşetler, kutular, ambalaj ve paketlerden elde edilecek veriler kişinin nasıl beslendiği (sağlıklı-sağlıksız, ev yemeği-dışarıdan sipariş, dışarıdansa nereden ve ne yediği vb.), neleri sevdiği, nerelerden alış veriş yaptığı, harcadığı para miktarı, ekonomik durumunu genel olarak gösterebilir. Yine aynı şekilde, kullanıp atmış olduğu ilaç kutularından hangi hastalıklardan muzdarip olduğuna kadar sınırsız sayıda bilgi elde etmek mümkündür.

İnsanlar duydukları haber/bilgi/dedikodu türünde (eşdeğer olduğunu düşündüğü) karşı bilgi vermeyi/aktarmayı tercih etmektedir. Bu bir bakıma borçlu kalmama, “iyiliğe iyilikle karşılık verme” ya da denge kurma, karşılıklı güven teyit etme içgüdüsüyle yapılmış bir davranış olarak bilinmektedir. Görgü tanıklıkları, zanlılarla yapılan pazarlıklar da bu türden alışverişlere örnek olarak gösterilebilir (bilgi ver - bilgi vereyim, iyilik yap - iyilik yapayım). Karşınızdakinden ne tür bir konuda bilgi edinmek istiyorsanız, benzer bir konudan söz etmek ya da bilgi/haber vermek (bu bazen dedikodu şeklinde de gerçekleşebilmektedir) -gerçek ya da

uydurma fark etmez- etkili bir yöntem olabilmektedir. Sosyal mühendisler özellikle iletişim kurmak istedikleri kişilerle yakınlık kurmak için onların işine yarayabileceğini düşündüğü bir bilgiyi benzer bir bilgi almak için karşılıklılık ya da borçlu kalmama ilkesini gözeterek verirler. Karşılığında büyük bir ihtimalle benzer değerde bir bilgi edinirler, bazen daha da fazlasını. Sahlins (2016, s.192-202)’e göre “Karşılıksız olarak verilen hediye ile hile arasında yer alan çeşitli karşılıklılıklar bir sosyallik yelpazesi oluşturur. Bu yelpazenin bir ucunda bir başkası için fedakârlık yapmak yer alırken, diğer ucundaysa bir başkasının sırtından kazanç sağlayan bencilce davranış yer alır”. “Karşılık verme, bir ihtiyaç onu daha acil hale getirene dek gerçekleşmeyebilir; verilen karşılık mutlaka ilk iyiliğe eşdeğer olmak zorunda değildir ve maddi akış uzunca bir süre şu ya da bu tarafın lehine dengesiz biçimde sürebilir”.

Sosyal mühendislerin, hedeflerindeki kişilerden daha fazla bilgi alabilmek için kullandıkları bir diğer yöntem ise onları övmektir; yaptıkları işlerde ne kadar başarılı olduklarını bildiklerini, isimlerini birçok defa duyduklarını, bu konuda insanların onları ne kadar takdir ettiklerini, hatta otorite sayılabilecekleri gibi sözlerle yakınlık kurabilmekte ve hemen ardından (övgüde bulunulan kişiler buna bir tür teşekkür karşılığı verme hissi içerisinde) çeşitli bilgiler edinebilmektedirler.

Diğer bir yöntem, kişilerin kendilerinden ve yaptıkları işlerden bahsetmekten hoşlandığını bilmekten geçmektedir. Hedefteki kişi (eğer yeterli bir donanıma sahip değil veya bu konuda çeşitli bilgilendirme ve eğitim almamışsa) ilk önce kısıtlı bilgiler vermeye ama sosyal mühendis tarafından birkaç manevra sonrasında (evet bu bahsettiğiniz şeyler genel olarak bilinen bilgiler, ama eminim ki siz çok daha derin ve önemli bilgilere sahipsinizdir, bu bilgiler ancak sizin kadar başarılı insanlarda vardır. vb.) daha çok ve detaylı bilgiler vermeye başlayabilir.

SM’de kullanılan bir başka yöntem ise, her zaman tüm bilgilerin yalnızca tek bir kişiden ya da tek bir kaynaktan gelmeyeceğini iyi bilmektir. Herhangi birisinden ya da bir yerden edinilmiş bilgi kırıntısı doğru şekilde kullanılabilirse başka bilgi kapılarının kilidini açabilir. Bu tür saldırılarda bilgiler bir yapboz’un parçalarıymışçasına toplanır, bir araya getirilir. Örneğin, yetkili birisinin şu an nerede olduğu bilgisine sahip olmak (başka bir toplantıda, yemekte, tatilde, iş gezisinde) o kişinin sekreteriyle iletişime geçmeyi ya da ondan bir şey talep etmeyi

kolaylaştıracaktır. Örneğin; (teknik ekipten biri gibi davranarak bir sekretere) “Müdürünüzün şu an toplantıda olduğunu ve çok yoğun olduğunu biliyorum, bana toplantı süresince odasının müsait olacağını ve benim bu esnada bilgisayarındaki problemi çözmemden çok memnun kalacağını, bu şekilde zamandan da tasarruf edeceğini bildirdi. Sizden ricam beni müdürünüzün odasına kadar götürmeniz, eminim sorunun çözülmesinden çok memnun kalacaktır...” Bir bilgi bir başka bilginin ifşasında ya da davranışın icrasında kolayca araç olarak kullanılabilir.

“İnsan davranışının bilinen bir ilkesine göre birisinden bize iyilik yapmasını istediğimizde bir sebep sunarsak başarılı olma şansımız daha yüksektir” (Cialdini, 2018, s. 24). Cialdini, Langer’ın bu durumu şu örnekle açıkladığını ifade etmektedir; kütüphanede fotokopi sırasında arkalarda beklerken, sıradaki insanlara “Afedersiniz, beş sayfa kadar fotokopim var, fotokopi makinesini kullanabilir miyim?” dediğinde yalnızca %60 oranında olumlu yanıt alabilirken, “Afedersiniz, beş sayfa kadar fotokopim var, fotokopi makinesini kullanabilir miyim? *Çünkü acelem var da...*” dediğinde ise olumlu yanıt oranı birden %94’lere çıkmıştır.

Doğru mekân ve zamanlama da bir sosyal mühendisin ustalıklı kullandığı bir araçtır. Tahmin edilebileceği gibi yoğun, kalabalık ve acil bir işin ortasında, haftanın ilk mesai gününde (Pazartesi Sendromu) SM bağlamında rahatça iletişime geçebilmek ve bilgi edinmek çok kolay olmayacaktır. Sakin bir ortam ve haftanın son mesai günü ve saatleri daha iyi bir tercih olabilir. Bu durumla çelişkili gibi görünse de bazen insanlara karşı, hiç hoş olmayan bir davranış olsa da, aşırı ısrarcı olmak (aynı şeyi tekrar tekrar sorup, istemek) -hedef ısrarlardan bıkip yorulabilir ve bir an önce maruz kaldığı bu durumdan/baskıdan kurtulmak isteyebilir- işe yarayabilmektedir. Bu davranış şekli ilk tercih edilen yöntem değildir, ancak seçenekler tükendiğinde ya da duruma göre kullanılabilen bir yöntemdir.

SM’de kapalı uçlu sorular hedefteki kişiyi daha dar bir alana sokarak sonuca net ve hızlı adımlarla ilerleme imkânı vermekle birlikte risklidir de; konuşmanın tıkanmasına veya hedefteki kişinin rahatsız olmasına sebebiyet verebilir. Bu nedenle, sorular doğrudan değil, sohbet havasında ve açık uçlu olmalıdır. Evet ya da Hayır’dan ziyade, nasıl, nerede, ne zaman, kiminle gibi cevaplar daha çok işe yaramaktadır.

Bir diğ er ara ise, karřılıkt a bulunma ilkesidir. Bu ilkeye g re bize yapılanın aynısını karřı tarafa yapmak isteriz. Bir yardım, iyilik g rd ysek (bir anlamda borlandıysak) iyilik ve yardım yapmak isteriz, biri bizi yemeğ  davet ettiyse onu yemeğ  davet ederiz, hediye aldıysak hediye veririz vb. Sosyal m hendisler k  k iyilikler (borlandırma) yaparak k  k iyilikler (karřılıklar) bekleyebilirler. Bu ilke toplumsal bir kural gibi alıřtığ ndan “Bir bařkasının itaat etmesini saėlamak iin kullanılması n sebeplerinden biri de g c d r. Normalde reddedilecek taleplere, var olan borluluk hissi sayesinde ‘evet’ cevabı verdirebilecek b y k bir g c  vardır. Genelde sevmediğ miz kiřiler, davetsiz satıř temsilcileri, sevimsiz akrabalar, garip ya da bilinmedik firma temsilcileri taleplerini s ylemeden  nce bize k  k bir iyilik yaparak isteklerini kabul ettirme řanslarını olduka artırabilmektedir” (Cialdini, 2018, s. 49-50).

Sosyal m hendisler “kartvizit”in g c n  de ok iyi bilir ve kullanırlar; kartviziti, hedefi y nlendirmek veya ikna etmek iin uėrařılan onca zaman ve dakikayı bir anda “resm  olarak teyit eden” bir belge, bir kimlik gibi g r rl r. 15-20 TL  deyerek bastırılabilen, hatta evdeki/ofisteki renkli yazıcıdan kolayca hazırlanabilen (isteğ  g re d zenlenmiř) kartvizitler kolayca ve oğ  zaman sosyal m hendislerin “geiř kartı” olurlar.

Hedefteki kiři gibi d ř n p konuřup davranmak yani onu anlamak, onun gibi davranmak insanları ikna etmenin diğ er bir yoludur. Sosyal m hendisler bu konuyu ok iyi bildikleri iin hedefleriyle eř g d m ierisinde davranmaya  zen g sterirler, bu davranıř řekli hedefi rahatlatır ve istekler karřısında hedef daha olumlu tepkiler vermeye bařlar. Aynı ses tonunu kullanmak, benzer el kol hareketleri yapmak, ortak y z ifadeleri takınmak, benzer oturuř řekilleri, yani kısacası, senkronize olmak bu s rete kullanılan diğ er bir aratır.

Sosyal m hendislerin hedefleriyle iletiřim kurabilmelerinde aracılık eden diğ er bir ara ise *mikro-ifadeler*’dir. Mikro-ifadeler;  fke, iğrenme, korku, neře,  z nt  ve řařkınlıktır (daha sonra bu guruba k  mseme de eklendi). Dr. Ekman tarafından insanların duygularının/hissettiklerinin y z ifadeleri aracılığ yla yansıtılması alıřmaları olan Y z Hareketi Kodlama Sistemi’ne (Facial Action Coding System), 1970’lere dayanmaktadır. Hadnagy (2017, s. 130), Dr. Ekman’ın alıřmalarından hareketle, mikro-ifadelerin alıřma tekniğinin ř  řekilde olduėunu

belirtiyor; “Mikro-ifadeler, kolayca kontrol edilemeyen ve duygulara verilen tepkide meydana gelen ifadelerdir. Bir duygu yüzde bir takım kas tepkilerini tetikler ve bu tepkiler bazı ifadelerin ortaya çıkmasına neden olur. Çoğu zaman bu ifadeler, saniyenin yirmi beşte biri kadar kısa sürer. Bunlar, duygusal bir karşılık nedeniyle ortaya çıkan istemsiz kas hareketleri olduklarından, kontrol edilmeleri neredeyse imkânsızdır”. Mikro-ifadeleri doğru okumada kendini geliştiren sosyal mühendisler hedefle senkronize hareket edip edemediğini, doğru yolda ilerleyip ilerlemediğini hedefin haberi olmadan, sessiz bir doğrulama aracı olarak kullanabilmektedir.

Dr. Paul Ekman, yedi farklı temel duygu tanımlamaktadır: Bunlar; öfke, iğrenme, korku, sevinç, üzüntü, şaşkınlık ve küçümseme. Şekil 7’de Tim Roth’ın “*Lie To Me*” serisindeki Cal Lightman rolündeki performansından, bu duyguların altısına dair bir örnek verilmiştir (Henningesen, 2013, s. 10):

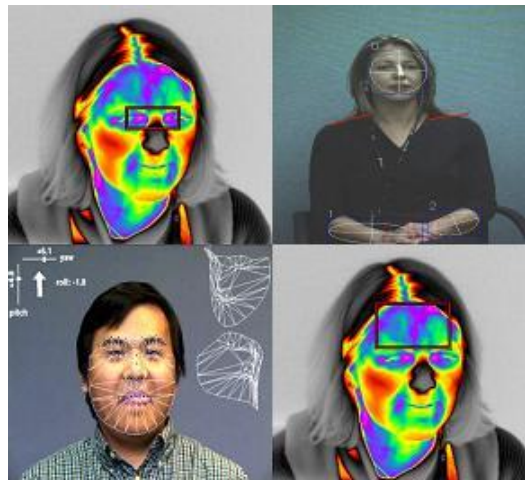
Şekil 7. Tim Roth’un “*Lie To Me*” İsimli Dizide Cal Lightman Rolünde Göstermiş Olduğu Mikro-İfadeler.



Kaynak: Henningesen, 2013, s. 11

Homeland Security Department, mikro-ifadeler temelli çalışmaları daha da geliştirerek güvenlik önlemlerine yeni bir proje olarak entegre etme çabalarını sürdürmektedir. Birleşik Devletler Milli Güvenlik Departmanı (Homeland Security Department) “*Aldatmayı Algılama: Düşmanca Niyeti Belirleme - Project Hostile Intent*” isminde bir proje üzerinde çalışmaktadır. Projeye ilişkin bir ekran görüntüsü Şekil 8’de verilmiştir. Bu projenin amacı ülkeye giriş yapan insanlar (2007 verilerine göre yıllık 400 milyon insan giriş yapmaktadır) arasından Birleşik Devletlere ve vatandaşlarına karşı düşmanlık niyeti barındırabilecek bireyleri tespit etmektir. Bilinen (veri tabanlarında kayıtlı) teröristleri tespit etmek için parmak izi, iris ve yüz taramaları dâhil olmak üzere birçok biyometrik önlemler alınsa da geçmiş iz bilgileri bulunmayanları tespit etmek için neler yapılabilir sorusuyla yola çıkan bu proje müdahalesiz sensörleri kullanarak gerçek zamanlı olarak, aldatma ve düşmanlık niyetini belirleme konusunda girişimler içeriyor. *Project Hostile Intent* isimli bu proje iki bileşenden oluşmaktadır; birincisi, davranışsal ve konuşma ipuçlarına odaklanma (bunun için operasyonel temelli senaryolardan türetilen deneylerden yararlanılmakta), ikincisi ise, invaziv olmayan sensör ve algoritma paketleridir. Entegre olarak çalışan bu bileşenler ipuçlarını otomatik olarak algılamakta ve izlemektedir. Projenin program yöneticisi Larry Willis, bu teknolojinin, sınırlar ve kritik altyapı için erişim kontrolünü destekleyen tarama ve görüşme sürecinde devrim yaratma potansiyeline sahip olduğunu belirtmektedir (U.S. Department of Homeland Security, 2019).

Şekil 8. Project Hostile Intent (Tehdit Algılama)



Kaynak: <https://www.dhs.gov/science-and-technology/deception-detection>, Erişim: 01.02.2019

Sosyal mühendisler hedefteki kişinin doğru bilgiler vermesini sağlamak amacıyla onlar üzerinde bir miktar rahatsızlık duygusu yaratmaya/oluşturmaya çalışırlar; direk göz teması kurmak (doğru uygulanmadığında rahatsızlık veren bir sürece dönüşebilir, birkaç saniyeden uzun sürmemelidir), kolları çapraz bağlamak, postür olarak dik durmak, tonlama vb. Rahatsızlık vermeyecek kadar bir miktar baskı kuracak düzeyde kullanılan bu araçlar, hedefte, kendisinin kontrol altında olduğu ve yalan söylerse bunun anlaşılacağı endişesini yaratacaktır ve bu sayede yönlendirilmeye daha açık konuma gelecektir.

Fiziksel iletişim kurma aşamasında “koku”nun etkisi de oldukça yüksektir. Koku fenomeni her ne kadar karmaşık bir konu ve kişisel tercihlerin söz konusu olduğu bir alan olsa da, “kötü kokuyu” herkes bilir ve ondan uzak durmaya çalışır. Sosyal mühendisler bu aşamada birçok kişinin beğenebileceği kokular kullanmasını bilir ve onun gücü sayesinde hedeflerine daha kolay yaklaşır.

Araştırmalar fiziksel çekiciliği daha fazla olan iyi görünümlü insanların daha kolay iş bulabildiklerini, bulduğu işlerde daha fazla ücret alabildiklerini, taleplerini daha kolay gerçekleştirebildiklerini (olumlu cevap aldıklarını), suç işlediklerinde jüri tarafından daha az suç isnat edildiğini, para cezasında da yine benzer suç işleyenlere oranla daha az cezaya çarptırıldıkları göstermektedir: Yapılan bir işe alma canlandırma çalışmasında -işe almada görevli olanlar her ne kadar aksini iddia etseler de- daha iyi görünümlü adayların tercih edildiği gözlemlenmiştir (Mack ve Rainey, 1990 Akt: Caldiani, 2018, s. 230). Bu tutumun yalnızca işe alma süreçleriyle sınırlı olmadığını, çekici olan çalışanların çekici olmayan çalışanlara oranla %12-14 civarında daha fazla ücret aldıklarını (Hammermesh ve Biddle, 1994 Akt: Caldiani, 2018, s. 230) yapmış oldukları çalışmalarda gözlemlediklerini ifade etmektedirler. “Ayarlanmış” bir ihmal davasında ise, kurbanından daha iyi görünümlü olan sanıklar, kurbanın daha iyi görünümlü olduğu durumlarda %50 daha az para cezasına çarptırılmışlardır. Jüride bulunan hem erkek hem kadın üyeler bu çekiciliğe bağlı taraf tutma davranışını sergilemişlerdir (Kukla ve Kessler, 1978 Akt: Cialdini, 2018, s. 231). Bu durum, daha az çekici olanların SM’yi uygulamayacağı anlamında yorumlanmamalıdır ama son yıllarda (kötü niyet ve amaçları olan kişi veya grupların sosyal mühendisliğin sınırlarını da zorlayacak düzeyde) terör ve topluma yönelik düzenlenen olaylarda, daha çekici fiziksel özelliği olan, iyi görünümlü (bazen iyi

giyimli) kişilerin kullanıldığı bilinmektedir. Her nedense tehlikenin daha çok, daha az çekici olanlardan geleceğine yönelik duygularımız bulunmaktadır. İnsanların bu tutumları sosyal mühendislerin işini kolaylaştırabilmektedir.

Kazanmak yerine, kaybetmekten kaçınma duygusu çok daha güçlü bir duygudur (eldeki bir kuş, ağaçtaki iki kuştan iyidir). Cialdini (2018, s. 311) bu konu hakkında “insanlar için bir şeyi kaybetmek aynı değerde bir şeyi kazanmaktan daha fazla motive edicidir” demektedir. Doktorların sigara içenlere yazdığı (ya da gönderdiği broşürlerde) yazılarda, eğer sigara içmeyi bırakmazlarsa hayatlarından kaç sene gideceğini anlatan mektup, sigarayı bırakırlarsa kaç sene kazanacaklarını anlatan mektuptan daha etkilidir (Wilson, Kaplan ve Schneiderman, 1987; Wilson, Purdon ve Wallston, 1988 Akt: Cialdini, 2018, s.312). Statükoyu (mevcut durumu) koruyup, değişime karşı mukavemet gösterme eğiliminde de benzer duygular söz konusu olabilmektedir. Bu çıkarımdan hareketle, özellikle örgütsel değişimlerde, değişime direnci kırabilmek için, çalışanlara, bu değişimi uyguladıklarında neler kazanacakları yerine, uygulamazlarsa neleri kaybedecekleri anlatılabilir.

SM araçlarını ve çıktılarını makro açıdan incelemek gerekirse Tablo 4’de düzenlemiş olduğumuz tabloda yer alan listeyi çok daha geniş bir şekilde uzatmak elbette mümkündür. Örneğin; web sitesi klonlama uygulamaları. Bu uygulamalar sayesinde herhangi bir web sitesi olduğu gibi bilgisayara indirilebilir. İndirilen bu web sitesini çevrimiçi taklit site haline getirmekse oldukça basittir. Bu sayede bir harf değişikliği ya da belirleyeceğiniz herhangi bir linkten bu siteye yönlendirme yapılarak birçok hedef hakkında bilgi toplanabilir. Bu işlem öylesine inandırıcı olabilmektedir ki, hedefteki kişi(ler) resmi bir web sitesinden alışveriş yaptığını düşünebilir. Diğer bir araç ise, hedefteki kişinin telefonunda gözüken (arayan) numaranın sosyal mühendisin belirlediği bir numara (hedef için ilgi çekebilecek bir numaradır bu; tanıdığı birinin, bir kurumun, resmi bir işyerinin, okulun telefon numarası gibi) olmasıdır. Bunu sağlayan uygulamalara ulaşmak da oldukça kolaydır. Genellikle bu işlemle eş zamanlı kullanılan diğer bir uygulama da ses değiştirme programlarıdır (bu sayede hem kimlik korunmuş olabilmekte, hem de genç, yaşlı, çocuk, kadın, erkek vb. sesleri elde edilebilmektedir).

Tablo 4. Sosyal Mühendislik Araçları ve Çıktıları

Araçlar (Tools)	Çıktılar (Outputs)
Güvenini kazanma	Bazı teknik bilgiler elde etme
Korku/Kaygı yaratma	Enformasyon
Acındırma	Zayıf yönlerin tespit edilmesi
İyilik yapma arzusunu tetikleme	Giriş kodları gibi özel bilgilerin edinilmesi
Kanıt gösterme	Hassas bilgiler toplama
İkna etme	Yönetme/yöneltme
Çerçeveleme etkisi	İçeride tanıdık birisinin (onaylama, tasdik vb. için) bulunması
Toplumsal kanıt	Gelecekte yardım almak için ilişki kurma (zemin hazırlama)
Manipülasyon	Atlama taşı olarak kullanma
Yönlendirme	İçeriden yardım alma
Kıtlık prensibi	
Çekicilik (fiziki)	
NLP	
Borçluluk duygusu yaratma, yardım etme, iyi davranma, hediye alma vs.	

SM'nin karakteristik yapısı (özellikleri) ve çıktıları. Greitzer, Strozer, Cohen, Moore, Mundie ve Cowley tarafından Tablo 5'de gösterildiği şekilde sınıflandırılmıştır (Akt: Allen, Jain, Tailang, Goswami, Dutta, Sankhla, Kumar, 2016, s. 97).

Tablo 5. Sosyal Mühendislik'in Karakteristik Yapısı

Göze Çarpan Özellikler	İstenen (Talep Edilen) Tipik Bilgiler	Olası Sonuçlar / Çıktılar
Dikkat çekme - Genellikle iyi ya da kötü haberler - Aciliyet duygusu (yaratma) - Hassas veya gizli (kişisel) konular - Tanıdık birisindenmiş gibi gönderimde bulunmak İstenen cevap - Özel bilgi sağlamak - Kişisel hesap/bilgilerini güncelleme - E-posta mesajındaki linke tıklama - Bir eki (ekli dosyayı) açma Şüpheli göstergeler - Genel selamlamalar - Şüphe uyandıran içerikler - İmla ya da yazım hataları - Tanımadık ya da sıra dışı (garip) bir gönderici - Yanlış bilgi - Yasal olmayan gömülü (saklı) URL'ler (linkler)	- Hesap bilgileri - Kullanıcı adı - Şifre veya PIN bilgileri - Kredi kartı numarası - Sosyal güvenlik numarası - Banka hesap numarası - Banka (teyit) yönlendirme numarası - E-posta adresi - Telefon numarası - Diğer kişisel bilgiler	- Finansal kayıplar - Kimlik hırsızlığı - Çalınan gizli, özel ve kişisel bilgiler - Çalınan fikri mülkiyetler - Bilgisayarın tehdit altında olması ve/veya kötü amaçla yerleştirilmiş virüsler - Manipüle ya da imha edilen veri, yazılım, bilgi veya donanımlar - Kişisel veya örgütsel utanç (sırların açığa vurulması) - Politik kazanç - Hizmet reddi

Kaynak: Greitzer vd. Akt: Allen vd., 2016, s. 97'den uyarlanmıştır

1.6 Sosyal Mühendislikte Genel Saldırı Teknikleri

Çoğu SM saldırısının ilk adımı, saldırganın hedef üzerinde araştırma ve keşif yapmasıyla başlar, yani bu bir tür istihbarat toplama işidir. Daha sonra bu bilgilere dayanılarak ne tür bir saldırı düzenleneceğine dair karar verilir. Son adım ise karar verilen planın uygulanmasıdır. Saldırı başarılı olmazsa döngü yeniden başlatılır. SM'nin ana hedefi zayıf halka olan insandır. Genel olarak iki ana yöntem kullanılmaktadır: Teknik saldırı (bilgisayar ve benzeri teknik/teknolojik yapılara) ve psikolojik saldırı (algı, yönlendirme, manipülasyon vb.).

SM saldırıları hem sosyal psikoloji hem bilgisayar bilimi alanları içerisinde (disiplinlerarası) yer almaktadır. Kötü amaçlı (kurbana zarar veren) ve kötü amaçlı

olmayan (eğitim, deneme, açıkları keşfetmek, iyi bir şey için yönlendirme) şeklinde ikiye ayırmak mümkündür. Mouton, Malan, Kimppa ve Venter (2015)'a göre, kötü amaçlı olmayan saldırılar üç ayrı grupta kategorize edilebilir: Saldırıların yapıldığı ortamlar kamu iletişimi (radyo ve televizyon gibi), penetrasyon testi ve SM araştırması olabilir. Bunlardan herhangi birinde gerçekleştirilen SM saldırısında mağdurlara zarar verilmesi veya toplanan bilgilerin kötüye kullanılması amaçlanmamaktadır (s. 115). Kötü amaçlı saldırılarda ise alan daha da genişlemektedir; radyo, televizyon, telefon, yazılı basın, sosyal medya, bilgisayar, fiziksel ataklar vs. Bu bölümde yer alan örnekler her iki alanı da içermekle birlikte daha çok kötü amaçlı atakları açıklamak içindir.

SM saldırıları çok yönlüdür ve asıl saldırının farklı aşamalarında kullanılan fiziksel, sosyal ve teknik yönleri içerir (Krombholz, Hobel, Huber ve Weippl, 2015, s. 114), bunlar;

- **Fiziksel Yaklaşımlar:** Adından da anlaşılacağı gibi fiziksel yaklaşımlar, saldırganın gelecekteki kurbanı hakkında bilgi toplamak için gerçekleştirmiş olduğu bir takım fiziksel girişimleri içerir.
- **Sosyal Yaklaşımlar:** Başarılı SM saldırılarının en önemli yönü sosyal yaklaşımlardır. Bu nedenle saldırganlar kurbanlarını manipülasyonla ikna etmek için sosyo-psikolojik tekniklere güvenirler.
- **Teknik Yaklaşımlar:** Teknik saldırılar çoğunlukla internet üzerinden gerçekleştirilen saldırılardır.
- **Sosyo-Teknik Yaklaşımlar:** Başarılı SM saldırıları genellikle yukarıda açıklanan farklı yaklaşımların birkaçını veya tümünü birleştirir. Ancak, sosyo-teknik yaklaşımlar, sosyal mühendislerin en güçlü silahlarını oluşturmaktadır. Örneğin, kötü niyetli yazılım barındıran bir USB belleğini mağdurun kolayca bulup (merakından) bilgisayarına takması vb.

Tersine Sosyal Mühendislik: Bir potansiyel kurbanla doğrudan temasa geçmek yerine, saldırgan, güvenilir biri olduğuna inanılmasını sağlar. Buradaki amaç, potansiyel mağdurların ihtiyaç duyduklarında kendilerine gerekli yardımın (saldırgan tarafından) sağlanabileceği konusunda ikna olmalarını sağlamaktır. Ya da, saldırgan, kurbanın (sisteminde) bir sorununun

olduğunu (bazen sistemde bir sorun yaratarak) veya gelecekte olabileceğini (ikna ederek) eğer isterse kendisine yardım için her zaman hazır olduğuna inandırır. Yardım talebi geldiğinde, sosyal mühendis sonraki aşamaya geçer.

Tersine SM üç bölümden oluşur (Shetty, 2019):

- **Sabotaj:** Saldırgan sisteme basit bir şekilde eriştikten sonra, sistemi bozar veya bozulmuş gibi görünmesini sağlar. Kullanıcı, sistemi bozuk durumda gördüğünde, sorunu çözmek için yardım aramaya başlar.
- **Pazarlama:** Kullanıcının var olan (gerçekte sorun olmayabilir de) sorunla ilgili olarak yardım talebinde bulunmasının ardından, sosyal mühendis kendisinin bu sorunu çözebilecek tek kişi olduğunun pazarlamasını yapar ve bu konuda kullanıcıyı ikna eder.
- **Destek:** Bu adımda hedefin güveni kazanılır ve hassas bilgilere erişim sağlanır.

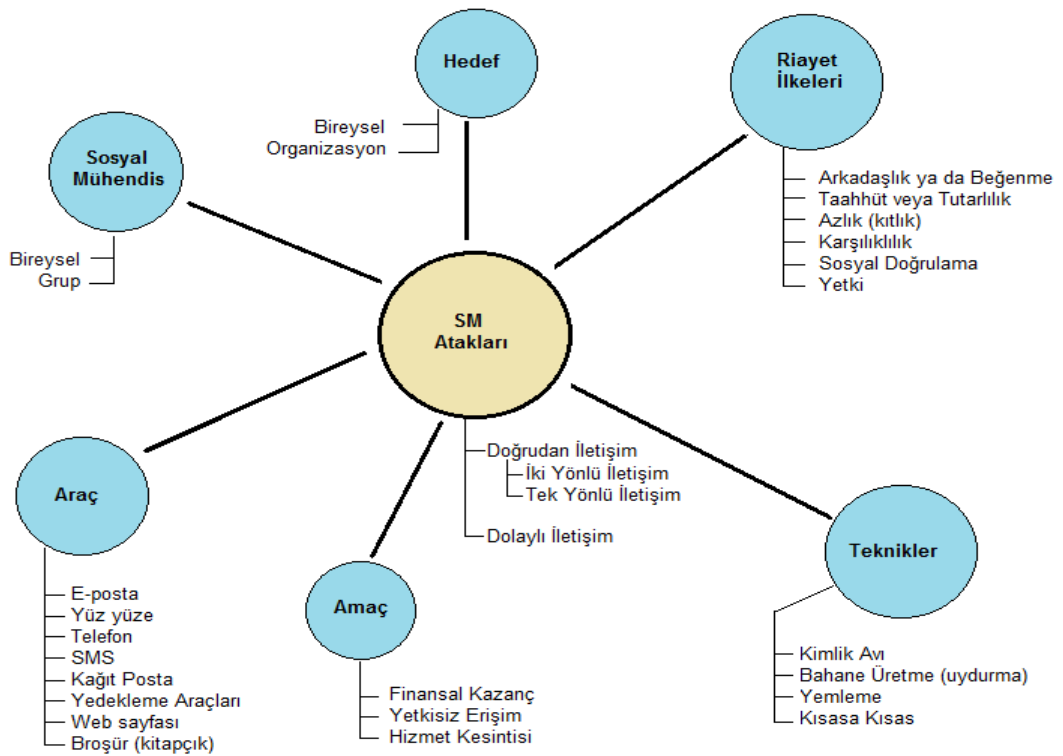
Dadkhah ve Quliyeva (2014) SM'nin pek de bilinmeyen bir alanda uygulanışından bahsetmektedir: "Akademi Dünyasında SM". Akademik makalelerin yayınlanmasına aracılık etmek için (maksatlı) gönderilen (sahte) linkler, yüksek etki faktörü sağladığı iddia edilen sahte ya da düşük etki faktörü olan dergiler (genellikle Thomson Reuters veya Scopus tarafından sunulan dergilerin etki faktörü, gerçek olmayan dergiler için de söylenerek araştırmacılar kandırılabilir), gerçekte var olmayan konferanslar, tanınmış kişilerin yer aldığı (sahte) yayın kurulu üye listeleri gibi daha birçok yanıltıcı bilgi sunulabilmektedir. Burada da esas niyet akademisyenlerin zafiyetlerinden yararlanarak, istenilen yere yönlendirilmeleriyle elde edilen bilgiler ve onların açıklarından faydalanmayı kapsamakta ya da araştırmacıların çalışmalarını etki faktörü (impact factor) yüksek dergilermiş gibi gösterilen adreslere/yerlere postalamalarını sağlamaktır. Daha da kötüsü gerçekte var olmayan akademik platformlara ödeme yaptırarak başvuru yapmalarını sağlamak şeklinde de olabilmektedir.

SM, insanları eylemlerde bulunmak veya gizli bilgileri açığa çıkarmak için manipüle etmekte kullanılan tekniklerden oluşur. SM, bir yabancı tarafından hassas bilgilerin ele geçirilmesidir. Bunu başarmak için bir sosyal mühendis, bilgiye erişim sağlama veya normal güvenlik prosedürlerini ihlal etme konusunda kişileri kandırmaya çalışır. Bu süreç SM saldırısı olarak bilinir. SM, yüz yüze etkileşimlerde,

telefon üzerinden, mektuplarla, e-postalarla, web siteleri üzerinden veya kişiler aracılığıyla kullanılabilir. Yalnızca şirketleri, kuruluşları ve hükümetleri değil, bireyleri de tehdit etmektedir (Sadiku, Shadare, Musa 2016, s. 64).

Şekil 9’da gösterilen Mouton, Leenen vd.’nin (2014) ontolojik modeline göre bir SM saldırısı doğrudan veya dolaylı iletişimi kullanmaktadır. Saldırı birden fazla saldırı aşamasına ayrılabilir ve her aşama modele göre yeni bir saldırı olarak ele alınır (Merwe ve Mouton, 2017, s. 28).

Şekil 9. Sosyal Mühendislik Saldırısının Ontolojik Bir Modeli

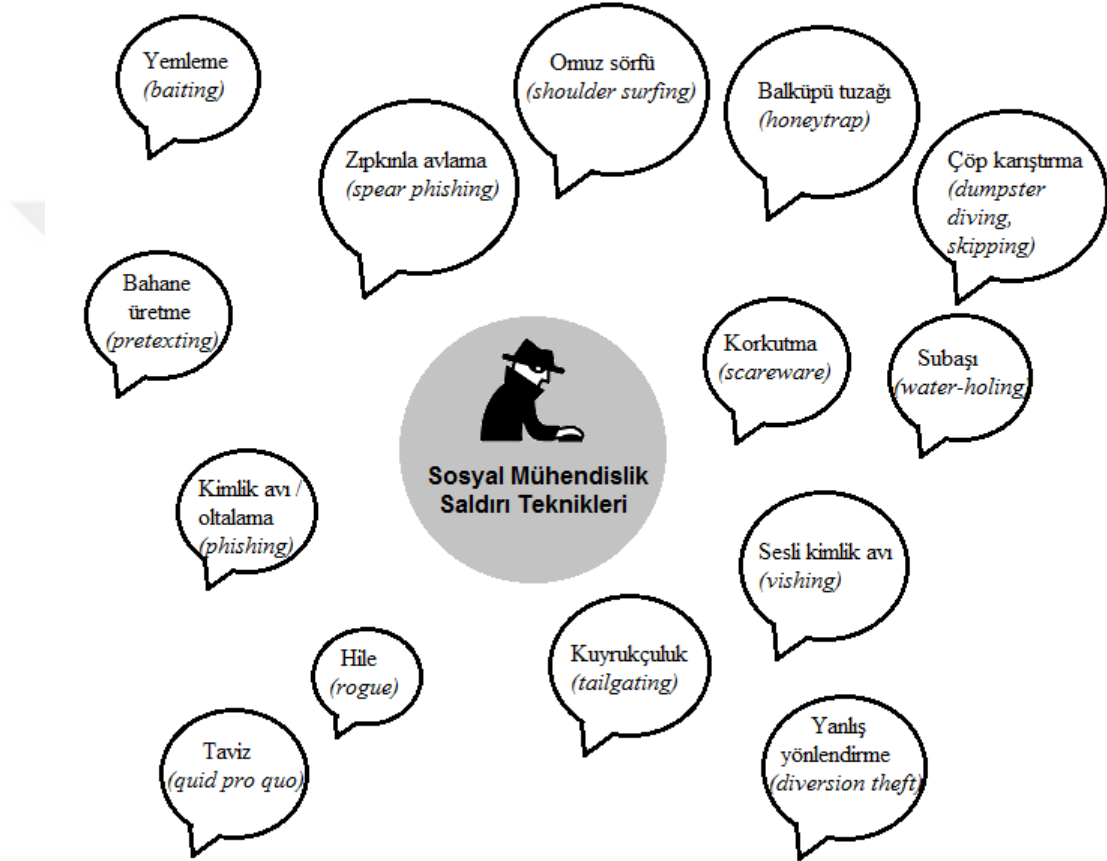


Kaynak: Mouton, Leenen, vd., 2014 Akt: Merwe ve Mouton, 2017, s. 28

SM’de sürekli yeni saldırı teknikleri üretilse de kullanılan teknikler içerisinde en çok bilinenler ve tercih edilenleri (literatür araştırması sonucunda elde edilen veriler ışığında) belirli başlıklar altında sınıflandırmak mümkündür. SM alanında detaylı çalışmaları bulunan “Knowbe4.com” sitesi de bu saldırıları benzer şekilde on başlık altında toplamaktadır; bahane üretme (pretexting), kimlik avı/oltalama (phishing), subaşı (water-holing), taviz (quid pro quo), balküpu tuzağı (honeypot), yanlış yönlendirme (diversion theft), zıpkınla avlama (spear phishing), yemleme

(baiting), kuyrukçuluk (tailgating) ve hile (rogue). Bu başlıklara omuz sörfü (shoulder surfing), korkutma (scareware), sesli kimlik avı (vishing) ve çöp karıştırma da (dumpster diving, skipping) eklenebilir. Şekil 10'da toplam on dört saldırı tekniğini bir arada gösterilmiştir.

Şekil 10. Sosyal Mühendislik Saldırı Teknikleri



1.6.1 Sosyal Mühendislik Alanında Bilinen (En Çok Tercih Edilen) Saldırı Teknikleri

Farklı çalışmalarda farklı gruplandırmalara gidilmiş olmakla birlikte en çok kullanılan, tercih edilen ve bilinen SM saldırı teknikleri aşağıda başlıklar altında kısaca açıklanmıştır. Bu başlıklara ilave edilebilecek birkaç başlık daha bulunsa da pek bilinmediği ve çok nadir kullanıldığı için bu başlıklara burada yer verilmesi araştırmacı tarafından uygun bulunmamıştır. Ayrıca her geçen gün yeni tekniklerin inşa edildiği ve henüz sınırlı bir kesim tarafından kullanıldığı (bilindiği) için burada bahsedilmeyen tekniklerin de bulunabileceği hususunu hatırlatmak uygun olacaktır.

1.6.1.1 Bahane Üretme (*Pretexting*)

Bahana üretme; uydurma bir senaryo ile potansiyel bir mağdurla iletişim kurup (örneğin; doğum tarihi veya sigorta numarasını söyleyerek) daha fazla bilgi alma girişimidir. Ayrıcalıklı verilere erişmek için bir tarafın diğerine yalan söylemesi, bahane uydurmasıdır. Örneğin, önceden hazırlanmış bir aldatmaca ile, alıcının kimliğini doğrulamak için kişisel veya finansal verilere ihtiyaç duyulduğunu iddia eden bir saldırı çeşidini içerebilir. Sadiku vd. (2016)'ne göre bu durum, önemli/ayrıcalıklı bilgilere erişmek için bir tarafın diğerine yalan söylemesiyle oluşur. Bir saldırgan (sahtekâr), mağdurun hassas/özel bilgileri vermesi için onu etkilemek adına tasarlanmış bir ortam yaratır. Kimlik avı için gönderilen e-postalar, kurban olarak seçilen kişinin belirli avantajları yitirmemesi için, kurban üzerinde korku ve aciliyet hissi yaratma mekanizmalarını kullanır. Bu tür saldırılar kurbanda sahte bir güven duygusu oluşturmaya dayanır. Örneğin, saldırgan hedefin kimliğini doğrulamak için bazı kişisel bilgilere ihtiyaç duyduğunu ifade edebilir (s. 65).

1.6.1.2 Kimlik Avı / Oltalama (*Phishing*)

Kimlik avı; güvenilir bir kişi ya da organizasyonmuş gibi davranarak, toplu e-posta yoluyla güvenlik/spam filtrelerinden korunarak, kullanıcı adı, parolalar, kredi kartı bilgileri gibi hassas bilgileri toplama sürecidir. Hadnagy (2017)'ye göre oltalama, daha fazla bilgi almak için, hedefler tarafından açılması umulan aldatıcı mesajlar, bağlantılar ya da dosyalarla e-posta gönderme işlemidir ve genellikle bu bağlantılar (linkler) ya da içerdikleri dosyalar kötü niyetli veri yükü içermektedir (s. 33). E-postada gönderilen bağlantı adresinin (link) tıklanması ya da ekli dosyanın açılması sonucunda bir program/uygulama (genellikle Truva atı -trojan- ya da *keylogger* vb.) kullanıcıların bilgisayarına yüklenir ve saldırganın komutlarına göre süreç devam eder. Sadiku vd. (2016)'ne göre kimlik avı en yaygın SM saldırısı türü gibi görünmektedir. Sahte e-postalar ve web siteleri ile ilişkilidir. İnsanlar bazen hassas veya özel bilgileri zorunluluk duydukları kişilere açıklamaktadırlar. Kimlik avı uzun süredir uygulanmaktadır, ancak son zamanlarda daha fazla sayıda ve sofistike hale gelmiştir (s. 65).

1.6.1.3 Subaşı (*Water-Holing*)

Subaşı; insanların güvendiği ve sıkça ziyaret ettiği web sitelerinin tespit edilen güvenlik zafiyetlerinden (açıklarından) yararlanılarak bu web sitesinin

hacklenmesi ve bu siteyi kullanmakta olan hedef gurupların bilgilerine ulaşarak onların kullanmış oldukları bilgisayar sistemlerine giriş sağlanmasıdır.

1.6.1.4 Taviz (*Quid Pro Quo*)

Taviz; hedef kullanıcının bilgisayarındaki (sözde) bir teknik hatadan yola çıkarak bilgi paylaşımı ya da yardım önerisi gibi bir yöntemle kullanıcının bazı bilgilerine erişim sağlanmasıdır. Teknik destek bölümünden bir yetkili gibi gözüktüp, “...şuna yönelik problemlerinizi halledebilmemiz için sizin şu... bilgilerinize ihtiyaç duymaktayız” vb. cümlelerle bilgilere erişim sağlanmaktadır. Saldırgan, bu şekilde kurbanın bilgisayarına zararlı yazılım yükleyerek elde edeceği bilgilerin kullanıcısına geri iadesi vb. karşılığında fidye isteyebilmektedir.

1.6.1.5 Balküpü Tuzağı (*Honeytrap*)

Balküpü tuzağı; sosyal mühendisin, herhangi bir kişiyle çevrimiçi iletişime geçerek, ona çok çekici biriymiş gibi davranıp, kurbanından hassas bilgiler toplamasıdır. Çekici ve güzel kadınların, önemli pozisyonlarda olan erkeklerle iletişime geçerek (tam tersi de geçerlidir) bilgi edinmesinde olduğu gibi.

1.6.1.6 Yanlış Yönlendirme (*Diversion Theft*)

Bu tür saldırılarda, sosyal mühendisler bir teslimatı (paketi) veya kurye şirketini yanlış konuma (kendilerine) yönlendirerek işleme/sürece müdahale ederler.

1.6.1.7 Zıpkınla Avlama (*Spear Phishing*)

Sosyal mühendisler bu yöntemde oltalama (phishing) saldırısında olduğu gibi toplu olarak ya da rastgele değil, tam aksine, hedef (özel olarak seçilmiş) bir kurbanı ya da organizasyona saldırarak bilgi elde etmeye veya sızmaya çalışırlar. Kurban hakkında internet üzerinden ve sosyal medya sitelerinden çeşitli bilgiler toplanıp derlenerek kişiye yönelik, onun ilgisini çekecek tetikleyici e-postalar gönderilir. Gönderilen e-postalarda kurban olarak seçilen kişinin zararlı yazılımların olduğu web sayfasına yönlendirileceği linkler bulunur ve bu linklere tıklaması hedeflenir.

1.6.1.8 Yemleme (*Baiting*)

Yemleme; kurbanın önünde bir şeyleri sallayıp, harekete geçirme anlamına gelir. Örneğin, ilgi çekici bir film indirmesi sağlanarak, film içine yerleştirilmiş kötü amaçlı yazılımlar kullanılabilir. Ya da, kurbanın bulabileceği bir yer seçilerek, içerisinde kötü amaçlı yazılım barındıran bir USB hafıza belleğinin ortalık yere

bırakılması olabilir. Yemleme, sosyal mühendislerin, kurbanlarının istediği bir şeye erişmesi için onlara sunulan bir dizi avantajı içerebilir. Kimlik avı saldırılarına benzemektedir. Örneğin, saldırgan, kurbanına eğer kişisel (bazı) bilgilerini verirse onun için önemli olan bazı web sitelerine ücretsiz erişim sağlayabileceği vb. tekliflerde bulunabilmektedir.

1.6.1.9 Kuyrukçuluk (*Tailgating*)

Kuyrukçuluk; sosyal mühendislerin, korunaklı bir binaya, mekâna, odaya vb. erişim sağlamak için, yetkili birisinin güvenli alana geçişini beklemesi ve onu takip ederek hemen ardından (sıvışarak) içeri giriş yapması yöntemidir. Bu saldırı aynı zamanda “piggybacking” (sırtında taşıma) olarak da bilinmektedir.

1.6.1.10 Hile (*Rogue*)

Hile; kötü amaçlı yazılımları bilgisayardan kaldırmayı vaat ederek, içinde zararlı kod bulunan bir yazılımı, zararlı yazılımlardan koruma sağlayan (anti-malware) programmış gibi tanıtarak hedefteki kurbanın bilgisayarına indirmesini sağlama işlemidir. Son zamanlarda bu yöntem sıkça kullanılmaktadır.

Yukarıda verilen bu başlıklara ek olarak SM’nin saldırı teknikleri içerisinde yer alan diğer başlıklar ise şunlardır;

1.6.1.11 Sesli Kimlik Avı (*Vishing*)

Sesli kimlik avı yöntemi, hedefteki kişilerin kişisel ve finansal bilgilerini toplamak için SM’nin telefon üzerinden gerçekleştirilmesidir. Telefon görüşmeleri yapılarak insanları kandırıp bilgiler elde etmek için sıkça başvurulmuş bir yöntemdir.

1.6.1.12 Korkutma (*Scareware*)

Korkutma; bilgisayarına kötü amaçlı yazılım bulaştığını veya yanlışlıkla yasa dışı olarak indirilen bir içeriğe sahip olduğunu düşünmesi için hedefteki kurbanın kandırılmasıdır. Saldırgan, kurbanı, var olduğuna inandırdığı bu sahte sorunu çözecek bir (sahte) çözüm sunar. Gerçekte ise, kurban, saldırganın kötü amaçlı yazılımını indirmek ve yüklemek için sadece kandırılmaktadır. Korkutma saldırıları, kurbanın sistemine virüs bulaştığının iknasıyla başlar ve ardından bu virüslerden kurtulabilmesi için ona (ücret ödeyerek) indirmesi gereken anti-virüs yazılımının linkini sunmakla devam eder. İlerleyen aşamalarda ise ayrıca, (sözde) güvenlik

yazılımı çeşitli zaman aralıklarıyla enfeksiyonlara yönelik uyarılar görüntüler ve bunları kaldırmak için kurbandan yeniden ödeme yapması talep edilir. Döngü bu şekilde devam eder. Korkutma saldırıları son zamanlarda sıkça kullanılmakta olup, kendisini polis, savcı, hâkim vb. kimliklerle tanıtıp, kurbanın adının terör örgütüne, çetelere vs. karıştığını, belirli bir ödeme karşılığı bunu kolayca halledebileceklerini söylemeleri şeklinde icra edilmektedir.

1.6.1.13 Omuz Sörfü (*Shoulder Surfing*)

Omuz sörfü; kişisel bilgilerin bilgisayara, telefona vb. girilirken, ya da deftere veya her hangi bir yere not alınırken, hedefteki kişinin yakınlarında durularak, kullanmış olduğu şifre, PIN kodu, kullanıcı adı gibi bilgileri veya içerikleri belli etmeden not etme, çalma işlemidir (iş yerinde, ofiste, toplu ulaşım, uçakta, kafede, ATM’lerde ve her yerde uygulanabilmektedir).

1.6.1.14 Çöp Karıştırma (*Dumpster Diving, Skipping*)

Çöp karıştırma; hedefteki kişi ya da kuruma yönelik her türlü bilgiyi toplamak için kullanılan bir SM yöntemidir. Tam olarak yırtılmadan atılan kâğıtlardaki bilgiler, faturalar, çizelgeler, hesap numaraları, müşterilere ait bilgiler, kişisel bilgiler, CD’ler vb. pek çok parçadan faydalanmak suretiyle tahminlerin üzerinde bilgi elde edilebilmektedir. Kişisel çöplerinizden ne yediğiniz, ne içtiğiniz, kullandığınız ilaç kutuları, marka tercihiniz gibi onlarca bilgi toplanabilmektedir. Sosyal mühendisler ve dedektifler için bu alanlar bir hazine olarak değerlendirilmektedir. Yalnızca çöplerden elde edilen bilgiler doğrultusunda çok detaylı raporlar dahi hazırlanabilmektedir. Artık kullanılmayan, hurdaya çıkmış donanımlardan da birçok bilgi (geri dönüştürülerek) elde edilebilmektedir. Uygun bir şekilde imha edilmemiş, CD, harddisk, hafıza kartları vs. buna örnektir.

Yukarıda açıklanan tekniklerin yanı sıra, kullanılan diğer SM saldırı tekniklerden bazıları ise şunlardır;

Reddetme ve Geri Çekme: Reddedilmesi kesin olan uç bir taleple başlayarak, kabul edilmesi muhtemel olan daha küçük bir talebe geri çekilmedir. Aslında başından beri hedeflenen talep de bu daha küçük olan taleptir. “Yapılan araştırmalara göre, reddetme ve geri çekme tekniği sadece birinin talebe evet deme olasılığını artırmakla kalmaz o kişinin bu talebi yerine getirmesini ve ileride yapılacak benzer talepleri de kabul etme şansını yükseltir” (Cialdini, 2018, s. 89). Burada dikkat

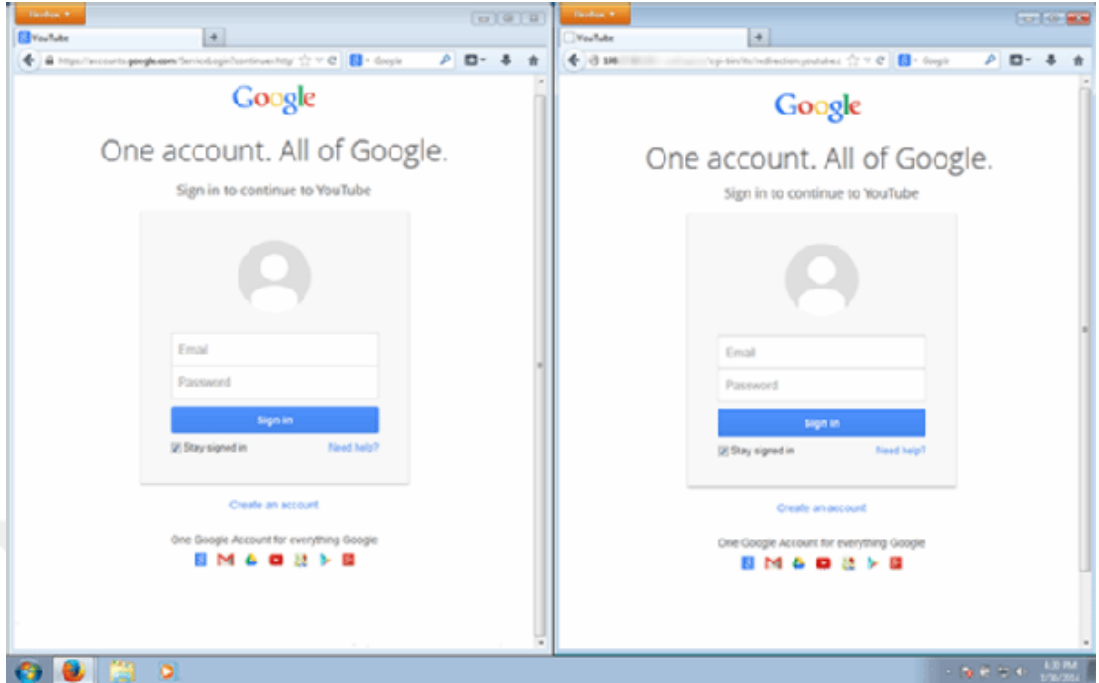
edilmesi gereken en önemli husus daha küçük (esas) talepten önce sunulan uç talebin aşırı uç talep olmaması, esas talebin ise uç talepten belirgin bir seviyede aşağıda (kabul edilebilir, taviz verilebilir) olması gerektiğidir. Diğer önemli husus ise, almış olunan taviz abartılmadığı sürece tekrar tekrar (ileriye dönük zamanlarda) alınabilecek olmasına yol açmasıdır. Taviz veren kişi, önceki davranışına uygunluk göstermesi (mantıksal tutarlılık) açısından yeniden taviz vermekten kolay kolay kaçamayacaktır.

Çekicilik: Palo Alto, Calif’de bulunan Adallom bulut uygulama güvenlik firması şirketi başkan yardımcısı Tal Klein, bir sosyal mühendisin şirket çalışanlarının isim listesini ele geçirebileceğini ve sanki bir çalışandan diğerine gönderiliyormuş gibi içerisinde karşı konulamaz ve çekici bir YouTube video linki barındıran e-posta gönderebileceğini ve bu şekilde insanların tehlike içinde olduklarını daha zor anlayacağını söylüyor (Johnson, 2018).

Merak: Merak etme içgüdüsünün problem yaratabileceği konusunda mağdurların yeterince bilgilendirilmemesi, sosyal mühendisler tarafından kullanılan bir boşluktur. Çekici tasarımlar, ümit verici ilginç buton ve pencereler insanların gönderilen bilgileri doğrulamadan web bağlantılarına tıklamalarını sağlamaktadır. Yakınlık izlenimi oluşturmak da kullanıcıların istenilen yönde davranmalarını sağlar. İnsanların sosyal mühendisler tarafından suistimal edilen bir başka özelliği de insanların yardıma ihtiyacı olanlara nezaket göstermesidir. Davetsiz misafirlere çalışanlar tarafından (genellikle) bu yüzden yardım edilir. Açgözlülük ise insanları rüşvete veya kandırılmaya iten şeydir. Bu nedenle, aldıkları ücretlerden (maaşlarından) memnun olmayan hamal, kapıcı, müstahdem gibi daha düşük pozisyonda olanlar, maddi fayda karşılığında binalara erişim sağlama ya da bilgi sızdırma konusunda yönetimde olanlardan (karar almaya katılanlardan) daha kolay bir şekilde ikna edilirler (Şerban ve Şerban, 2014, s. 7).

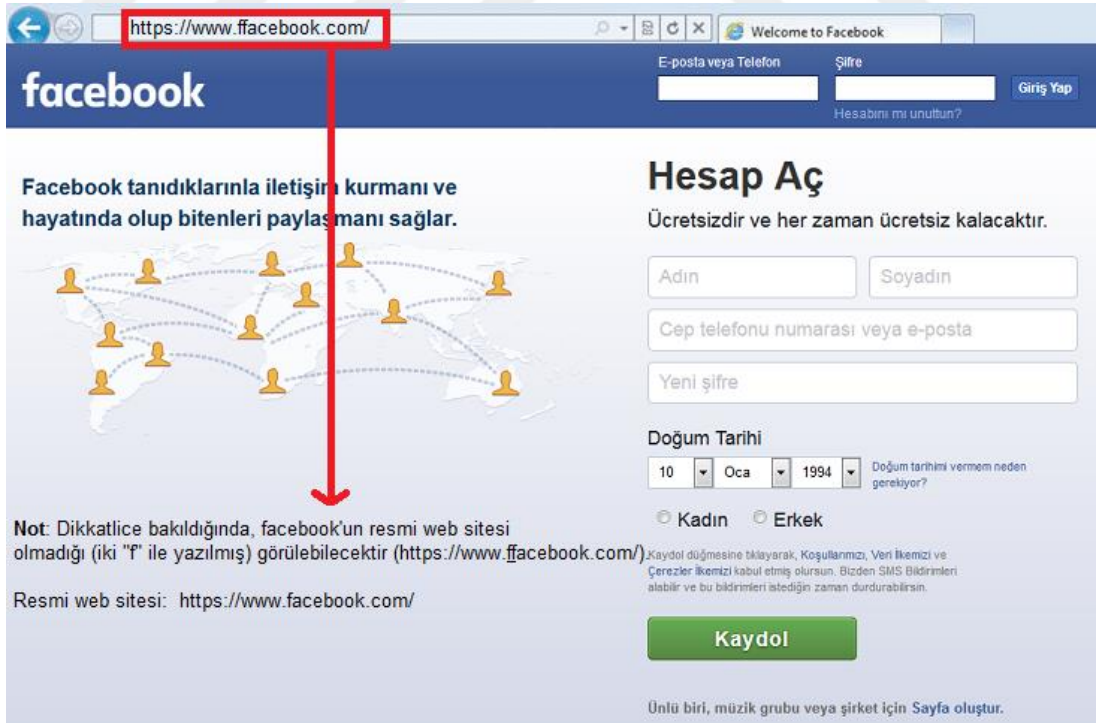
Son zamanlarda çok kullanılan bir diğer bilgi avcılığı yöntemi ise, kullanıcıların bildik, tanıdık, aşina olduğu web sitelerin görünüm olarak aynısının (ikizinin) dizayn edildiği ve kullanıcıların güvenli bir siteye giriş yapıyormuş gibi bilgilerini “huzur” içerisinde girmesiyle sonuçlanan ataklardır. Şekil 11 ve Şekil 12’de yer alan ekran görüntüleri ile bu durum açıklanmaya çalışılmıştır (Benzer ekranlar ama hangisi gerçek? Google ve Facebook hesap örnekleri)

Şekil 11. İkiz Görünümlü Web Siteleri (Arayüzleri) - Google



Kaynak: Adallom Inc. Akt. <https://searchsecurity.techtarget.com/feature/Social-engineering-You-got-nailed>, Erişim: 03.12.2019

Şekil 12. İkiz Görünümlü Web Siteleri (Arayüzleri) - Facebook



Kaynak: <https://www.facebook.com/>, Erişim: 03.12.2019 (facebook web sitesi ana sayfa görüntüsü kullanılarak oluşturulmuştur)

Yine, kötü amaçlı yazılımlar, sosyal paylaşım sitelerinde gezinirken kullanıcıların yoğunluklarından yararlanarak, yasal reklamları taklit edip, bu reklamlara tıklama meraklarından faydalanır. Kullanıcılar için bu şekilde davranmak kötü amaçlı yazılımın tespit edilmesini zorlaştırır (Mansour, 2016, s. 351).

1.6.2 Sosyal Mühendislik Saldırı Vektörleri

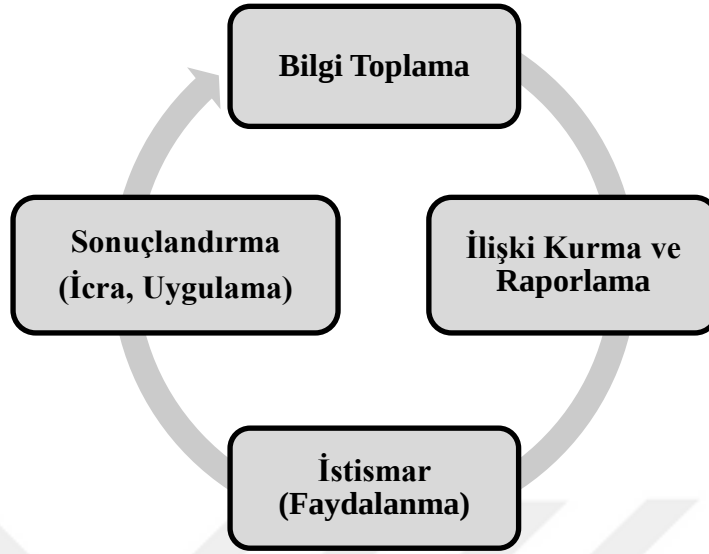
Social-engineer.org sitesi genel saldırı vektörlerini dört aşamada incelemekte ve bunun yanı sıra Nyirak (2018) saldırı döngüsünü de yine aynı şekilde dört aşamalı olarak açıklamaktadır. Bu aşamalar kısaca şu şekildedir: Kötü niyetli kişiler, bireylere ve örgütlere saldırı için çeşitli yöntemler kullanırlar. Genelde en çok kullanılan dört saldırı vektörü; phishing, vishing, impersonation ve SMiShing'dir. Bunlar bazen tekli olarak bazen de daha etkili olması için kombine olarak kullanılmaktadır;

- **Phishing:** Kişisel bilgilere erişme maksadıyla güvenilir gözüken adreslerden e-posta gönderme yöntemi.
- **Vishing:** Telefon aracılığıyla bilgi elde etmeye çalışma yöntemi.
- **Impersonation:** Kişi, kurum veya bilgisayar sistemlerine erişim elde edebilmek için başka birisinin yerine geçme (kimliğine bürünme) yöntemi.
- **SMiShing:** Cep telefonu mesajıyla (SMS), kurbanların kötü amaçlı yazılımları indirmelerini, kötü amaçlı bir web sitesini ziyaret etmelerini ya da sahte bir telefon numarasını aramalarını sağlamak üzere acil eylemler için kullanma yöntemi.

1.6.3 Sosyal Mühendislik Saldırı Döngüsü

Şekil 13'de gösterildiği üzere, tipik SM saldırı döngüsü dört aşamalıdır; bilgi toplama, ilişki kurma ve raporlama, istismar (faydalanma), sonuçlandırma (icra, uygulama). Bazı durumlarda döngünün bir kısmı ya da tüm aşamaları yeniden tekrar edilir. Saldırı ve hedefin yapısına göre bazı adımlar ya da tüm adımlar birkaç defa saldırgan yakalanana, vazgeçene ya da istediğini elde edinceye kadar devam eder.

Şekil 13. En Temel Sosyal Mühendislik Saldırı Döngüsü



Kaynak: Allen, 2016 Akt: Jain, Tailang, Goswami, Dutta, Sankhla, Kumar, 2016, s. 95-96'den uyarlanmıştır

Bir SM saldırı başlangıçta isimler, telefon numaraları, doğum tarihleri gibi hedefe ait bilgileri halka açık bir şekilde erişilebilen ortamlardan, organizasyon şemalarından vb. yerlerden toplar. Hedefteki kişinin güvenini kazanmak için sosyal mühendis bu bilgileri kullanarak iletişim kurmayı dener ve karşı tarafta bir güven hissi yaratarak başka türlü ele geçiremeyeceği bilgileri elde etmek ve/ya eylemlerini uygulamak için hedefini ikna etmeye çalışır. Son aşamada ise elde edilen bu bilgiler kullanılarak yönlendirmeler gerçekleştirilir (Allen, 2016 Akt: Jain, Tailang, Goswami, Dutta, Sankhla, Kumar, 2016, s. 95-96).

1.6.3.1 Bilgi Toplama

Birçok SM saldırısının başarı olasılığı bu aşamaya bağlıdır. Bu nedenle dikkatin ve zamanın çoğunu buraya harcamak oldukça doğaldır. Bilgi toplama teknikleri şu çerçeve içerisinde değerlendirilmelidir; toplanan bilgiler saldırı vektörünün ne olacağını belirler, olası şifreler elde edilir, hedefler yeniden yapılandırılır, hedefe yakınlık sağlanır ve güçlü bahaneler üretmek için kullanılır.

1.6.3.2 İlişki Kurma ve Raporlama

Bu aşama hedefle bir tür ilişki (iletişim) kurma aşamasıdır. Saldırganın hedefle kuracağı ilişkinin kalitesi, saldırı esnasında hedefin ne kadar işe yarayacağı açısından oldukça kritik bir noktadır. Güzel bir gülümseme ve göz teması kurarak

hedefin giriş kapısını açık tutmasına yarayacak kadar kısa bir ilişki de olabilir, kişisel düzeyde bir telefon konuşması, ya da lobide ön büroda çalışan birisine aile resimlerinin gösterildiği bir ilişki kurma da olabilir veyahut sosyal paylaşım sitelerinden arkadaşlık kurmak adına sahte bir profil ile çıkma teklifi şeklinde daha kapsamlı da olabilir.

1.6.3.3 İstismar (Faydalanma)

Saldırgan bu aşamada, hedefe sızmak için hem bilgiyi hem de kurduğu ilişkiyi aktif olarak kullanır. Görünüşte önemsiz gibi görünen bilgiler ışığında saldırgan hedefine ulaşmaya çalışır.

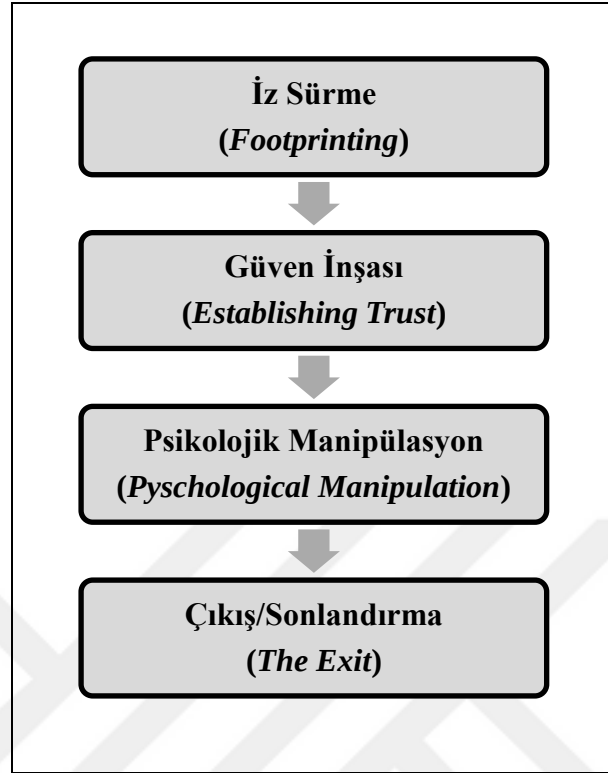
1.6.3.4 Sonuçlandırma (İcra, Uygulama)

Bu aşama saldırının nihai amaca ulaştığı ya da çeşitli sebeplerden dolayı şüphe yaratmadan sonlandırıldığı aşamadır. Hedefi, neler olduğunu sorgulaması aşamasında terk etmekten ziyade, iyi bir şeyler yaptığını hissetmesini sağlayarak ayrılmak gelecekte ilişkinin devam etmesi açısından önemlidir. Bu aynı zamanda geride bir iz bırakmamak ve saldırı düzenlendiğinin (ve saldırı düzenleyenin kimliğinin) anlaşılmasını sağlayacak bir ipucunun geride kalmaması bakımından da önemlidir. İyi planlanmış ve sorunsuz bir çıkış (kaçış) saldırıdaki son hamledir.

1.6.4 Sosyal Mühendislik Yaşam Döngüsü

SM saldırı döngüsü ile SM yaşam döngüsü aslında aynı şeyleri ifade etmekle birlikte, araştırmacılara göre farklı başlıklar altında ifade edilmeye çalışılmakta ve göz ardı edilebilecek küçük ayrıntılar içermektedir. Her SM saldırısı benzersizdir, ancak karşılaşılan durumların biraz anlaşılması ve açığa çıkmasıyla, bir SM faaliyetinin kaba bir döngüsünü hazırlamak mümkündür. Şekil 14’de SM yaşam döngüsünün genel bir temsili dört ana aşamada gösterilmektedir (Shetty, 2019). Shetty’nin ifade ettiği bu aşamalar aşağıda verilmiştir:

Şekil 14. Sosyal Mühendislik Yaşam Döngüsü-I



Kaynak: Shetty, 2019

1.6.4.1 İz Sürme (Footprinting)

Bu aşama hedef(ler) ve çevre ile ilgili bilgi toplama aşamasıdır. İz sürme, başarılı bir saldırı şansını artırmak için saldırganın hedefle bağlantılı kişilerin kim olduklarının ortaya çıkartılmasını da içerir. İz sürme aşaması toplanan bilgilerin yanı sıra şunları da içerir: Çalışanların isim ve telefon listesi, organizasyon şeması, departman bilgileri, konum bilgileri vb. İz sürme aşaması SM ataklarının ilk (hazırlık) evrelerinden birisidir. Bu aşamada kullanılan yardımcı araçlardan (yazılımlardan) bazıları ise *Creepy*, *SET* ve *Maltego*'dur.

1.6.4.2 Güven İnşası (Establishing Trust)

Muhtemel hedef(ler) belirlendikten sonra, saldırgan daha sonra hedefle iyi bir ilişki kurabilmek (geliştirebilmek) için genellikle işyerinde çalışan birileriyle ilişki kurmak için harekete geçer. Sosyal mühendisin kazandığı güven, daha sonra işletmeye ciddi zararlar verebilecek gizli bilgileri açığa çıkarmak (elde etmek) için kullanılır.

1.6.4.3 Psikolojik Manipülasyon (*Psychological Manipulation*)

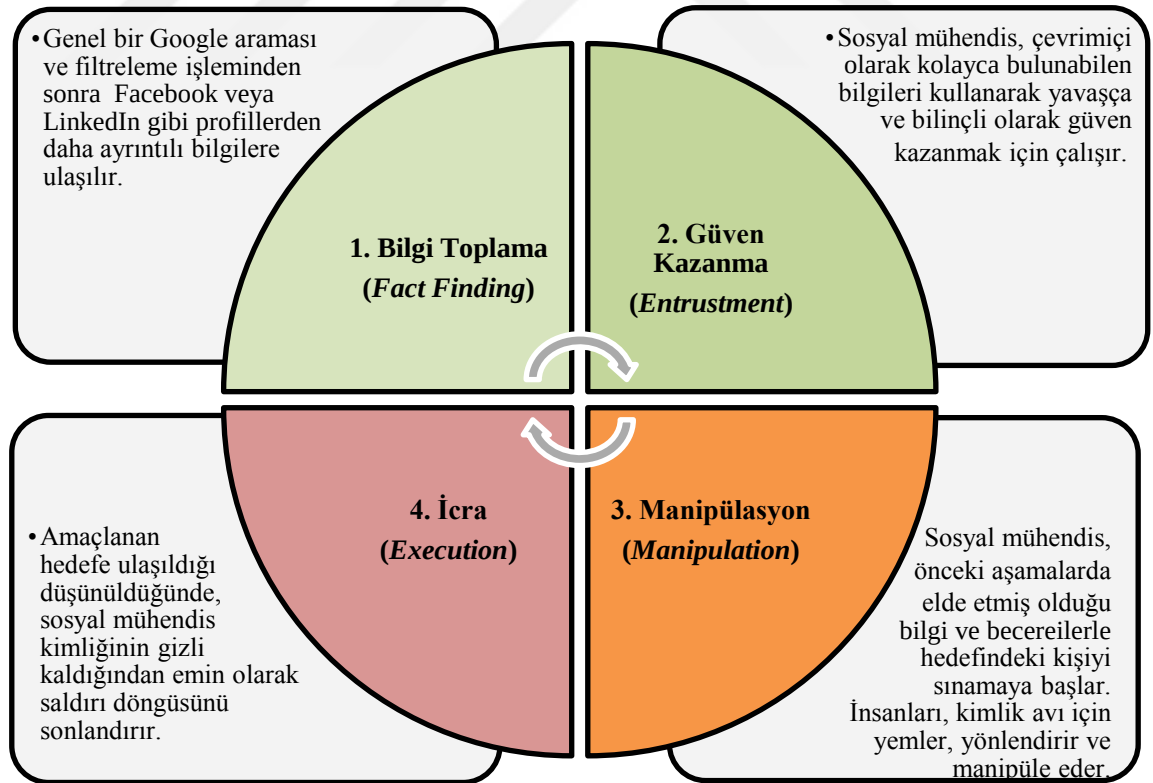
Bu aşamada, sosyal mühendis önceki aşamada edindiği güveni kullanarak, gizli bilgileri elde etmek veya sisteme erişim sağlayabilmek için hedefi manipüle eder. Gerekli tüm hassas bilgiler toplandıktan sonra, sosyal mühendis bir sonraki aşamaya geçebilir veya söz konusu sistemin istismarına odaklanır.

1.6.4.4 Çıkış/Sonlandırma (*The Exit*)

Tüm gerekli bilgiler ele geçirildikten sonra, sosyal mühendis, herhangi bir gereksiz şüphe yaratmayacak şekilde temiz bir çıkış yapar. Sosyal mühendis (gerektiğinde hedefe tekrar erişim sağlayabilmek için) geride gerçek kimliğini ortaya çıkarabilecek bir bilgi ve/ya link izi bırakmadan işlemini (saldırısını) sonlandırır.

Şekil 15’de gösterildiği üzere Wilcox, Bhattacharya ve Islam (2014)’a göre ise SM yaşam döngüsü şu dört aşamadan oluşmaktadır: Bilgi toplama, güven kazanma, manipülasyon ve icra.

Şekil 15. Sosyal Mühendislik Yaşam Döngüsü-II



Kaynak: Wilcox, Bhattacharya ve Islam, 2014

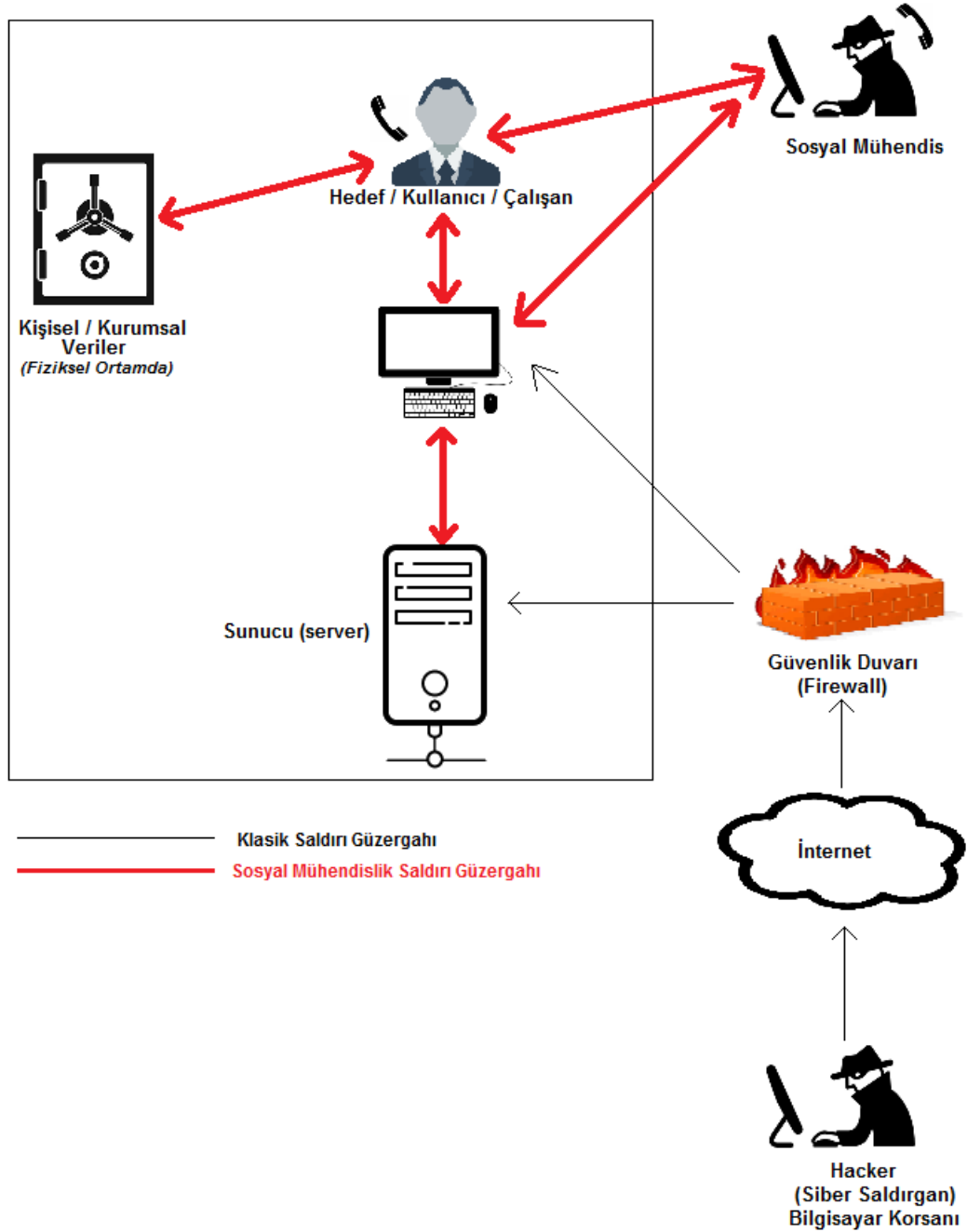
Wilcox vd. (2014)'ne göre;

- **Bilgi Toplama** (*Fact Finding*): Bir saldırgan (sosyal mühendis) tarafından bilgi toplamak için çeşitli teknikler kullanılabilir. Hedefler hakkında bilgi bir kez toplandığında, bu bilgi daha sonra hedefle iletişime (temasa) geçmek veya saldırının başarısı için önemli olan (kilit) birisiyle iletişim kurmak için kullanılabilir.
- **Güven Kazanma** (*Entrustment*): Bir saldırgan, hedefin güvenini kazanmak için ondaki isteği sınırsızca istismar edebilir. Bu ilişkiyi kurma/geliştirme esnasında saldırgan, kendisini daha sonra bundan faydalanacağı bir güven konumuna oturtmaya çalışır.
- **Manipülasyon** (*Manipulation*): Hedef daha sonra “güvenilir” saldırgan tarafından, bilgi (örneğin şifrelerini) ifşa etmesi için veya normalde yapmayacağı bir işlemi/eylemi yapması maksadıyla manipüle edilebilir. Bu eylem saldırının sonu veya bir sonraki aşamanın başlangıcı olabilir.
- **İcra** (*Execution*): Hedef, saldırganın istediği görevi/eylemi tamamladığında, döngü tamamlanır.

1.6.5 Sosyal Mühendislik Atak Güzergâhı

SM ataklarında izlenen yöntem ve güzergâh, klasik siber saldırı ataklarından (bilgisayar korsanlığından) tamamen bağımsız (ayrıştırılmış) olmamakla birlikte, temel farklılaşma noktaları Şekil 16'da yer alan çizimde görsel olarak açıklanmaya çalışılmıştır. Siber saldırgan teknik bilgi ve araçları kullanarak saldırısını doğrudan sistemlere yaparken, sosyal mühendis ise hedefe erişimini daha çok insan faktörü üzerinden sağlamaya çalışmaktadır.

Şekil 16. Sosyal Mühendislik Atak Güzergâhı



1.7 Sosyal Ağlarda Tersine Sosyal Mühendislik

Facebook, LinkedIn ve Twitter gibi geniş hacimli kullanımlara sahip olan sosyal ağlar insanlara resim ve video paylaşımı, mesajlaşma imkânı, eskiden tanıdığı bir arkadaşıyla yeniden bağ kurma imkânı, haberleri ve günceli takip etme vb. kolaylıklar/hizmetler sunmaktadır. Bu süreç esnasında kullanıcıların etkinlikleri hakkında çeşitli bilgiler toplanmakta (daha çok sınıflandırma, kategorilere ayırma, benzer lokasyonları belirleme vb.) ve bir birini tanıma olasılığı bulunan kullanıcıları

belirlemek için çeşitli analizler yapılmakta ve ilişkilendirilmektedir. Sonraki adımda ise, kişilerin tanıma olasılığı yüksek olan bir kullanıcıyı hesaplarına eklemeleri için otomatik önerilerde bulunulmaktadır. Aynı şey karşı kullanıcı için de geçerlidir. İyi niyetli bir şekilde yapıldığında işler buraya kadar normal gözükmemektedir. Fakat, insanlar genellikle tanıdıkları (güvendikleri) insanlardan gelen soru, bilgi talebi vb. istekler karşısında oldukça cömert davranmaktadır. Esas tehlike ise bu aşamadan sonra başlamaktadır. Sosyal medyayı kullanan saldırganlar, sizi tanıyan bir kişinin kimliğine büründüğünde birçok bilgi açığa çıkarabilmekte ve bu girişim telafisi zor hasarlar bırakabilmektedir.

Herhangi bir güvenlik ihlali saldırısında olduğu gibi, SM saldırılarının da bazı sonuçları vardır. Bu sonuçlar genel olarak şunları içerebilir (Okeyni ve Owens, 2007, s. 4):

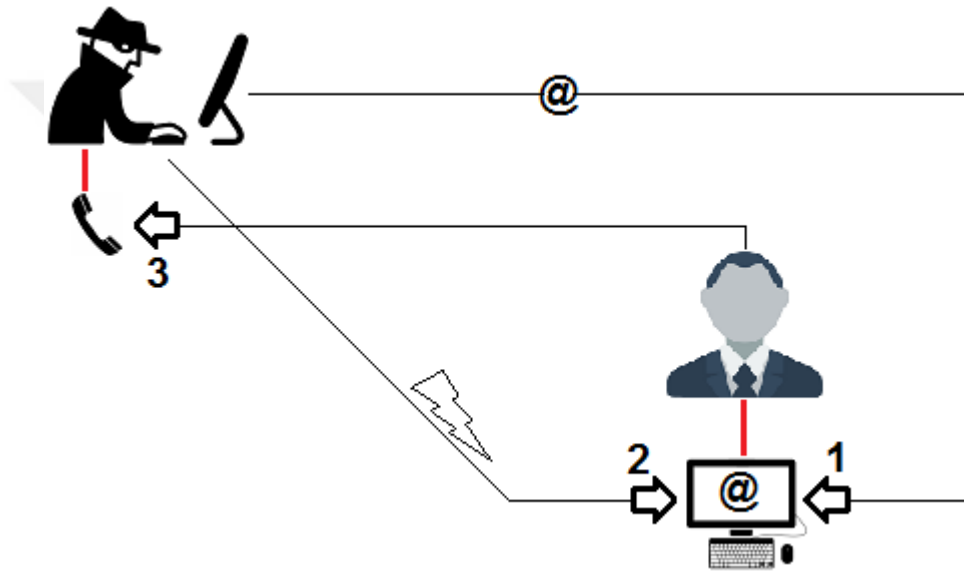
- Halkın güven kaybı
- Hisse senedinin pazar payındaki ve değerindeki düşüş
- Olumsuz medya tanıtımı
- Para cezaları ve diğer düzenleyici sonuçlar
- Muhtemel yasal işlemler
- İlgili düzenleyici makamların gözetim ve müdahalelerinde artış

Çevrimiçi SM saldırılarının yayılması kolay, saldırganın izinin sürülmesi zor ve genellikle hedeflenen kullanıcı başına düşük maliyetlidir. Bunlar saldırganın kurbanlarını etkilemeyi ve kendi adına eylemler gerçekleştirmelerini sağlamayı amaçladığı iyi bilinen tehditlerdir. Saldırgan tipik olarak mağdurları hassas veya önemli bilgileri açığa vurmaları için kandırmakla ilgilenmektedir. Bu saldırıların örnekleri arasında geleneksel e-posta hileleri ve kimlik avı ya da hedef (nokta atışı) avcılığı gibi daha gelişmiş yöntemler de bulunabilir (Irani, Balduzzi, Balzarotti, Kirda, ve Pu, 2011).

Tersine bir SM saldırısında ise, saldırgan mağdurla temas kurmaz. Aksine, kurban saldırganın kendisiyle iletişim kurması için kandırılır. Sonuç olarak, mağdur ile saldırgan arasında yüksek derecede güven tesis edilir, çünkü mağdur görünürde ilk ilişki kurmak isteyen taraftır (Irani vd., 2011). Tersine SM atak güzergahı Şekil 17’de yer alan görsel ile açıklanmaya çalışılmıştır. Örneğin, belirli bir süre öncesinde

hedefteki kişiye eğer sisteminizde herhangi bir teknik hata oluşursa lütfen şu telefon numarasıyla irtibata geçin vb. içerikleri taşıyan bir e-posta (1) gönderilip, birkaç gün sonra, çeşitli yazılım araçlarıyla sistemde bir arıza (2), tıkanıklık vs. yaratılır ve beklemeye geçilir. Bu durumda sorun yaşayan kişi, önceki e-postayı hatırlayarak orada yer alan telefon numarasını arayacak (3) ve yardım isteyecektir. İletişime geçmek isteyen ilk kişi kurbanın kendisi olacağı için, kendisinden istenen bilgileri almak ve istenilen yönde hareket etmesini sağlamak SM saldırısında bulunan kişi için oldukça kolaydır.

Şekil 17. Tersine Sosyal Mühendislik



1.8 Sosyal Mühendisliğin Tehlikeleri ve Tehditleri

SM saldırılarında en zayıf halkanın kişilerden (çalışanlar, kullanıcılar, görevliler vs.) yani insan faktöründen (zafiyetinden) kaynaklı olduğu düşünülmektedir. Bu bilgileri teyit açısından Hadnagy (2017, s. 23)'nin vermiş olduğu şu bilgiler dikkat çekicidir; 2003 yılında Bilgisayar Güvenliği Enstitüsü'nün (CSI) FBI ile yapmış olduğu bir araştırma (şirketlerle yapılan görüşmeler) sonucunda, bu şirketlerin güvenlik açısından en büyük tehlikenin hoşnutsuz bir çalışandan kaynaklanma oranının %77 olarak belirtildiği ifade edilmektedir. Bu oran ilk başta herkese abartılı bir oran gibi gelebilir fakat aynı araştırma sonucunda aşağıda verilen (şirketlerin görüşleri doğrultusundaki) diğer bilgiler bu konuda oldukça ikna edici gözükmemektedir;

- İş yerlerinde müşteri verilerinin tehlikeye atılabileceği (kimlik hırsızlığı) oranı %62.
- Hacker’lardan ziyade iş arkadaşlarının müşteri mahremiyetini tehlikeye atabileceği yönündeki görüş bildirenlerin oranı %66.
- Şirketlerde tutulan hassas verilerin, çalışanlarca “kolay” ya da “çok kolay” bir şekilde dışarı çıkarılabileceği oranı %46.
- Veri korumayla ilgili şirket politikasından habersiz çalışanların oranı %32’dir.

Check Point tarafından desteklenen ve amacı SM saldırıları ve bunların iş hayatı üzerine etkileri algısı hakkında veri toplamak olan, Temmuz ve Ağustos 2011’de Amerika Birleşik Devletleri, Birleşik Krallık, Kanada, Avustralya, Yeni Zelanda ve Almanya’da 853 Bilgi Teknolojileri (BT) uzmanı üzerinde yürütülen küresel bir ankete dayanan araştırma raporunda özetle şu bilgilere yer verilmiştir (Dimensional Research, 2011):

- SM tehdidi gerçektir;
 - Güvenlik uzmanlarının %97’si ve tüm BT uzmanlarının %86’sı bu potansiyel güvenlik tehdidinin farkındaydı veya yüksek düzeyde farkındaydı.
 - %43’ü SM programları tarafından hedeflendiklerini bilmekteydi.
 - Sadece %16’sı SM tarafından hedef alınmadığından emin, %41’i ise saldırıya uğrayıp uğramadıklarını dahi bilmiyordu.
- Finansal kazançlar, SM’nin temel motivasyonudur;
 - SM saldırılarının %51’i maddi kazançla motive olmuştu.
 - SM saldırılarının %14’ü intikam hırsınca motive edilmişti.
- SM saldırıları özellikle büyük kuruluşlarda maliyetlidir;
 - Son iki yılda büyük şirketlerin %48’i ve her büyüklükteki şirketin %32’si 25 veya daha fazla SM saldırısı geçirmişti.
 - Tüm katılımcıların %48’i, olay başına ortalama 25.000 ABD dolarının üzerindeki bir fiyattan (maliyetten) bahsetmektedir.
 - Büyük firmaların %30’u, olay başına 100.000 ABD dolarının üzerindeki bir maliyetten bahsetmektedir.
- SM tekniklerine karşı en çok risk altında olanlar yeni çalışanlar;

- Yeni çalışanlar %60, yükleniciler %44 ve yönetici asistanları %38 oranında SM teknikleri açısından yüksek risk altında.
- SM saldırılarını önlemek için proaktif eğitim eksikliği bulunmakta;
 - Katılımcıların sadece %26'sı sürekli eğitim almakta.
 - Ancak %19'unun eğitim almak için bir planı varken, %34'ü şu anda çalışanlarını eğitmek için herhangi bir girişimde bulunmamakta.

Verizon Veri İhlali Araştırmaları Raporunda, 2011 yılında 36 ülkede çeşitli kuruluşlarda meydana gelen 855 olay örneğinin analiz edildiği ve yaklaşık 174 milyon kayıtlın tehlikeye girdiği belirtilmiştir. En az 1.000 çalışanı olan büyük organizasyonlarda 60 olayın, 1.000'den az çalışanı olan kuruluşlarda ise 660 olayın meydana geldiği, geriye kalan kuruluşlardaki olay sayısının ise bilinmediği ifade edilmiştir. Bu rakamlar, büyüklüğü ve coğrafi konumu ne olursa olsun her kuruluşun, her türlü güvenlik saldırısı için potansiyel birer hedef olduğunu göstermektedir. Dışsal ajanların veri ihlallerinin %98'inden sorumlu olduğunu, saldırganların %7'sinin SM taktiklerini uyguladığını, daha büyük organizasyonlarda ise, SM saldırılarının %22'ye ulaştığını, bunun da SM için hedef olma olasılığının daha büyük kuruluşlar için daha yüksek olduğu anlamına geldiği ifade edilmiştir (Quiel, 2013, s. 1).

SM, sanal topluluklarda ciddi bir tehdit olarak ortaya çıkmıştır ve bilgi sistemlerine saldırmanın etkili bir yoludur. Günümüz bilgi çalışanlarının kullandığı hizmetler, sofistike SM çalışmaları için zemin hazırlamaktadır. Kendi Cihazını Kendin Getir (BYOD: Bring Your Own Device) politikalarına yönelik artan eğilim ve özel ve iş ortamlarında çevrimiçi iletişim ve işbirliği araçlarının kullanılması sorunu daha da kötüleştirmektedir (Krombholz, Hobel, Huber ve Weippl, 2015). Bu uygulama işverenler açısından ekonomik ve iş görenler açısından mobil, kullanışlı ve sempatik olmakla birlikte, organizasyonların (iş yerlerinin) bilgi teknolojileri güvenlik standartlarını ve korumalarını kısmen de olsa devre dışı bırakarak ön görülemez zararlara yol açabilmektedir. Sonuçta kişisel bilgisayarlar ve/veya ekipmanlar iş yerindeki network aracılığıyla internete çıkış yapmak durumunda ve/veya çeşitli proje çalışmaları için yerel ağa bağlanmak zorundadır. Bu tür

kullanımlar için yeni güvenlik önlemleri ve kullanım standartları geliştirmek zaruridir.

Siber güvenlik şirketi Agari, 2016 yılında ankete katılan ticari işletmelerin %60'ının geçtiğimiz yıl boyunca SM saldırılarına maruz kaldıklarını, ayrıca, ankete katılanların %89'unun aynı yıl SM saldırılarında sürekli bir artış gördüklerini ifade ettiklerini belirtmektedir. İşletmelere güvenlik danışmanlığı sağlamak için profesyonel bilgisayar korsanlarını kullanan bir şirket olan Social Engineering Inc., sosyal mühendisliği “en az dirençli yol” olarak adlandırıyor ve işletmelerin saldırılara karşı her zaman risk altında olduğunu çünkü eğitimsiz kullanıcılar için herhangi bir “yama”nın olmadığını belirtiyor (www.tsys.com).

Birleşik Devletler Ulusal İstihbarat Yönetim Ofisi ve İç Güvenlik Departmanı, 2017 Kamu-Özel Analitik Değişim Programı, *Fidye Yazılım ve Sosyal Mühendisliğin Geleceği* başlıklı çalışmasında “Fidye Yazılımı ve Sosyal Mühendislik Atakları” için önümüzdeki iki yıllık süreçte neler olabileceğine dair değerlendirmelerini şu şekilde özetlemektedir:

- Fidye-yazılımı⁴ finansal olarak motive edilmiş siber aktörler tarafından kullanılmaya devam ederken, inkâr ve aldatma gibi diğer amaçlar için artan bir şekilde kullanılmaya devam edecek veya diğer siber tekniklerle birleştirilecektir.
- Siber suçlular mağdurdan ek fidye almak için çevrimiçi veri yayınlama tehdidinde bulunabilirler.
- Bir fidye yazılımı saldırısı, bir kuruluşun tüm yönlerini etkileyebilir. İlk etki, mağdurun fidyeyi ödeyip ödememesiyle sınırlı olsa da, bir saldırının uzun vadeli etkileri çok daha kapsamlı ve maliyetli olabilir.
- Fidye yazılım araçlarının çoğalması nedeniyle saldırıların sayısı artacak.
- Fidye yazılım saldırıları muhtemelen Nesnelerin İnterneti (IoT) cihazlarının hedeflenmesini içerecek şekilde genişleyecektir.

⁴ **Fidye-yazılımı (ransomware):** Fidye-yazılımı, bilgisayara ya da network servis sağlayıcılarına gasp amacıyla (genellikle uzaktan erişimle) kurulmuş/yüklenmiş zararlı kod barındıran yazılımdır. Kötü amaçlı yazılım, kurbanın verilerini ve/ya sistemlerini okunamaz/kullanılamaz hale getirerek şifreler. Mağdurdan, kilitlenmiş dosyaların şifresini çözmek ve/ya tekrar erişim kazanmasını sağlamak için (saldırgana) parasal bir ödeme yapması beklenir.

- SM, bir siber suçlunun bir fidye yazılımı saldırısı yapmak için bir bilgisayar sistemine erişmesi için en kolay yollardan biri olmaya devam edecektir. Bu bilgiyi toplamak için teknolojiyi ve insan manipülasyon yöntemlerini içeren çeşitli tekniklerin kullanılmasına devam edilecektir.

İnsanlar yaptıkları bağılıkları desteklemek için yeni sebepler ve bahaneler üretirler. Bu süreç içerisinde bazı bağılıkların gerekçesi olan sebepler ortadan kalksa bile bağılıkları devam eder (Cialdini, 2018, s. 155), en azından devam etme eğilimindedir. Bu süreç siyasi partilerin, hükümetlerin verdiği sözleri ya da ilk dönem göstermiş oldukları olumlu performansları göstermeseler dahi oy almaya/destek bulmaya devam etmelerine kısmi bir açıklama olabilir.

Ashford (2018), güvenlik firması olan Positive Technologies'nin, insan faktörünün işletmeleri nasıl risk altına soktuğuna dair hazırlamış olduğu bir raporuna dayanarak SM'nin halen siber saldırı ataklarının en güçlü araçlarından biri olduğunu belirterek şu verilere dikkat çekmektedir; 10 kadar sızma (penetrasyon) testi aracılığı ile 3.300 den fazla mesaj gönderilip, bunlardan %17'sinin başarılı olduğu tespit edilmiştir. Eğer bu ataklar gerçek saldırganlar tarafından düzenlenmiş olsalardı, çalışanların iş bilgisayarları belki de iş yeri bilgisayar ağının tamamı bu saldırıdan etkilenecekti. Rapora göre, en etkili SM saldırılarından birisi, gönderilen linke tıklanarak belirli bir (genelde sahte) web sayfasına yönlendirilmedir. Raporda, tuzak bir link içeren e-postalara, kullanıcılardan %27'sinin dikkatsizce tıkladığını ve sonrasında yönlendirildikleri adreste aslında sahte bir web sitesini ziyaret etmekte olduklarını bilmediklerini (adrese dikkatlice göz atmadıklarını veya umursamadıklarını) belirtmektedir. Yapılan bu sızma testleri, çalışanlardan %15'inin "ek" içeren e-postaları ve linkleri, %7'sinin ise e-posta ek'ini tıkladığını göstermektedir. Rapor, çalışanların genellikle bilinmeyen dosyaları açtığını ve şüpheli bağlantıları tıkladığını da belirtiyor: Bunu yapanların sayısı, çalışanlarda, muhasebecilerde, avukatlarda, yöneticilerde ve Bilgi İşlem Bölümü dışındaki çalışanlarda %88, müdür ve amirlerde ise %25. Ayrıca, güvenlik uzmanlarından dahi %3'nün bu gruba dâhil olduğu ifade ediliyor. Raporda, dosyaları açamayan ya da sahte sitelerde şifrelerini kırk defaya kadar deneyerek girmek isteyenlerin olduğu, bunlardan bir kısmının dosyayı bilgi işlem bölümüne gönderdiklerini, bilgi işlemde

alıřanların da kendi personelinden gelen bu dosyaya gvendiđini belirtiyor. Raporda, sahte bir řirketten gnderilen mesajlardan %11'inin iře yararlıken, tanıdık bir kiři ya da řirketten gnderilen mesajlarda bu sayının belirgin bir řekilde artarak %33'lere ıktıđı ifade ediliyor. Aynı raporda, siber suluların saldırılarını daha etkin hale getirmek iin kurbanın korku, ađzllk, umut ve diđer duygularına yneldikleri belirtilmektedir. Dikkatlice/kurnazca seilen mesaj konuları bu srete olduka etkili olabilmektedir. rneđin "iřten ıkarılacakların listesi" konu bařlıđı ile gnderilen mesajlara %38, "yıllık ikramiye" iin ise %25'lik bir tıklanma olduđu belirtiliyor.

1.9 Sosyal Mhendislik Saldırılarından Korunma Yntemleri

Mitnick ve Simon (2001), Albert Einstein'ın, "*Sadece iki řey sınırsız; evren ve insanın aptallıđı, ilkinden emin deđilim.*" szn hatırlatarak, SM saldırılarının, insanlar aptal olduđu srece veya daha genel olarak iyi gvenlik uygulamaları konusunda bilgisiz kaldıklarında bařarılı olabileceđine (s. 12) vurgu yapmaktadır.

Norton antivirs programının reticisi Symantec firmasının gvenlik teknik direktr, kt niyetli kiřilerin bilinenin aksine genellikle iřletim sistemindeki teknik gvenlik aıklarından yararlanmaya alıřmadıklarını, bunun yerine kiřilerin peřine dřtklerini, insanların zayıf anlarını ve zayıf yanlarını kullanarak (SM yaparak) zararlı ierik barındıran bir eki amaya istekli olabileceklerinden yola ıktıklarını, saldırganlar aısından ok fazla teknik beceriye ihtiyaın bulunmadıđını ifade etmektedir. Kt amalı yazılımların yalnızca %3'nn teknik bir istismarı denerken, kalan %97'lik kısmın kiřilere uygulanan SM'den oluřtuđunu belirtmekte ve son savunma hattının kiřilerin kendilerinin olduđunu eklemektedir (www.knowbe4.com).

Guenther (2001), SM ataklarına karřı giriř dzeyinde de olsa herkesin kolayca uygulayabileceđi ve iře yarayacađını nerdiđi drt adımlık sreci řu řekilde aıklamaktadır:

1. Adım: Kendiniz veya bir bařkası hakkında kiřisel bilgiler isteyen (ađrı numarası veya alıřan numarası dhil), bilgisayar sisteminiz hakkında bilgi veya diđer hassas bilgiler iin arayan bir kiřiye kiřisel olarak tanımlayamıyorsanız, bilgi vermeyin. Arayanın kimliđini, (řirket adı) telefon rehberinde listelenen uygun telefon numaralarından tekrar arayarak

doğrulamakta ısrar edin. Bu prosedür, potansiyel zararların kapsamı ile karşılaştırıldığında kesinlikle asgari düzeyde sıkıntılı bir önlemdir.

2. Adım: Şifrelerin hassas olduğunu unutmayın. Kişisel hesabınız için bir şifre sadece sizin tarafınızdan bilinmelidir. Hesabınıza bir şey yapması gerektiğini söyleyen sistem yöneticileri veya bakım teknisyenlerinin şifrenizi bilmelerine ihtiyaçları yoktur. Onların, şifre veya benzer bilgilerinizi ifşa etmenize gerek kalmadan hesabınızda çalışabilmelerini sağlayacak sistem ayrıcalıklarına sahip kendi şifreleri vardır. Bir sistem yöneticisi veya bakım yapmak istediğini söyleyen bir teknisyen sizden şifrenizi sorarsa şüphe duymalısınız.

3. Adım: İşyerinize dışarıdan gelen sistem bakım teknisyenlerine işyerinizin kendi sistem yöneticisi eşlik etmelidir (sizin tanıdığınız biri). Sistem bakımı için gelenler size tanıdık gelmiyorsa bunu kontrol etmek için sistem yöneticinize bir çağrı yapmanız akıllıca olur. Ne yazık ki, birçok insan bunu yapmakta isteksizdir. Çünkü genellikle, bu durumun kendilerini paranoyak göstereceğinden endişe etmekte ve/ya bir ziyaretçiye güvenmediklerini göstermenin utanç verici olduğunu düşünmektedir.

4. Adım: SM girişimi tarafından engellendiğinizi veya belki de mağdur edildiğinizi düşünüyorsanız, olayı derhal yöneticinize ve güvenlik personeline bildirmelisiniz.

Son on yılda, sofistike teknikler sayesinde SM saldırılarında ve uygulamalarında önemli artışlar meydana gelmiştir. Araştırmacılar, sistem yöneticileri, ağdaki zayıf düğümleri temsil eden bireyleri (kullanıcıları, iş görenleri) tanımlamak için kendi kuruluşlarına (örneğin kimlik avı e-postaları, spam vb.) karşı (test ve önlem amaçlı) SM teknikleri kullanmaya başlamışlar, bunun sonucunda da ortaya *iç sosyal mühendislik* kavramı çıkmıştır (Hatfield, 2018, s. 108). SM saldırılarından korunmak için bu saldırıyı düzenleyenlerin düşünce biçimlerini ve saldırı tekniklerini öğrenmek gerekmektedir. Hırsızların ev sahibinden, hacker'ların güvenlik duvarlarını kuranlardan, virüslerin anti-virüslerden hep bir adım ileri de olduğunu da unutmamak gerekir. Korunma sistemleri (yöntemleri) genel olarak savunmaya yönelik (defansif) çabalar içerir, oysa bazen en iyi savunma yöntemi

saldırmaktır (ofansif). Bu saldırılar genellikle sistemi test etme, sızma (penatrosyon), tatbikat yapma, yani kendi hacker'larınızı ve kendi sosyal mühendislerinizi hazırlamak (kullanmak) şeklinde yürütülebilir.

SM saldırılarından korunmanın en temel yöntemlerinin başında hiç şüphesiz konuyla ilgili temel düzeyde de olsa bilgi edinilmesi, genel saldırı tekniklerinin ne olduğunun derinlemesine olmasa da öğrenilmesi gelmektedir. Bunun yanı sıra, güvenlik ya da bilgi teknolojileri uzmanlarının SM tekniklerini kullanarak düzenli olarak sızma (penetrasyon) testleri düzenlemeleri uygun olacaktır. Bu testler sonucunda elde edilen bilgiler, zayıf yönler, dikkatsiz çalışanlar vb. tespit edilerek hem çalışanlara hem de yöneticilere bu bilgileri sunmak ve gerekli önlemlerin alınması için açıklayıcı ve uyarıcı bilgilendirme toplantılarının yanı sıra hizmet içi eğitimlerinin de verilmesi gerekmektedir. Yazılımların güncel olması, güvenlik yamalarının zamanında indirilmesi, güvenlik duvarı yazılımlarının aktif olması, anti-virüs programlarının bulunması gibi önlemler her ne kadar bilgi güvenliğinin alanı içine giriyor gibi gözükse de SM uygulamalarının (saldırıların) bir sonraki adımını içerdiklerinden, bu önlemlerin de SM ataklarından korunma yöntemleri içerisinde bütünleşik ve ilişkisel düzeyde ele alınması oldukça faydalı olacaktır. Özellikle küçük işletmeler ve kişisel korunmalarda bu böyledir.

Araştırmalar gösteriyor ki “Bütün saldırıların/hacklemelerin %30'u dış kaynaklardan (saldırıya uğrayan örgüt için çalışmayan insanlardan) geliyor. Bu durum saldırıların %70'inin örgütün kendi içinden geldiği anlamına geliyor. Sosyal mühendislere karşı savunma geliştirirken bu gerçeğin akılda tutulması gerekmektedir” (Peltier, 2006 Akt: Major, 2009, s. 43).

Karşılıklı bulunma ilkesini uygulayan biriyle karşılaşıldığında, zorlu bir düşmanla karşı karşıya kalınmış demektir. Bu kişi bize ilk iyiliği yaparak itaat etmemiz için güçlü bir sebep kazanmış olur. Bu talebi yapan kişinin ilk iyiliğini veya tavizini reddederek problem çözülebilir. Buradaki asıl sorun yeterince dikkatli olunmadığında, sunulan teklifin dürüst mü yoksa istismar amacıyla mı yapıldığı anlaşılmadığında, gelen teklifleri olduğu gibi reddetmek iyi kişiler tarafından gelecek iyilik ve tavizlerden olmamıza sebep olabilmektedir (Cialdini, 2018, s. 82-83).

Bilgisayarlardan bilgi elde etmek için yetkisiz yazılım kurulumu söz konusu olduğunda, insanlar çok daha dikkatlidirler, ancak özellikle SM baskısı altındaki kişiler bununla başa çıkma konusunda yetersiz kalmaktadır. İnsanlar yabancılara ya da pek tanımadıkları kişilere kısmen de olsa güvenme eğilimindedirler; ya görmezden gelindiklerinden ya da fark edilmeye istekli olmalarından dolayı çalışmaları hakkında (kıymetli ya da az kıymetli) bilgi paylaşmayı kabul ederler. Bu sorunun çözümü, işlerinden bağımsız olarak çalışanların, SM'nin tehlikeleri hakkında bilgilendirilmesi ve eğitilmesi ile mümkün olabilmektedir (Şerban ve Şerban, 2014, s. 6).

Sosyal medya sitelerini izleme araçları, kuruluşların kötü niyetli etkinlikleri ve onlara yönelik tehditleri izlemelerine yardımcı olabilir. Kuruluşlar/Kurumlar sosyal medya içeriğini (trafiğini) analiz ederek içeriden kaynaklı tehditleri tespit edebilir. Eğitim ve öğretimi en iyi teknolojiyle birleştirmek, SM risklerini ve zararlarını azaltabilir (Tayouri, 2015, s. 1096).

Önceki bölümlerde anlatılan SM saldırı tipleri, yöntemleri ve içeriklerinden hareketle ister kişisel isterse kurumsal düzeyde olsun alınabilecek birçok önlem bulunmaktadır; daha önce de belirtildiği üzere bu önlemlerin en başında SM saldırılarının neler olduğu hakkında bilgi edinmek ve buna karşı önlemler geliştirmek için bilgi sahibi olmak, yani eğitim gelmektedir. Şüpheli SM saldırısı her nereden gelirse gelsin, ister telefon aramaları, mesajlar, e-postalar, ya da fiziksel temasla, bunlara karşı ne tür bir karşılık verileceğine dair açık politikaların belirlenmesi gerekmektedir ve sonrasında bu politikaların açık bir şekilde ilgili kişilere iletildiğinden emin olunması uygun olacaktır. Bu politikalara uygun hareket edenler ödüllendirilmeli, eksikleri olanlar için ise çeşitli eğitimler düzenlenmelidir. Social-engineer.org sitesine göre, hangi tür saldırılardan nasıl korunulacağına dair bazı ip uçları Tablo 6'da verilmiştir.

Tablo 6. Bazı Sosyal Mühendislik Ataklarından Korunma Yöntemleri ve Önlemler

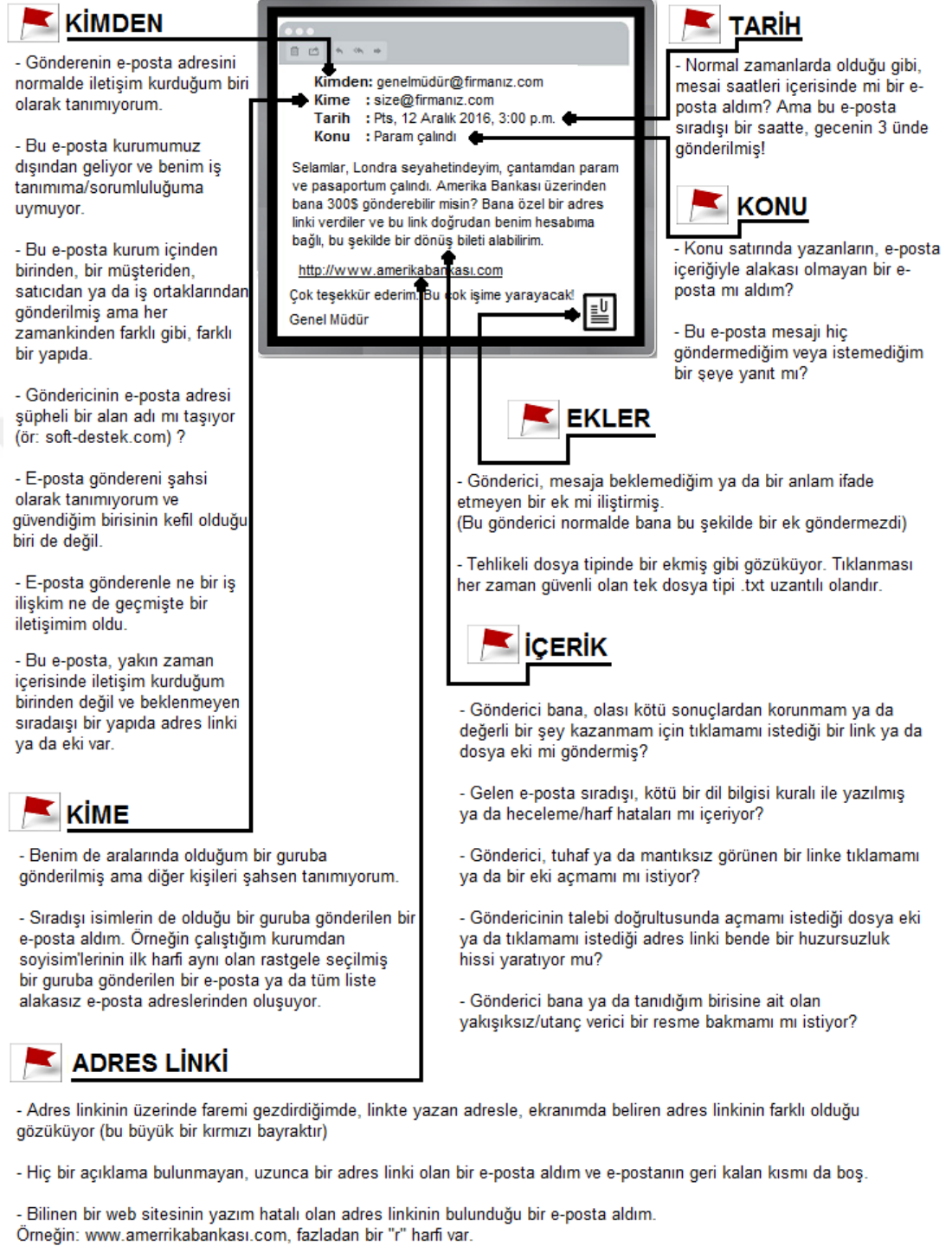
Phishing Yemleme / Kimlik Avı (e-posta ile)	Bu tür aldatmacalara karşı korunmanın en iyi yolu, size şüpheli görünen herhangi bir şeyi açmamaktır. Teknik destek, kullanıcı adınızı ve şifrenizi ASLA istemez, ihtiyaçları olduğunda ona zaten erişebilir. Eğitimli kullanıcıların bu tür saldırılardan korunabilmeleri için mükemmel bir yol vardır; URL linklerindeki yazım hatalarını kontrol etmek ve fareniz ile linkin üzerine konumlanarak bu linkin sizi gerçekte nereye götürmek istediğine bakmak.
Vishing Sesli Kimlik Avı (telefon ile)	Bu tür saldırılara karşı korunmanın en iyi yolu kiminle konuştuğunuzu onaylamanın bir yolunu bulmaktır. En iyi uygulama, kimlikleri doğrulanmayan kişilere hiçbir şekilde bilgi verilmemesi politikasıdır. Arayanı geri arayabilmek için telefon, firma ismi gibi bilgileri isteyin, amatör kişiler bu aşamada saldırıdan vaz geçer ama daha profesyoneller size onları geri arayabileceğiniz bir numaraya sahip olabilirler, dikkatli olun. Kurum içindenmiş gibi düzenlenen ataklara karşı ise İK bir tür doğrulama önlemi almalıdır.
Tech Support Teknik Destek	Bilgisayarlarınıza erişim için teknik destek ekibi gibi davrananlara karşı önlem için bir doğrulama politikası geliştirilebilir; teknik ekipten olanların kimlik ya da rozetlerinin arka tarafına bir doğrulama kodu iliştilerilebilir ya da daha karmaşık bir etiketleme sistemi kullanılabilir. Ayrıca personelin bu doğrulamanın ne zaman ve nasıl yapılacağına dair bilgilendirilmesi (eğitilmesi) de gereklidir.
Delivery Person Kurye	Bu tür atakların önüne geçmek biraz zordur ama bazı politikalarla çözüm aranabilir; örneğin, kuruma gelen teslimatlar yalnızca belirli bir yerde (odada) teslim alınabilir. Kişiye doğrudan teslimat şart ise, bir görevli kuryeye eşlik etmelidir. Eğer gelen kuryenin kim olduğundan şüpheleriniz varsa geldiği firmayı arayıp teyit edebilirsiniz. Şüpheleriniz varsa (kurye sahte bir kimlik kartı edinmiş olabilir) teyit edici sorular sorabilirsiniz.
Impersonation/Physical Attack Kimliğe Bürünme / Fiziksel Saldırı	Kimliğe bürünme saldırılarından korunmanın en önemli yolu çevrede olup bitenlerin farkında olmaktan geçer. Etkinliğe/içeriye kimlerin giriş sağlayabileceği ve giriş kuralları net olarak belirlenmelidir. Saldırganlar, hedeflerindeki kalabalığın dikkatsizliğinden ya da onların nezaketlerinden yararlanmak isteyecektir.
USB Drops Ortalığa USB Bellek Bırakma	Teknik ekipten, içerden ya da dışarıdan birisinin USB sürücünüzü kullanma yetkisi var mı? Bununla ilgili kurumunuzda bir politika var mı? Önce bunu öğrenmelisiniz. Ortalığa bırakılmış (gibi) duran USB bellek ya da CD'leri kullanmayın. Şirketler kurum içerisinde bulunan USB bellek veya CD'lerin belirli bir yere ya da kişiye teslim edilmesi kuralını uygulayabilirler. USB okuyucu portları (belli alandaki bilgisayarlar için) kullanıma yazılımsal olarak kapatılabilir.

Kaynak: <https://www.social-engineer.org/framework/attack-vectors/how-can-you-protect-yourself-against-common-attacks/> adresinden uyarlanmıştır, Erişim: 06.12.2018

Teknoloji, kişileri ya da kurumları (tam olarak) SM'den koruyamaz çünkü SM ataklarında güvenlik duvarı, Web sunucusu veya veri tabanı hedef değildir: Teknoloji hedef olsaydı, karşı korunmak daha kolay olabilirdi. Sorun, bir kişiyi yeniden programlamanın kolay olmamasıdır. Ancak birçok eğitim seansı ve güvenlik denetimleri işe yarayabilir. Buna rağmen halen insani duygularla hareket etme olasılığı vardır. Esasında, SM ataklarından korunmanın başında, yönetim kurulu tarafından açıkça tanımlanmış ve onaylanmış bir kurumsal politikaya ihtiyaç vardır. En kapsamlı haliyle, insan kaynakları, BT güvenliği, fiziksel güvenlik ve tesis yönetimi (binalardan, resepsiyondan vb. sorumlu olanlar) ve ilgili iş birimlerinden yetkilendirilmiş temsilcileri içeren bir komite gerektirmektedir (Barber, 2001).

Knowbe4.com web sitesinde, e-posta üzerinden yapılabilecek SM saldırılarına karşı kullanıcıların saldırılardan korunabilmesi için ilk başta dikkat etmeleri gereken temel bilgiler “22 Sosyal Mühendislik Kırmızı Bayrağı” başlığı altında derlenmeye çalışılmıştır. Şekil 18’de bu derlemeye ait detaylar yer almaktadır.

Şekil 18. Sosyal Mühendisliğin Kırmızı Bayrakları (Belirtileri)



Kaynak: <https://www.knowbe4.com/what-is-social-engineering/> adresinden uyarlanmıştır, Erişim: 03.12.2018

Daha önceki başlıklar altında bahsedilen “çöp atıkları” konusuna da yeterince özen gösterilmesi gerektiği düşünülmektedir. Çöplerden elde edilebilecek bilgilerin ne kadar geniş olabileceğini artık biliyoruz. Buradaki bilgilerin sosyal mühendislerin eline geçmemesi için gelişmiş öğütücülerin kullanılması gerekmektedir. Öğütücü kullanılmıyorsa, evraklarda yer alan önemli bilgilerin (özellikle el ile yazılmış şifre, isim, hesap numarası, tel vb.) önüne arkasına çeşitli harf ve rakamlar eklendikten sonra keçeli kalemlemlerle üzerleri çizilip imha edilmelidir. Önemli bilgiler içerebileceği düşünülen evrakların imhasından sonra mümkünse atılan çöplerin hepsi aynı çöpe atılmamalıdır. Üst düzey gizliliği olan evrak imhalarında (eğer kurumda imha gerçekleştiriliyorsa, protokollere uygun imhanın gerçekleştirilmesi gerekmektedir) su ile ıslatma, hamur haline getirme ya da yakma gibi yöntemler kullanılabilir. Bilgisayar diski (HDD) gibi çok daha fazla bilgiyi barındıran parçaların imhasında (imhası zor olan parçalardır) matkapla çoklu delik açma ve benzeri yöntemler yeniden kurtarmanın (recovery) önüne geçebilir.

SM ataklarından korunmak, donanımın (fiziki ya da yazılımsal) güvenliğini sağlamak kadar kolay değildir. Geleneksel savunmacı güvenlik ile çevre güvenliğini sağlamak için izinsiz girişleri tespit etme sistemlerine, güvenlik duvarlarına, anti virüs programlarına ve başka çözümlere önemli miktarlarda para harcanabilir fakat SM söz konusu olduğunda, çalışanlara/personelere takılabilecek (koruyucu) bir program yoktur (Hadnagy, 2017, s. 355). SM saldırılarıyla başa çıkabilmek için, daha çok eğitim ve bilgilendirme çalışmalarının yapılması gerekmektedir. Çeşitli prosedürler ve standartlar oluşturmak ve düzenli aralıklarla bu bilgileri güncellemek ve uygulamasını (tatbikini) yapmak oldukça etkili ve faydalıdır.

İnsanlar doğası gereği (çoğunlukla) yardıma ihtiyacı olduğunu hissettiği (daha ziyade emin olduğu) durumlarda yardım etme eğilimindedir. Bu davranış şekli sosyal mühendislerin çok iyi bildiği ve tatbik ettiği bir konudur ve bu nedenle bazı durumlarda bu yola başvurmaktan (yardımınıza ihtiyaçları varmış gibi davranmaktan) hiç kaçınmazlar. Bu nedenle talep edilen yardıma gerçekten ihtiyaç olup olmadığı konusu dikkatli bir şekilde ele alınmalıdır. Bu durum normal seyrine devam eden yaşam süreci içerisinde oluşabilecek durumlar için değil, bir SM saldırısının söz konusu olabileceği durumlar için önerilmektedir.

SM ataklarından korunabilmek için kurumların (eksiklikleri ve açıkları yerinde tespit edebilmek ve önlem almak için eğitim amaçlı düzenlenen) SM ataklarını simüle etmesinde sayısız fayda vardır. Yalnız, bu testler yapılırken, ulusal güvenlik yasalarına ve kanunlara, kişisel yaşama ve kişisel hayatın gizliliği ve benzeri pek çok konunun ihlal edilmemesine dikkat edilmelidir. Birçok alan için geçerli olan reaktif değil, ön alıcı (proaktif) önlemlerin uygulanması SM saldırıları için de geçerlidir. Ön alıcı önlemlerin açıklarını da test amaçlı önceden tasarlanmış ataklarla ortaya çıkarmak, güvenlik kalkanlarını daha güçlü hale getirecektir. Test amaçlı önceden tasarlanmış ataklar içerisinde yer alabilecek bazı örneklerle aşağıda yer verilmiştir;

- Güvenli kabul edilen alanlardan, girişlerden, geçiş ve kontrol noktalarından izinsiz giriş yapmaya çalışmak.
- Bu alanlarda görev yapanları çeşitli SM saldırı tekniklerine maruz bırakarak sonuçları gözlemlemek ve not etmek (kişi ve/ya birim bazında).
- Kamera ve hareket sensörlerinin çalışıp çalışmadığını ve doğru açılarda olup olmadığını kontrol etmek.
- Çalışanlara tanımadıkları, güvenmedikleri yerlerden gelen e-postalar ve linkler göndererek kimlerin ve ne kadarının dikkatli davranıp davranmadığını saptamak.
- Kurum içerisinde çeşitli yerlere CD, USB bellekler bırakılıp bunların bilgisayarlara takılıp takılmadığı veya nereye teslim edilmeye çalışıldığını izlemek.
- Önemli bilgileri barındıran birimlerde çalışan personelden kurum içinde ve kurum dışında bilgi sızdırılıp sızdırılamayacağının kontrolünü yapmak (toplantı, kutlama, kafeler gibi yerlerde sohbet içerikli girişimler başlatılarak test edilebilmektedir).
- Kurum içerisinden dışarı çıkmaması gereken bir bilgi, evrak ya da malzeme için çeşitli taleplerle personel üzerinde deneme girişimleri yapmak.

Medya aracılığıyla yapılan algı yönetimi, yönlendirme ve SM çalışmaları için bir tür doğrulama (doğrulayıcı/referans merkez birimi) mekanizması geliştirilebilir. İnternet sitelerinin güvenliği (daha çok e-ticaret) için geliştirilmiş olan SSL (Secure

Sockets Layer) protokolüne benzer bir yapı inşa edilebilir. Örneğin, “doğrulayıcı/referans merkez birimi” tarafından içerik/haber doğrulaması almış haber/duyuru/ilan ve benzerlerinin bir logo/ikon/sembol ile temsil edilmesi vb. Hâlihazırda, tüm dünyada doğrulama (confirmation) platformları oluşturulmaya çalışılıyor. Çavuş (2018, s. 55) bu konu için şu açıklamaları yapmaktadır;

Medyaya olan güvenin azaldığı bilgi ortamında haber tüketicilerinin karşısına bu güvensizliği dengede tutması beklenen yeni araçlar çıkıyor. Bunların başında tüm dünyada hızla yaygınlaşan doğrulama platformları geliyor. Doğrulama, siyasetçilerin söylemlerini doğrulama temelli çalışanlar (fact-checking) ve özellikle kullanıcı üretimi içerikleri ve medyayı doğrulama temelli çalışanlar (verification) olarak ikiye ayrılabilir.

Öğrenen algoritmalar sayesinde ve yapay zekâ platformlarında “büyük veri”yi kullanarak yakın gelecekte daha tutarlı içerik, ses, görüntü ve vücut dili analizlerinin yapılacağına hiç şüphe yok. %100 tutarlılık/doğrulayıcılık göstermeyecek olsa da, birçok konu ve alan için %95’ler civarında olması, yeterli ilgiyi bu platformlar üzerinde toplamaya yetecektir. İçerik doğrulamanın neden çok önemli olduğunu basit bir örnekle açıklamak gerekirse, örneğin birden fazla gazeteyi aynı haber için çapraz okuma yapan bir okuyucu olduğunuzu hayal edin, aynı haberle ilgili iki “büyük” gazetenin birinde kazada ölen kişinin “anne”, diğesinde ise ölen kişinin “kızı” olarak karşınıza çıkması olasıdır. Ya da tren kazasında ölü sayısını bir gazete 10 olarak duyururken, diğeri bu rakamı 30 olarak duyurabilmektedir. Bunların muhabir dikkatsizliğinden kaynaklı hatalar olduğunu varsayalım (bu verilen yanlış haber için bir özür değildir elbette). Peki medya tarafından yanlış bilgiye maruz bırakılmak istenen kitlelere karşı, güven duyulan ya da tanınmış kişilerin bu haberlerde kullanılması nasıl önlenebilecek? Bu durum zihinlerde önemli bir soru işareti oluşturmaktadır. Sonuç olarak doğrulama kaynaklarına gerçekten ihtiyaç duyulduğu açıkça ortadadır. Tekzip mekanizmasının ise yeterince işe yaramadığı çoktandır bilinmekte. Çavuş (2018) bu konuyla ilgili açıklamasını şu şekilde dile getiriyor; 1985 yılında psikologların ortaya atmış olduğu “tekzipteki netlik” kavramına göre, insanlar bir bilgiyi diğeri bilgiyi silmek üzere kullanmadıklarını ve bu nedenle basit inkâr ve ikazların tek başına bilgiyi şekillendirmediği ve bu bilgiyi alırken insanların diğeri (önceki) bilgiyi de depoladıklarını (s. 66) belirtiyor. “Çamur at izi kalsın” deyiimi buna verilecek iyi bir

örnektir. Ne yazık ki bazı durumlarda medya, olayları bildirme/doğrulama aracı olması gereken yerde, yanlışları doğrulama aracı olabilmektedir. Spinoza ise, insanların gerçeği sevmenin önüne geçemeyeceklerine inanıyordu. Spinoza'ya göre, insanlar gerçeği sevmek durumundadır. Çünkü hayatta kalmaları, kendilerini anlamaları ve kendi gerçek doğalarıyla uyum içinde yaşamlarını sürdürebilmeleri açısından gerçek vazgeçilmezdir (Lord, 2012 Akt: Paktin ve Karaca, 2018, s. 130).

2018 RSA Konferansında yapılan bir röportajda, San Francisco merkezli Social Proof Security CEO'su ve kar amacı gütmeyen Kadın Güvenliği ve Gizliliği Yönetim Kurulu Başkanı Rachel Tobac, kişilerin kendi başlarına SM ataklarını nasıl etkisiz hale getirebileceği ve işletmelerin kendi çalışanlarını nasıl daha etkili bir şekilde eğitebileceği hakkında ne tür girişimleri olduğu hakkında şu bilgilere yer veriyor (Heller, 2018); açık kaynak istihbarat toplama aracı olan OSINT aracılığıyla çevrimiçi olarak kişiler hakkında bulabileceğimiz her şeyi araştırır ve bunun bir kaydını tutarız. Bu bilgileri fazlalıklarından arındırır, temizler, düzenler ve size geri bir bildirimde bulunuruz ve bu şekilde kendinizle ilgili bilgilerin nereden sızdırıldığını (Instagram, Twitter, Facebook, diğer web siteleri vb.) öğrenmiş olursunuz. Ayrıca sizlere gerçek hackleme olan vishing (telefonla bilgi toplama) atakları düzenleyerek ne kadar bilgi edinebileceğimizi görürüz. Tüm bunlara dayanarak sizinle ilgili bir risk haritası oluşturup daha sonra SM'den korunma eğitimleri düzenleriz. Tobac, yaşlılara karşı kullanılan taktikler ile gençlere karşı kullanılan taktiklerin de farklı olduğunu (kuşak farkını) özellikle ifade ediyor. Örneğin; yaşlıların daha çok “acil”, “önemli”, “şimdi yapmalısınız” gibi uyarılara, gençlerin ise daha çok “ödül”, “bedava” vb. uyarılara kolay tepki verdiklerini hatırlatıyor. Herkesin teknoloji bilgisinin iyi olmadığını, bu nedenle yapılacak eğitimlerin yılda bir kez yapılan teknolojik eğitimler yerine, yılın her çeyreğinde yapılan on beşer dakikalık özet ve bilgi içerikli eğitimler şeklinde olması gerektiğini öneriyor. Tobac, *olumlu raporlama kültürü*'nün oluşturulması gerektiğini öneriyor ve insanların hata ve yanlışlarından yola çıkarak yapılan uyarı ve düzenlemelerden utandığını ve başarısız olduğunu belirtiyor.

Yukarıda bahsedilen yöntem, şirket çalışanlarının SM saldırılarına karşı ne tür bir önlem ile korunabileceğine dair iyi bir örnek oluşturabilir. Tobac'ın uygulamış olduğu bu yöntem, şirketlerin/kurumların kendi içlerinde

oluşturabilecekleri bir birim tarafından ya da bilgi işlem birimleri tarafından kolayca uygulanıp, şirkete/kuruma ait bir risk haritası oluşturulabilir. Düzenli aralıklarla bu faaliyetler yerine getirilirse, savunma sistemleri de sürekli güncel kalmış olacaktır.

Güvenlik önlemleri alınırken ve eğitimler esnasında anlatılanların çok sade, basit ve anlaşılır halde sunulması önemlidir. Birçok ihtiyacı bir arada gidermek için, önlemler paketini yeniden düzenlemek, ürün sadeleştirme mantığıyla aynı şeydir. Koch ve Lockwood (2018, s. 31)'a göre, Henry Ford'un T modelindeki ana fikri de aynıydı; "ürünü yeniden tasarlamak, tek, basit ve standart bir model üretmekti".

Güvenlik uzmanları, bugünün SM saldırılarına karşı savunmanın zor olduğunu ancak imkânsız olmadığını söylüyor. Sosyal ağların, SM'nin altın madenleri olarak görüldüğünü ve bu nedenle dikkatli olunması gerektiğini ifade ediyorlar. Dijital çağda SM yeni bir şey değil elbette, ancak güvenlik uzmanları, şirketlerin ağlarını güvence altına alma konusunda daha iyi olduklarından suçluların SM alanını daha fazla zorladıkları ifade ediyor.

Human Compromise: The Art of Social Engineering adlı kitabın yazarı Mike Murr, eskiden güvenlik açıklarını kapatarak yazılımsal olarak önlem almanın kullanıcılar açısından daha kolay olduğunu, ancak şimdi, sosyal medya üzerindeki bilgilerinden kişilere ulaşılması, istenilen linklere tıklamalarının sağlanması, belirli programları bilgisayarlarına indirmeleri ve bu sayede bilgisayarın ve kişisel bilgilerin ele geçirilmesi saldırganlar açısından daha kolay bir iş haline geldiğini (Savage, 2018) ifade ediyor.

Kişiselleştirilmiş bilgiler oluşturmak artık sosyal medya üzerinden toplanan bilgiler sayesinde daha kolay. Bu sayede kişisel hedef/kurban seçmek de daha kolay hale gelmektedir. Şirket yöneticilerinin bu konu hakkında çalışanlarını bilgilendirmesi ve hatta uyarması gerekebilir. Özellikle şirket profillerine ait bilgilerin sosyal medya araçları üzerinden korumasız bir şekilde paylaşılmasının önemli sorunlara yol açabileceği, bu durumdan hem şirketin hem (dolaylı da olsa) kişilerin (çalışanların) zarar görebileceği göz önünde tutulmalıdır.

Güvenlik uzmanları, program yamaları ve güncel tutulan sistemlerin kritik öneme sahip olduğunu, ancak teknoloji ataklarındaki kurnazlığının devam ettiğini, hedef gözetilerek yapılan SM saldırılarına karşı şirketlerin savaşmalarının zor olabileceğini ancak bunun yanı sıra çalışan güvenliği bilinçlendirme eğitimlerinin de

önemli ve etkili olduğunu söylüyor. MANDIANT'ta kıdemli danışman olan Frank Nagle, SM saldırılarında çalışanların gerçekten ön sırada (ilk hedefler arasında) olduğunu ifade ediyor. Bu nedenle çalışanların eğitimine önem verilmesi ve şüpheli e-postalar için çalışanların bu tür saldırılara karşı uyanık olmaları ve sezgilerine, içgüdülerine güvenmeleri gerektiğinin öğretilmesinin önemli olduğunu belirtiyor. LoganWHC ve Offensive Security operasyon yöneticisi Chris Hadnagy, şirketlerin, çalışanların kendilerini çevrimiçi olarak profillemenin ne kadar kolay olduğunu ya da şifrelerini kırmanın ne kadar basit olduğunu gösteren eğitimler ile çalışanlar için güvenlik bilincini oluşturan bir program yaratmaları gerektiğini ifade ediyor (Savage, 2018). Lewis (2018) ise insanların en kolay araçları kullanarak hedeflerine varmak istediklerini belirterek alınabilecek çeşitli önlemleri şu şekilde sıralıyor;

Sosyal ağ üzerinden yapılan SM saldırıları, meşru görünen birine güvenme yanılsamasını kullanır, çünkü saldıranın iddialarını desteklemek için elinde zengin bir sosyal ağ üzerinden sahip olunan veriler bulunmaktadır. Bu nedenle savunmalara karşı korunmak sanıldığı kadar kolay olmayabilir. SM saldırılarına karşı savunma, bir işletmenin Bilişim Teknolojileri ortamının dikkatle izlenmesini içeren katmanlı bir koruma gerektirir. Tüm SM saldırılarını önlemek mümkün değildir, bu nedenle kurumsal güvenlik ekipleri izleme, müdahale ve eğitime odaklanmalıdır. Ayrıca, çalışanların dikkatini biraz daha çekmek için, kullanmış oldukları bilgisayar ağının ve bilişim teknolojilerinin ilgili birimce izlendiğini bilmeleri faydalı olabilir. SM riskini değerlendirirken göz önünde bulundurulması gereken bir başka husus, SM saldırılarını durdurmak için gerekli olabilecek potansiyel karmaşıklılıktır; bu karmaşıklık, sistemleri daha kırılgan hale getirebilir ve yönetilmesi zorlaşabilir, ayrıca izleme yapmak için ek kaynaklar gerektirir. Bazı kuruluşlar işyerinde sosyal medya kullanımını yasaklamaya karar verebilir, ancak bu akıllı telefonların veya diğer popüler teknolojilerin kullanımını yasaklamak kadar etkili olacaktır. Çalışanlar şüpheli bir mesaj, belge, e-posta vb. aldıklarını düşündüklerinde, ek sorgulama yapma ihtiyacı duymaları gerektiğini öğrenmelidir. SecureWorks ayrıca Microsoft Office'teki *makroları* devre dışı bırakmak ve uç nokta güvenlik araçlarını kullanmak gibi temel güvenlik kontrollerini önermektedir. Bu araçlar kötü amaçlı çalıştırıcıların *PowerShell*⁵ komutlarının yürütülerek sisteme zarar vermelerini önleyebilir.

Johnson (2018), hiçbir önlemenin, işletmelere yönelik acımasız SM saldırılarına karşı %100 koruma sağlamadığını, sadece 2014 yılında, RSA'nın küresel kuruluşlara yapılan kimlik avı (phishing) saldırılarının maliyetinin 4.5 milyar dolar

⁵ MicroSoft'un geliştirmiş olduğu PowerShell kısaca, nesneleri yönetmeye yarayan (lokal ya da uzaktan) komut satırı olarak ifade edilebilir.

olarak tespit ettiğini, şirketlerin bu zararlardan korunmaları için, şüpheli, tuhaf ve olağan dışı faaliyetleri kendilerine bildirmeleri için çalışanlarını bilgilendirmeleri ve gerekli özeni göstermeleri için ödülleri teşvik etmeleri gerektiğini ifade etmektedir. Önleme stratejilerinin ötesindeki savunmaları güçlendirmenin bir yolu da veri merkezli algılama yaklaşımlarının benimsenmesidir. Bazı kuruluşlar kritik bilgileri ve bunlara nasıl, ne zaman, nerede, neden ve kim tarafından erişildiğini bilmek için otomatik algılama ve davranışsal analitik izleme kullanmaktadır. Johnson (2018), New York güvenlik firması White Ops'un kurucu ortağı ve bilim insanı şef Dan Kaminsky'nin, artık enformasyon güvenliği sorumlularının, önlem almak yerine tespit etme stratejisini kullandıklarını, çünkü saldırganların önlem bariyerlerini bir defa aştıklarında içeriye erişim sağlamış olduklarını söylediğini aktarıyor.

Son zamanlarda güvenlik uzmanları ve şirketleri *otomatik ihlal algılama sistemleri* üzerinde çalışmaktalar, bu sistemler sayesinde ihlaller aylar içerisinde değil anlık olarak tespit edilebilecek ve önlemler hızlıca alınabilecektir. Atlanta'daki Damballa Inc.'deki CTO'dan Brian Foster, otomatik ihlal tespit sistemlerinin, meydana gelebilecek bir kırılmaya neden olabilecek bir bulaşma riski konusunda kullanıcıları/sorumluları uyarabileceğini söylemekte ve bu sistemin gelen-giden internet trafiğini analiz ederek ve e-posta akışlarını kontrol ederek bu işi yapabileceğini ifade etmektedir. Foster, indirilmesi istenilmeyen (sorunlu) dosyaların %20'lik kısmının ise SM yöntemleriyle başarıldığını da belirtmektedir (Johnson, 2018).

Güvenliği sağlamanın diğer bir yolu da veri hırsızlığına karşı koruma sağlamaktır. Saldırganların esas istedikleri şey kişi ya da kurumların verileridir. Büyük Veri depolama, veri analizi, bulut bilişimler ile ilişkili olarak verilerin güvenli ortamlarda tutulması, hatta şifreli olarak saklanması faydalı olabilecektir. Veri merkezli bir strateji geliştirmek hangi verilerin ne kadar ve ne derece önemli olduğunun anlaşılmasına da fayda sağlayacak ve belki önemine göre veri sınıflandırması yapılabilecek bir önlemler paketi geliştirilebilecektir. İşlemciler/sunucular da bu sınıflandırmaya uyumlu olarak farklı işler için farklı sunucular şeklinde görevlendirilebilir. Ayrıca, veri sınıflandırması yapmak aynı zamanda şirket veri varlıklarının neler olduğu ve tanınması konusunda yöneticilere/çalışanlara bilgi de sağlamış olacaktır.

Kurban olmamak için, özellikle kimlik avı (phishing attack) şeklinde yapılan yaygın SM ataklarından korunmak için bazı korunma yöntemleri vardır. Aslında bunların çoğu, başlangıç seviyesinde, önünüzdeki ayrıntılara dikkat etmekten çok daha fazlasını gerektirmez. Kimlik avı kurbanı olmamak için şunları dikkate almak faydalı olacaktır (www.reboot.com);

- **Ağır/yavaş olun:** Size spam (istenmeyen e-posta sağanağı) gönderenler önce hareket etmenizi daha sonra düşünmenizi isterler. Eğer mesaj, bir aciliyet hissi veriyorsa ya da baskıcı satış taktiklerine başvuruyorsa şüpheli olmalısınız. Aciliyet durumlarının, incelemelerinizi dikkatlice yapmanızı engellemesine izin vermeyin.
- **Gerçekleri araştırın/doğrulayın:** Talep etmediğiniz (gelmesini beklemediğiniz) mesajlara şüpheliyle yaklaşın. Eğer e-posta çalıştığınız bir şirketten geliyor gibiyse kendi araştırmanızı (teyidinizi) yapın. Şirketin gerçek web sitesine erişmek için arama motorlarını kullanın.
- **Linklerin sizi gerçekte gitmek istemediğiniz yere götürmesine izin vermeyin:** Gitmek istediğiniz yere (web sitesine) gittiğinizden emin olmak için arama motoru kullanın (şüpheli e-postalardaki/mesajlardaki adres ve linklere tıklayarak değil de, şirket/firma/kurum'u arama motorundan aratarak web sitesine erişmeye çalışın). Ayrıca e-postada size tıklamanız için gönderilen adres (link) satırının üzerine fareni gezdirirseniz, adresin sizi nereye götüreceğini (daha tıklamadan) ekranın en alt satır çubuğunda görebilirsiniz.
- **E-posta korsanlığı çok yaygın, dikkat edin:** Hackerlar, istenmeyen posta göndericileri (spammers) ve sosyal mühendisler kişilerin e-posta adreslerini ve diğer iletişim hesaplarının kontrolünü ele geçiriyorlar, bu çok yaygınlaşmış bir durum. E-posta hesaplarını bir kez ele geçirdiklerinde, isim listesindeki biri gibi davranıp kişileri avlıyorlar. Gönderen tanıdığınız biri gibi görünse bile, eğer bir bağlantı veya ek içeren bir e-posta beklemiyorsanız, bağlantıyı açmadan veya indirmeden önce gönderiyi yapan arkadaşınızla görüşün.
- **Herhangi bir indirme işlemine dikkat edin:** Göndereni kişisel olarak tanımıyor ya da onlardan bir dosya beklemiyorduysanız, bu şartlar altında dosya indirmek bir risktir.
- **Yabancı teklifler aldatıcıdır:** Yabancı bir piyango ve çekilişten e-posta, tanımadığınız bir akrabanızdan para, ya da yabancı ülkeden payınıza düşen bir para transferinin olduğunu görürseniz bu bir kandırmacadır, dikkatli olmalısınız.

Şüpheli yardım talepleri veya yardım teklifleri reddedilmelidir, meşru şirketler ve kuruluşlar yardım sağlamak için insanlarla iletişim kurmazlar. Spam filtrelerinin koruma seviyeleri yükseltmeli, spam klasörü de belirli aralıklarla kontrol edip temizlenmelidir. Anti-virüs programları güncellenip, güvenlik duvarı (firewall) sürekli aktif tutulmalıdır.

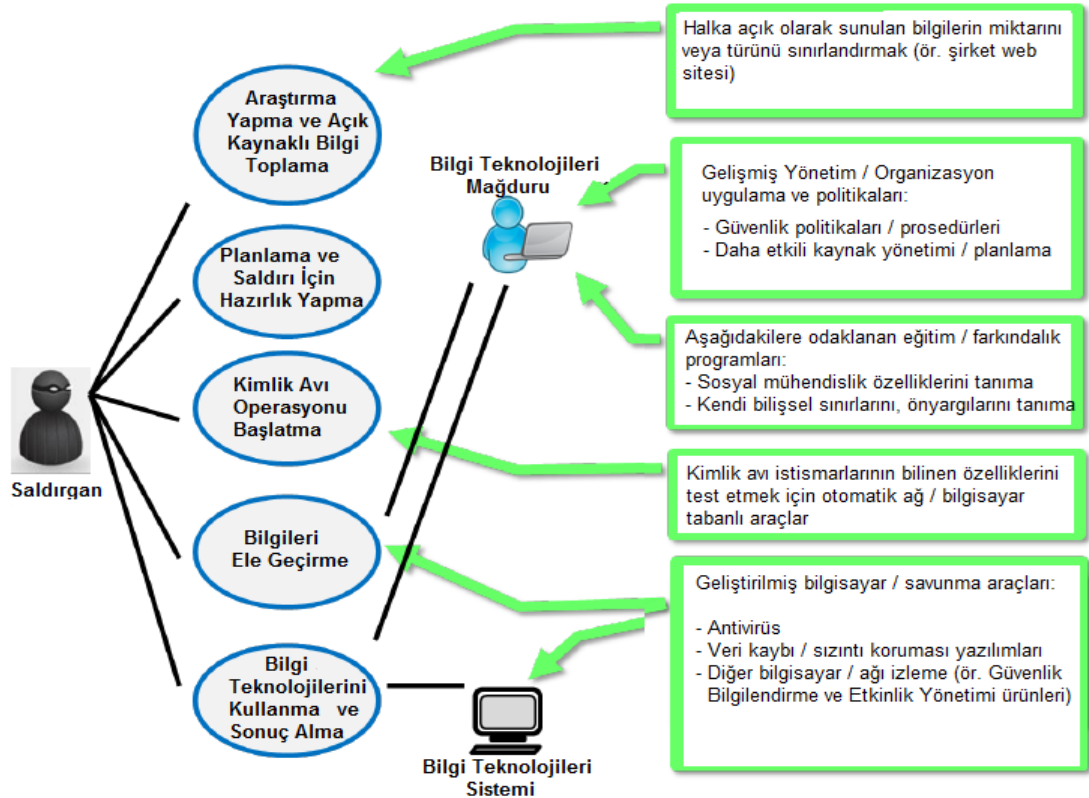
SM ataklarından korunabilmek için öncelikli olarak SM taktiklerine, zafiyetlere, güvenlik açıklarına bakmak gerekmektedir ve bazı soruları kendinize sorarak cevap verebilmeniz gerekmektedir. Clark (2017, s. 49-50) bu süreci aşağıda yer alan Tablo 7 ve Şekil 19'da şu şekilde özetlemiştir:

Tablo 7. Sosyal Mühendislik Taktikleri, Zafiyetler (Güvenlik Açıkları) ve Azaltıcı (Hafifletici) Önlemler

Taktik	Zafiyet	Önleyici Sorular
Sahte dostluk	Güvenme arzusu	Bu kişi bana neden bu kadar nazık davranıyor?
Sahte sempati (dalkavukluk)	Ortak kederi (üzüntüyü) paylaşma arzusu	Bu kişi gerçekten çocuğumun başına gelen kazayı önemser mi?
Sahte otorite	Gücün vermiş olduğu korku	Bu kişinin kim olduğuna (söylediği kişi olup olmadığına) nasıl inanabilirim?
Başka bir kimliğe bürünme	İşlerin/kişinin görüldüğü gibi olduğu varsayımı	Bu kişinin kıyafeti biraz fazlaca mı kusursuz?
Uyum (sağlama)	Uyum arzusu	Diğer herkesin bunu yapması biraz şaşırtıcı değil mi?
Azlık (az bulunurluk)	Kıt olan şeylere değer verme eğilimi	Bekle bir saniye, bunun hemen şimdi mi yapılması gerekiyor?

Kaynak: Clark, 2017, s. 4. <https://www.nsi.org/Impact17Presentations/J.Clark.pdf> adresinden uyarlanmıştır, Erişim: 09.01.2019

Şekil 19. Sosyal Mühendisliğe Karşı Önleyici Stratejiler



Kaynak: Clark, 2017, s. 50. <https://www.nsi.org/Impact17Presentations/J.Clark.pdf> adresinden uyarlanmıştır, Erişim: 09.01.2019

Douglas Twitchell'e göre, SM saldırılarına karşı korunma için güncel olarak önerilen üç yol bulunmaktadır: eğitim-öğretim-farkındalık, politikalar (geliştirme) ve denetim yoluyla yaptırımlar (Kumar, Chaudhary ve Kumar, 2015, s. 17). Kumar vd. bu önlemleri şu şekilde detaylandırmaktadır:

- Kurumun çalışanları veya bireyler, kişisel bilgileri açıklamaları konularında eğitim ve farkındalık yoluyla eğitilerek daha isteksiz hale getirebilir. Çalışanların derinlemesine güvenlik eğitimi yapılmalı, bu durum SM saldırı riskini azaltır ve organizasyonu daha korunaklı hale getirir.
- Çalışanlara, şirketin veya kişisel bilgilerinin ve kullanıcı verilerinin uygun şekilde korunması konusunda talimatlar veren politikalar/yönergeler düzenlenmelidir.
- Kuruluş/Kurum çalışanlarının politika ve prosedürlere uymasını sağlamak için denetimler yapılmalıdır.
- Kurumsal verilerin, kayıtların veya kişisel bilgilerin basılı (fiziksel) kopyaları (çöpe) atılmadan önce imha edilmelidir. Basılı kopya bilgilerini imha etmenin yaygın ve etkili yöntemleri arasında öğütücüler ve yakma tesisleri bulunmaktadır (Luco, 2015 Akt: Kumar vd., 2015, s. 17).
- Çalışanlar veya bireyler, (her kim kendini yetkili olarak tanımlıyorsa) kişinin kimlik bilgilerini sorgulama konusunda eğitilmelidir.
- Kuruluşlar, şirketlerinin web sitesinde ne yayınladıklarına dikkat etmelidir. Yetkili kişilerin isimleri ve iletişim numaraları ya da şirket bilgi detaylarının aleni olarak yayımlanmasından kaçınılmalıdır.
- Kendiniz veya şirketinizle ilgili (telefonda, çevrimiçi veya şahsen) gizli, kişisel veya şahsi bilgileri, soran kişinin kimliğini ve gerçekten bu bilgiye sahip olması gerektiğini teyit etmeden asla verilmemelidir.

Symantec firmasından Mick Jones, SM ve aslında diğer bir çok alan için (teknolojik ataklara karşı) çözümün ağ güvenliği katmanının veri altyapısı katmanıyla bütünleştirmek olduğunu, böylece şirket ağındaki olağandışı etkinlikleri izleyen otomatik bir *bilgi teknolojileri* (BT) güvenlik sisteminin devreye girebileceğini ifade ediyor (Gold, 2010, s. 13). Jones, bu süreçte “JITS - tam zamanında güvenlik” diyor diye açıklıyor. Bu süreçte, çalışanlar, BT güvenlik

sisteminden otomatik olarak bir çağrı/mesaj alır ve kendilerinden verilerin harici bir e-posta adresine iletilmesinin güvenlik etkilerini dikkate almaları istenir.

Kurumlar SM saldırıları karşısında ne durumda olduklarını (açıklarını) görmek ve çeşitli önlemler almak (proaktif davranışlar geliştirmek ve sergilemek) için sızma (penetrasyon) testlerini kendi iş yerlerine uygulayabilirler. Bu yöntem aslında birçok büyük kurum ve kamu kuruluşu tarafından siber saldırılardan korunmak maksatlı (stres testleri) çeşitli zaman aralıklarıyla tatbikat şeklinde uygulanmaktadır. Barrett (2003)'e göre bu tür sızma testleri uygulamasının güvenilir, tekrarlanabilir ve raporlanabilir olmasını sağlamak için, profesyonel kuruluşlarla, kabul edilmiş ve iyi anlaşılmış bir metodolojiyi benimseyerek uygulamak gerekmektedir. Bu metodolojinin ayrıntı düzeyi organizasyondan organizasyona değişip biraz farklı terimlerle ifade edilse bile, temel bileşenler şunlardır (s. 58):

- Hedef edinme ve inceleme.
- Erişim ve tırmanma (stres).
- Konsolidasyon ve raporlama.

Barrett (2003) bu bileşenleri şu şekilde açıklamaktadır:

İlk aşama, uygulanabilir izinsiz giriş hedeflerini keşfetme ve bunlar hakkında mümkün olduğunca fazla bilgi edinme çabasıdır. Birçok sızma testi kuruluşu, hedef şirketin bilgi altyapısı hakkında kamuya açık bilgilerin araştırılmasıyla başlar. Arama motorları da kullanılarak şirketle ilgili web siteleri, e-postalar, grup e-postaları (ve başlıkları), bunun yanı sıra sunucular, veri tabanı kayıtları ve bilgisayar sistemlerinin taranmasıdır. Ayrıca, güvenlik duvarları ve filtreleme cihazlarının olup olmadığı kontrol edilir. *Nmap*⁶ gibi bağlantı noktalarını taramak için çeşitli araçlar gerekebilir. Amaç, üzerinde çalışılan (hedef) bilgisayarlar ve ağlar hakkında olabildiğince fazla bilgi elde etmektir.

İkinci aşama, ilk aşamada elde edilen (keşfedilen) bilgilerin ışığında gerçek bir müdahaleyi içerir. Bu müdahale “kaba kuvvet” (ele geçirilmiş şifre ya ad kullanıcı adları kullanmak), özel güvenlik açıkları ve testi yapanlar tarafından

⁶ **Nmap**: Bilgisayar ve ağ makinelerinin açık portlarının belirlenmesi, bu makineler üzerinde çalışan servislerin taranması ve tespiti için yazılmış bir uygulamadır.

geliştirilmiş ya da internet üzerinden erişilebilecek güvenli yazılımlar ile yapılan saldırılardır.

Sızma testinin üçüncü aşamasında güvenlik ihlali konsolide edilir. Bu genellikle, davetsiz misafirin varlığını gizlemek ve davetsiz misafirin özel hedefine ulaşması için *rootkits*⁷ ile yapılır. Buradaki amaç, belirli bir dosyaya erişim sağlamak, bazı verileri değiştirmek veya sisteme bir şey eklemek/çıkartmak olabilir.

Bunların tamamının uygulanması sızma (penetrasyon) testi projesinin bittiğini göstermez. Daha sonra, sızma testi ekibinin görüşleri doğrultusunda bir rapor hazırlanmalıdır. Bu raporda hangi güvenlik açıklarının keşfedildiği, nasıl müdahale edildiği (erişim sağlandığı) ve tüm bunlardan korunabilmek için nelerin değiştirilmesi gerektiği tavsiye edilir (Barrett, 2003, s. 58-59).

SM her zaman insanların yanı başında bulunmaktadır. Ancak, insanlar kendilerinin ve işyerlerinin en değerli varlıklarını korumaya odaklanmak istiyorlarsa, işe kendilerini korumakla başlayabilirler. İş yerinde, gerekenden daha fazla erişim vermemek, bordro vb. gizli dosyalara erişimi olan kişilerin sayısını en aza indirmek riski azaltmaya yardımcı olabilir ancak ortadan kaldırmayacaktır. Sosyal mühendisler çalışanları eğiterek zararı en aza indirgeyebilirler. Günümüzde risk her yerde vardır. İnsanların kendilerini ve şirketlerinin varlıklarını korumak için saplantılı veya kaba olması gerekmez. Sadece risklere karşı dikkatli ve uyanık olmaları gerekir (Barber, 2001).

Bir ağın teknolojik olarak ne kadar güvenli olduğuna bakılmaksızın, insan unsurunun her zaman bir güvenlik açığı olacağı açıktır. Başarı oranı ve siber suç sayısının artması, SM'nin kötü niyetli oyunculara sunduğu anonimlik seviyesinden dolayı sürekli artmaktadır. SM ile ilgili riski tolere edilebilir bir seviyeye düşürmek için uygulanabilecek teknik ve teknik olmayan koruma önlemleri vardır. Şirketler güvenlik planlarına birden fazla katman ekleyebilirler, böylece dış katmandaki mekanizma başarısız olursa, en az bir iç katmandaki mekanizma bir tehdidin felakete dönüşmesini önlemeye yardımcı olabilir (Risk Azaltma). Bu kavram, *Çok Katmanlı Savunma* veya *Derinlikli Savunma* olarak bilinir. Bu yapıdaki bir savunma, aşağıdaki ihtiyati tedbirlerin bir karışımını içerir (Conteh, 2016, s. 438):

⁷ **Rootkits:** Bilgisayar (işletim) sistemine erişerek uzaktan kontrol ve/ya yetki sağlamak için kullanılan yazılım türevleridir.

1.9.1 Güvenlik Politikası

İcra/Yönetim Kurulu tarafından, teknik ve teknik olmayan yaklaşımları içeren iyi hazırlanmış/yazılmış bir politikadır. Her kuruluş, güvenliği kendi operasyonel hedeflerine entegre etmelidir.

1.9.2 Eğitim ve Öğretim

Çalışanların, başlangıç eğitimlerinin yanı sıra, oryantasyon ve tekrar eden tazeleme eğitimlerine katılmaları gerekir. Bu katılım onlara, sosyal mühendisler tarafından hedeflenen ve yaygın olarak kullanılan taktik ve davranışlar hakkında (güncel bilgiler vererek) farkındalık yaratır.

1.9.3 Ağ Yönergesi

Kuruluş, yetkilendirilmiş web sitelerini NAT⁸ (Network Address Translation) kullanarak beyaz listeye alıp, kullanılmayan bağlantı noktalarını (portları) ve uygulamaları devre dışı bırakarak ağ güvenliğini sağlamalıdır. Ağ kullanıcıları, her 60 günde bir (karmaşık) şifrelerini değiştirme işini düzenli/kalıcı hale getirmelidirler.

1.9.4 Denetimler ve Uyum

Kuruluşların güvenlik politikalarına uyulduğunu aktif bir şekilde doğrulamaları gerekir. Bazı denetimler arasında ağ kayıtlarını incelemek, çalışanların izinlerini doğrulamak ve en azından iki ayda bir masaüstü yapılandırmalarını kontrol etmek yer almalıdır.

1.9.5 Teknik Prosedürler

Verileri ve temel altyapıyı korumak için ağ birden fazla savunma katmanına sahip olmalıdır. İzinsiz Giriş Önleme Sistemleri, İzinsiz Giriş Tespiti Sistemleri ve güvenlik duvarları gibi yazılımlar her cihaza kurulmalıdır. Harici işlemlere erişim için ise web filtreleri ve Sanal Özel Ağ (VPN: Virtual Private Network) kullanılmalıdır.

1.9.6 Fiziksel Erişim Yönergesi

Fiziksel varlıkları korumak için uygulanabilecek çeşitli seçenekler vardır. Davetsiz misafirlerin binaya girmelerini engellemek için güvenlik görevlileri, panolar ve güvenlik kameralarının bir arada kullanılması yararlıdır. Fiziksel

⁸ NAT (Network Address Translation): Aynı ağ içerisinde bulunan birden fazla cihazın aynı public IP'yi kullanarak internete erişebilmesini sağlayan yöntemdir (Şengün, 2018).

donanımın bulunduğu yerlere erişim verilmeden önce çok faktörlü kimlik doğrulama, biyometri veya erişim kontrol listesi kullanılmalıdır.

SM ataklarına karşı korunmada Fiziksel Erişim Yönergesi en çok dikkate alınması gereken uygulamaların başında yer almaktadır. Yukarıdaki açıklamalara ilaveten ek uygulamalar ve korunma tedbirleri bu listeye eklenerek belirli aralıklarla listenin güncellenmesi faydalı olacaktır.

Cazier ve Botelho (2007) “Sosyal Mühendisliğin Kamu Güvenliğini Tehdidi” başlıklı çalışmalarında şu sonuçlara ulaşmışlardır: Aynı şifreyi birden fazla sistemde (yerde) kullanan kullanıcıların, şifrelerini açıklama olasılıklarının daha yüksek olduğu, güvenlik eğitimi alanların şifrelerini paylaşma eğilimlerinin daha az olduğu ve bunun yanı sıra daha güvenli (karmaşık) şifreler kullandıkları, çalışanların SM saldırılarına karşı çok savunmasız oldukları, bir tür eğitime katılsalar bile, çoğunun hala şifrelerini paylaşma eğiliminde oldukları biliniyor. Cazier ve Botelho (2007) alınabilecek önlemler ve eğitim konusunda şu çıkarımlarda bulunmaktadır: Öğrenciler hala okuldayken güvenlik konusuna daha güçlü bir bilinçlendirme yapılmalıdır. Bunlar geleceğin çalışanları olacağından henüz işgücüne katılmadan önce temel bir anlayışa sahip olmaları gerekir, aksi takdirde kolayca sosyal mühendislerin hedefi haline geleceklerdir. Kurumsal bilgi güvenliği eğitim programına katılmaları da önemlidir. Kurum bilgilerine erişimi olmadığını düşündükleri kişilere karşı durabilmeyi öğrenmelidirler. Bu ancak yönetim desteği ve izlenmesi gereken politikaların belirlenmesiyle mümkün olabilir. Her geçen gün daha fazla bilgi dijital hale geldikçe, güvenlik bilincinde daha büyük bir artış olması gerekmektedir.

2007 yılında yapılan bu çalışmadan on yıldan fazla zaman geçmiş olsa da aslında değişen pek bir şeyin olmadığı görülmektedir. İnsanlar, saldırılarda hala en zayıf halka olarak kabul edilmekte ve SM atakları aynı hızla sürmektedir. Daha önce de birçok kez ifade edildiği üzere eğitim ve bilinçlendirme, korunma tedbirlerinin en başındaki yerini korumaya devam etmektedir.

SM saldırılarının başarısını azaltmak için dikkat edilmesi gereken diğer kontrollerden bazıları ise şunlardır (Shetty, 2019):

- Güvenlik duvarı, antivirüs, casus yazılım önleme programı ve e-posta filtreleri yüklemek ve düzenli aralıklarla bakımını (güncellemesini) yapmak.

- İnsanların kuyruğunuza takılarak sizin peşinizden gelmelerine (ve bu şekilde içeri girmelerine) izin vermemek.
- Kuruluşların uygun bir *olay müdahale stratejisi* bulunmalıdır.
- Kurum kimliğinin, kamuya açık alanlarda, blog, tartışma forumu vb. ortamlarda kullanımı kısıtlanmalıdır.
- Bir web sitesinin URL'sine dikkat edilmelidir. Kötü niyetli web siteleri genellikle legal bir siteyle aynı görünümündedirler.
- Kurumsal posta kutusu gibi gizli ve kritik çevrimiçi detaylara, internet güvenliğinin olmadığı halka açık yerlerden, kafelerden, otellerden vb. erişilmemelidir.
- Bir web sitesinin güvenilirliğini kontrol edilmeden internet üzerinden hassas bilgiler gönderilmemelidir.
- E-postalarda kişisel veya finansal bilgiler ifşa edilmemeli ve bu tür bilgileri isteyen e-posta taleplerine cevap verilmemelidir.
- Tüm fiziksel giriş ve çıkış noktalarının her zaman güvenli olduğundan emin olunmalıdır.
- Birisinin, istenilen bilgiye sahip olma yetkisinin olduğundan emin olunmadığı süreçte, kuruluş/kurum hakkında bilgiler ya da kişisel bilgiler verilmemelidir.
- Uygun/mümkün olan yerlerde sanal klavye kullanılmalıdır.
- Şirketin web sitesinde nelerin olduğuna (yayınlandığına) çok dikkat edilmelidir. Mümkünse kuruluş isim şemaları veya kilit kişilerin listelerinin yayınlanmasından kaçınılmalıdır.
- Hassas veriler içerebilecek belgelerin atılırken/yok edilirken uygun bir şekilde imha edildiğinden emin olunmalıdır.

Politikaların, prosedürlerin ve standartların etkili olması için çalışanlara iletilmesi, öğretilmesi ve güçlendirilmesi gereklidir. Çalışanlar bir saldırıyı tanımlamak, saldırının etkisini en aza indirmek ve saldırgan için engeller oluşturmak için eğitilmelidir. Yukarıdan aşağıya herkes güvenlik ilkelerini anlamalı ve buna göre davranmalıdır (Sadiku, Shadere ve Musa, 2016, s. 65). Modern toplumumuzda hassas bilgilerin korunması önemlidir. BG tehditlerine dair artan farkındalığa

rağmen, BG ihlalleri var olmaya devam etmektedir. SM bir saldırı metodolojisi olarak algılanıyor. SM bir alan ve bu alandaki bir süreçtir. SM, bireyler, şirketler, organizasyonlar ve hükümetler için gerçek bir tehdit olmaya devam etmektedir. SM alanı hala başlangıç aşamasındadır (Sadıku vd., 2016, s. 66).

1.10 Sosyal Mühendislik Örnekleri

Bu başlık altında SM olaylarını daha iyi kavrayabilmek ve SM'ye daha farklı açılardan bakabilmeyi sağlamak amacıyla çeşitli örneklere yer verilmiştir. Şüphesiz ki bu örnekleri sonsuz sayıda artırmak mümkündür. Araştırmanın Birinci bölümünde kapsamlı bir şekilde anlatılmış olan SM'ye ait açıklamaların bir miktar daha kalıcı olabilmesi için hazırlanmış olan bu başlık altındaki örneklerin konuyu pekiştirme açısından faydalı olacağı düşünülmektedir.

Örnek I

Güvenlik şirketi RSA'ye yönelik 2011 yılında gerçekleşen veri ihlalinde saldırganlar iki farklı RSA çalışanına, konu satırında "2011 İşe Alım Planı" yazan ve bir Excel dosyası eki bulunan bir e-posta gönderdi. Bu Excel dosyası, Adobe Flash güvenlik açığından yararlanarak bir *arka kapı* açan kötü amaçlı kod içeriyordu. Tam olarak ne tür bir bilginin çalındığı net olarak bilinmese de, RSA'nın iki faktörlü kimlik doğrulama (2FA) sistemi ele geçirilerek ifşa edilmiş oldu ve şirket bu saldırıdaki kayıplarını kurtarmak için yaklaşık 66 milyon dolar harcadı.

(Kaynak: <https://searchsecurity.techtarget.com/definition/social-engineering>)

Örnek II

Büyük oyuncak firmaları, Noel sonrası (Ocak ve Şubat ayları bu sektör için yılın en az satışın yapıldığı aylardır) satışların azlığından muzdariptirler ve bunu gidermek için şöyle bir yöntem keşfetmişlerdir:

Noel'den önce televizyonda belli bir oyuncağın reklamını yapıyorlar. Çocuklar onu görüp istiyorlar ve ailelerinden Noel'de o hediye almaları için söz alıyorlar. İşte burada oyuncak firmalarının dâhiyane planları devreye giriyor. Mağazalara ailelerin almak için söz verdikleri oyunculardan az sayıda tedarik ediyorlar. O oyuncakların bittiğini öğrenen aileler (Noel öncesi olduğu için hediyesiz ve daha ucuz olan bir hediyeyle eve dönemeyecekleri için) aynı değerde olan başka oyuncaklar alarak durumu telafi ediyorlar (ettiklerini sanıyorlar). Noel'den sonra, o özel oyuncaklar için satıcı firmalar (daha fazla) yeni reklam veriyorlar ve bu durum çocukların o oyuncakları her şeyden daha çok istemelerine yol açıyor. Çocuklar ailelerine gidip "söz vermiştin, söz vermiştin" diye ısrar ediyorlar ve aileler de (artık bulunması kolay olan oyuncakları almak üzere) mağazalara gidip sözlerini tutuyorlar

Bu şekilde oyuncak firmaları ailelere bir oyuncak yerine eş değer fiyatta iki oyuncak satabilmiş oluyor. Hem Noel arifesini hem Ocak ve Şubat aylarını kazançla kapatmış oluyorlar. (Kaynak: Cialdini, 2018, s. 103).

Örnek III

Los Angeles'ta silikon vadisindeki bilgisayar şirketlerinde bir dönem çalışanların kökeni itibariyle önemli bir değişim yaşanmıştır. O dönemde çalışanların %70'i Uzak Doğulu ve Çinli yazılımcılardan oluşuyordu. Bu dönemde Amerikalılar tarafından Los Angeles'ta oraya özgü "ejderhaları öldürelim" yani bizi sınırlayan, yaratıcılığımızı öldüren yaklaşımları yok edelim düşüncesi ve bunu engelleyenleri de ejderha gibi göstermeye dönük bir kampanya başlatıldı. Ejderhalar yapılmış, şirketlerin kapılarına asılmış ve törenlerle indirilmişti. Yaratıcılığın artırılması yönünde yapılan bu girişim ertesi gün Çinli çalışanların %20'sinin işe gelmemesine neden olmuştur. Çünkü Çinliler için ejderha çok önemli ve kutsal bir figürdü

Bu örnek olay bize göstermektedir ki, SM faaliyetlerinde kültürel farklılıkların da dikkatlice gözetilmesi gerekmektedir. (Kaynak: Ertan, 2016, s. 8).

Örnek IV

Aşağıdaki örnek, İngiltere'deki bir finans kurumunda meydana gelen gerçek ve başarılı bir SM saldırısı olayıdır:

Çalışanlardan biri, yöneticilerden birisinden, bir bulut dosya paylaşım hizmetinde barındırılan bir faturaya atıf yapan bir e-posta aldı. Aynı çalışan, birkaç dakika sonra, aynı kuruluştaki çalışan bir başka yönetici tarafından telefonla aranarak kendisinden ilgili faturayı incelemesini ve onu işleme sokmasını istedi. Ancak, hem fatura sahteydi hem de arayan kişi yönetici değil, SM saldırısını yapan kişiydi. Görünürdeki bu fatura aslında sunucuyla iletişime geçerek onu kontrol altına almak amacıyla tasarlanmış bir Uzaktan Erişim Trojanı'ydı. Saldırgan, bu Trojanı kullanarak çalışanın bilgisayarını anında kontrol altına aldı. Çok katmanlı şifreli sunucunun tüm sunuculara erişimi engellendiği için saldırı ancak sunucunun bir bölümüne erişim sağlamayı başarabildi. Bu saldırı finansal kazanım sağlamak için SM saldırı tekniğini kullandı. Saldırı durdurulana kadar geçen sürede, saldırı aşağı yukarı 50.000 Sterlinlik bir parayı almayı başardı.

(Kaynak: Alavi, Islam, Mouratidis ve Lee, 2015, s. 167):

Örnek V

2013 yılında Suriye Siber Ordusu, Associated Press (AP)'in Twitter hesabına, ekinde zararlı bir yazılım bulunan bir olta (phishing) e-postası göndererek erişim sağladı. E-posta, kendi çalışanlarından biri kılığında AP çalışanlarına gönderilmişti. Saldırganlar, AP'nin hesabından sahte bir haber öyküsünü tweetledi ve Beyaz Saray'da iki patlamanın gerçekleştiğini ve ardından Başkan Barack Obama'nın yaralandığını söyledi. Bu durum hisse senedi piyasasının beş dakikadan daha kısa bir süre içerisinde 150 puan düşmesine sebep oldu.

(Kaynak: <https://searchsecurity.techtarget.com/definition/social-engineering>).

Örnek VI

Kendi çıkarını değil, müşterinin çıkarını düşünüyormuş gibi yapıp, karşı tarafın güvenini kazanan (ve sonrasında istediğini elde eden) garsonun taktiği;

Müşterilerin ilk seçtiği yemek ne olursa olsun, garson kaşlarını çatarak elini sipariş defterinin üzerinde tutuyor ve omzunun üzerinden şefe baktıktan sonra masaya eğilerek, “korkarım ki bu seçtiğiniz bugün her zamanki kadar iyi değil” onun yerine (daha ucuz olan) şunu ya da bunu önerebilir miyim, bugün her ikisi de harika diyor. Müşteriler, garsonun önerdiği yemeği seçmeseler bile, kendileri için bir iyilik yapıldığını (ilk sipariş etmek istedikleri yemeğin o gün için iyi olmadığı hakkında önemli bir bilgi elde edinerek!) düşünerek garsona minnettar kalıyorlar ve bahşiş bırakma zamanı geldiğinde *karşılıklı bulunma ilkesi* hiç şüphesiz garsonun lehine işliyor. Garson (müşterilerin gözünde) hem dürüsttü, hem de müşterinin çıkarını düşünerek daha ucuz ve güzel yemekler öneriyordu bu şekilde bahşişin yanı sıra siparişlerin artmasını da sağlayarak işletme sahibinin de takdirini kazanıyordu. Müşteriler, yemek sonunda sipariş edecekleri tatlıların seçimini de elbette (güvenilir!) garsona bırakmakta hiç tereddüt etmiyorlardı

Samimiyetini kanıtlamış, güvenilir, dürüst ve kendi çıkarını gözetmeyen bir sosyal mühendisten kim daha inandırıcı olabilir ki?
(Kaynak: Cialdini, 2018, s. 301).

Örnek VII

- **Sosyal Mühendis:** Web sitemi tarayamıyorum ve öyle sanıyorum ki sizden satın almış olduğum ürününüz (yazılımınız) beni sınırlandırıyor. ... şu siteye giderek kontrol edebilir misiniz? Böylece sizin yazılımınızdan kaynaklı bir durum olup olmadığını teyit edebilirim.

- **Teknik Destek Elemanı** (Hedef): Efendim, benim sizin istediğiniz siteye giriş yapıp yapmamamın bir önemi olmayacaktır, ürünümüz sizin o siteye girmenizi engellemez.

- **Sosyal Mühendis:** Ürününüzün o siteye girmemi engellemeyeceğini söylediğinizi biliyorum ama sizin ürününüzü yükleyene kadar normal çalışıyordu, bu yüzden lütfen benim için kontrol edebilir misiniz?

- **Teknik Destek Elemanı** (Hedef): Efendim, yaşamış olduğunuz bu sıkıntıdan dolayı üzgünüm ama ürünümüz sizin girişinizi engellemeyecektir ve benim o siteye girmem sizin probleminizi çözmenize yardımcı olmayacaktır.

- **Sosyal Mühendis:** (saldırganın hayır cevaplarından yılmayarak) Benim için o siteye girmeyi denemeniz kendimi daha iyi hissettirecektir. Lütfen, bana yardım edebilir misiniz?

Bu ısrarlar karşısında (saldırganın anlayışsız davranışları karşısında?) sinirlenen teknik destek elemanı yapmaması gerektiğini çok iyi bildiği bir davranışı sergiler ve (kötü niyetli yazılımı barındıran) o siteye giriş yapar. Burada üç önemli husus söz konusudur:

- Saldırganın (Sosyal Mühendisin) ısrarla denemelere devam etmesi
- Hedefin, bir an önce müşteriden (saldırgandan) kurtulmak isteyişi
- Saldırganın, yardıma ihtiyacı olduğu hissini uyandırması

(Kaynak: Hadnagy, 2017, s. 361)

İKİNCİ BÖLÜM

2. BİLGİ GÜVENLİĞİ

Bilgisayar ağları ve internet kullanımının hızla yaygınlaşması ve buna paralel olarak kişisel ve kurumsal veri trafiğinin bu ağ platformu üzerinde gerçekleşiyor olması, doğal olarak bilgi güvenliğini gündeme getirmektedir. Bilgi güvenliği (BG); bilgi teknolojileri güvenliğinden fiziksel güvenliğe, risk yönetiminden işlerin düzenli bir şekilde yürütülmesine (iş sürekliliği ve sürdürülebilirlik), müşteri bilgi güvenliği ve gizliliğinden uluslararası standartların inşasına, hukuksal hak ve sorumluluklara kadar uzanan geniş bir alanı kapsamaktadır. Burada bahsedilen ve benzeri birçok parametreyi içeren ve bu yüzden önemli bir kurumsal yönetim unsuru olan BG bu bölümde çeşitli başlıklar altında kavramsal olarak ele alınarak açıklanacaktır.

Kurum ve kuruluşların giderek daha fazla teknoloji ve bilgiye bağımlı hale gelmesi BG'ni yaşamsal öneme haiz kılmaktadır. BG'nin bir kurumsal yönetim unsuru olması ve bilgi teknolojileri güvenliği, fiziksel güvenlik, risk yönetimi, iş sürekliliği ile yasa ve yönetmeliklere uyum gibi unsurlarla yakından ilgili olması ve ayrıca çalışanlara, iş ortaklarına, müşterilere ve topluma yönelik çeşitli yükümlülükleri yerine getirme sorumluluğu taşıması nedeniyle de önceliğinin yüksek olması zarureti ortaya çıkmıştır (www.bilgi.edu.tr). Gerek kişisel düzeyde gerekse kurumsal düzeyde olsun yeni düzenlemeler, önlemler, hukuksal sorumluluklar ve BG'nin diğer alanlarla/disiplinlerle etkileşimi ve uyarlaması gün geçtikçe daha çok önem arz etmekte ve dikkatleri bu yöne çekmektedir.

Bilgi çok değerli bir varlıktır; kişiler, şirketler, kurumlar ve organizasyonlar için farklı kapsamlarda olabileceği gibi, özünde “gizli” olması gereken ve gizliliği bozulduğunda zarara uğratan varlıklar/değerlerdir (Çubukçu, 2018). Bu bir evrak, bilgisayardaki bir dosya, web sitesi veya e-posta olabilir. Bu açıdan BG'nin anlamı, bilgilerin korunmasını sistematik bir şekilde sağlayarak, bu yönde önlemler almak ve sistemler geliştirmek suretiyle, temelde kuruma ait bilgilerin güvenliğinin sağlanmasıdır (Çubukçu, 2018).

BG çok geniş bir alanı kapsamakta olup, bilgi denilince veri, veri denilince yazılım, yazılım denince donanım, donanım denince fiziksel güvenlik şeklinde zincirin halkaları kişisel, kurumsal ve ulusal güvenlik katmanlarına ulaşmakta ve tüm dünya genelinde uygulama alanı bulan siber saldırılara kadar genişleyebilmektedir.

Bilgi, bilgisayar, ağ ve sistem güvenliği gibi başlıklar altında toplanmaya çalışılan güvenlik ile ilgili konuların genel olarak şu alt başlıklar altında sıralandığını görmekteyiz:

- Haberleşme Güvenliği
- Bilgi Güvenliği Yönetimi
- Kriptografik Güvenlik
- Program, Yazılım ve Donanım Güvenliği
- Adli Bilişim Standartları
- Siber Güvenlik, Savaşlar ve Savunma, Siber Terörle Mücadele
- Veri Tabanı Bulut ve Sistem Güvenliği
- Bilgi Güvenliğinde Yapay Zekâ, Makine Öğrenmesi ve Derin Öğrenme Yaklaşımları ve Uygulamaları
- Risk Analizi ve Yönetimi
- Güvenli Kodlama ve Kaynak Kod Denetimi
- Yazılım Güvenliği ve Güvenli Yazılım Geliştirme
- Kritik Altyapılar ve Güvenliği
- Endüstriyel Casusluk ve Korunma
- Güvenlik Politikaları, Standartları ve Uygulamaları
- Kişisel Verilerin Mahremiyeti ve Güvenliği
- Kripto Analiz
- M2M Güvenliği
- Steganografi ve Steganaliz
- İşletim Sistemleri Güvenliği
- Bulut ve Sanal Sistemlerin Güvenliği
- E-İmza, M-İmza ve Kayıtlı Elektronik Posta, Açık Anahtar Altyapısı
- Mobil Cihaz ve Mobil Ağ Güvenliği
- Web Sistem ve Uygulama Güvenliği
- Erişim Denetimi ve Güvenliği
- Zafiyet Tespiti ve Sızma (Penetrasyon) Testleri
- Sosyal Ağlarda Güvenlik
- Yeni Nesil Ağlarda (4G, 5G, IPv6, SDN, NFV) Güvenlik

- Biyometrik Sistem Güvenliği
- Uluslararası Bilgi Güvenliği Politikaları ve Standartları
- Casus Yazılımlar ve Korunma Yöntemleri
- Sosyal Mühendislik
- Bilgi Güvenliği ve Bilişim Hukuku
- Büyük Veri Analitiği ve Güvenliği
- Endüstri 4.0 ve Güvenliği ve Nesnelerin İnternetinde Güvenlik
- VoIP (Voice Over IP) ve SIP (Session Initiation Protocol) Güvenliği

Siber güvenlik denilince, tüm bilişim sistemlerini çevreleyen genel bir güvenlik kavramı söz konusu olmaktadır. Siber güvenliğin çalışma alanına birçok farklı konu girmektedir; web güvenliği, ağ güvenliği, yazılım, donanım ve fiziksel kategoriler vb. Çoğu zaman bilgi güvenliği ile karıştırılmaktadır. Ancak siber güvenlik, bilgi güvenliğine göre daha geniş ve kapsamlı bir kavramdır, içerisinde siber ordu, siber savaşlar gibi kavramları da barındırır (Altınkaynak, 2018, s. 1). BG alanında çalışmalar yapmakta olan Securosis firması ise birbirine karıştırılan BG konusunu etraflıca detaylandırmış ve şu sınıflandırmayı yapmayı uygun bulmuştur (Pesen, 2015):

- Ağ Güvenliği (*Network Security*)
- Uç/Son Nokta Kullanıcı Güvenliği (*Endpoint Security*)
- Veri Güvenliği (*Data Security*)
- Uygulama Güvenliği (*Application Security*)
- Kimlik ve Erişim Yönetimi (*Identity and Access Management*)
- Güvenlik Yönetimi (*Security Management*)
- Sanallaştırma ve Bulut (*Virtualization and Cloud*)

Bazı araştırmacılara göre her ne kadar siber güvenlik, bilgi güvenliğine göre daha geniş ve kapsamlı bir kavram gibi gözükse de, bilgi güvenliği konusunun daha ayrıntılı olarak ele alınıp incelenmesinden sonra ve güncel yeni teknolojilere ait birçok uygulamanın ve alanın bilgi güvenliği konuları altında konumlandırılması ihtiyacı ve gerekliliğinden dolayı, BG'nin siber güvenlik de dâhil olmak üzere birçok alanı kapsayıcı olduğunu ileri sürmek de mümkündür.

BG; kullanıcı doğrulama ve yetkilendirme, ağ güvenliği, donanım güvenliği, yazılım güvenliği ve veri şifreleme gibi çeşitli alanları içerecek şekilde genişletilmiştir. BG, neredeyse tüm bilgi işlem uygulamalarını korumak için çok önemli bir ihtiyaç haline gelmiştir (Awad, 2018, s. 3). Bunun yanı sıra otomasyonlar, akıllı şehirler, sağlık ve tele-tıp, otonom araçlar ve Nesnelerin İnterneti gibi birçok yeni alan BG içine dâhil edilmeye başlanmıştır.

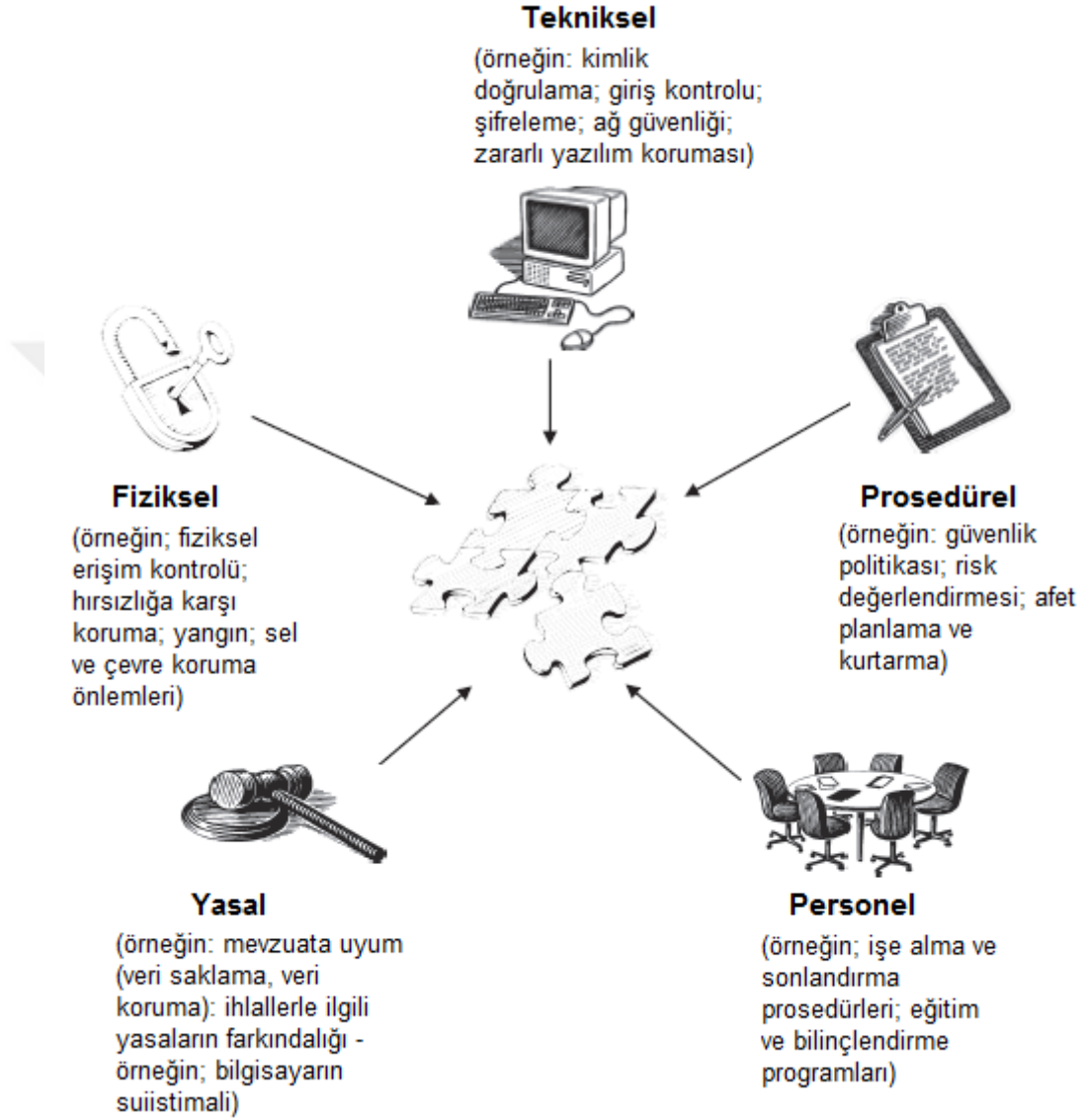
BG (information security); bilgilerin güvenliğinin sistemli bir şekilde sağlanması, kuruluşun faaliyetlerinin sürekliliğinin devamı üzerine bilgilerin olası her türlü tehlike ve tehditlerden korunmasıdır. BG’ni sağlamak için başta bilgisayar sistemlerinde, insan kaynakları bölümünde, üçüncü taraflarla ilişkilerde ve çevresel koşullarda yapılacak düzenlemeler olmak üzere birçok alanda alınması gereken önlemler/faaliyetler bulunmaktadır. (...) BG bir “kurum kültürü” olmalıdır. Kurum çalışanlarının top yekûn sorumlu olmaları gereken bir kavramdır (Çubukçu, 2018, s. 3). BG kavramına yalnızca veri güvenliği (verilerin korunması) olarak değil, bütüncü bir yaklaşım çerçevesinden bakmak gerekmektedir. Bu açıdan yaklaşıldığında Çubukçu (2018)’ya göre BG’ni sağlamanın şirketler için en doğru yolu ISO/IES 27001 standartlarının uygulanması ve onun yönetim sistemi olan Bilgi Güvenliği Yönetim Sistemini (BGYS) kurmak ve uygulamaktır. BG’nin şu başlıklar çerçevesinde bir bütün olarak ele alınması süreklilik, verimlilik, bütünlük ve güvenilirlik açısından önemlidir:

- Bilgilerin korunması, yetkisiz ve izinsiz erişimlerin engellenmesi
- BG ihlallerinin tespiti ve önlenmesi
- Siber saldırı risklerine karşı güvenlik önlemlerinin alınması
- İş sürekliliği ve rekabet üstünlüğünün sağlanması
- Üçüncü taraflarla, iş ortaklarıyla ve çalışanlarla gizlilik anlaşmalarının (confidentiality agreements) düzenlenmesi
- Yasal uygulamaların yerine getirilmesi ve takibi için gerekli yapı ve insan kaynaklarının, donanımın sağlanması

BG günümüzde tek bir alanı değil birçok alanı eş zamanlı olarak ilgilendirmekte olup, yaklaşımların bütüncü bir çerçeve içerisinde algılanması önem taşımaktadır. Büyük resmin görülebilmesi ancak bu şekilde mümkün olabilmektedir.

BG yapbozunun unsurlarını bu açıklamaya bağlı olarak Şekil 20’de şu şekilde ifade etmek mümkündür.

Şekil 20. Bilgi Güvenliği Yapbozu’nun Unsurları



Kaynak: Furnell, 2005. s. 7 Akt: Furnell, 2018, s. 19

Sadece birkaç yüz dolar karşılığında, suçlular bir *femtocell*, yani yeterli sinyal olmayan bölgelerde insanların mobil telefon hizmetlerini geliştirmek için kullandıkları bir kablosuz ağ genişleticisi satın alıp kullanarak (Montopoli, 2013 Akt: Goodman, 2016, s. 165) cihaz üzerinden gönderilen tüm verilerin elde edilmesini

sağlayabiliyorlar. Suçlular bu cihaz sayesinde, insanları kendi kulelerine (vericilerine) çekerek banka hesabına giriş şifrelerinden tutun da, gönderdikleri tüm hassas e-postalara kadar her şeye erişim sağlayabiliyorlar. Aynı yöntemle bir yandan ticari ofislerin etrafından bilgiler toplanırken, diğer yandan havalimanları ile çok sayıda iş adamının bulunduğu büyük konferanslar hedef alınabiliyor (Goodman, 2016, s. 165).

Henüz toplum tarafından kesin sınırlarla ayrılarak net olarak anlaşılamayan veri, enformasyon ve bilgi kavramları iç içe geçmekte, veri ve enformasyona yönelik tehditler dolaylı olarak bilgiyi tehdit etmektedir. Bu tehditlere yönelik önlemler de bu doğrultuda planlanmalıdır (Yiğitbaşı, 2015, s. 58). Dolayısıyla BG doğrudan veri ve enformasyon güvenliğini de kapsamaktadır.

2.1 Tanımı

BG, bir varlık türü olarak bilginin izinsiz veya yetkisiz bir biçimde erişim, kullanım, değiştirilme, ifşa edilme, ortadan kaldırılma, el değiştirme ve hasar verilmesini önlemek olarak tanımlanmakta ve “gizlilik”, “bütünlük” ve “erişilebilirlik” olarak üç temel unsurdan meydana gelmekte ve bu üç temel güvenlik ögesinden herhangi biri zarar görürse güvenlik zafiyeti oluşmaktadır (Pesen, 2015). Bu manada da BG kavramını bütüncü bir yaklaşımla ele almak ve gözetmek doğru bir adım olacaktır:

- *Gizlilik*: Bilginin yalnızca ilgili ve yetkili kişilerin erişimine açık olmasıdır.
- *Bütünlük*: Bilginin mevcut halinin değiştirilmeden (olduğu gibi) korunmasıdır.
- *Erişilebilirlik*: Bilginin yetkili kişilerce istenildiğinde ulaşılabilir ve kullanılabilir olmasıdır.

BG; işletme içinde, bilgilerin yetkisiz kullanıcılara ifşa edilmesine (gizlilik), uygunsuz değişikliklere (bütünlük) ve gerektiğinde erişime izin vermemeye karşı korunmasının sağlanmasıdır (uygunluk) (www.isaca.org). BG; bilgi ve bilgi sistemlerinin, izinsiz erişime veya bilgilerin depolanmasında, işlenmesinde veya nakliyesinde ve yetkili kullanıcıların hizmet reddine karşı korunmasına karşı korunmasıdır. BG, bilgisayar güvenliği ve iletişim güvenliğinden oluşur. Ayrıca INFOSEC olarak da bilinir (www.thefreedictionary.com). Bilgi Sistemleri Güvenliği

(Information System Security-ISS) ise, bilgilerin veya diğer kritik unsurların donanım veya yazılımı yetkisiz kullanım, erişim, açıklama, aksaklık, değişiklik veya imhadan korunmasıdır; böylece amaç, saklanan bilgilerin gizliliğini, bütünlüğünü ve kullanılabilirliğini sağlamaktır (www.isaca.org).

Hemen hemen tüm organizasyonlar için geçerli olan ve araştırmacıların üzerinde büyük oranda anlaşmış oldukları BG üçgeni (AIC triangle: availability, integrity, and confidentiality) *erişilebilirlik*, *bütünlük* ve *gizlilik* özelliklerinin bir arada bulundurulması üzerine inşa edilmiştir. Şekil 21’de bu durum görsel olarak ifade edilmiştir. Yukarıda da açıklandığı üzere erişilebilirlik/kullanılabilirlik (availability); ihtiyaç duyulan verilerin her zaman ilgili kişi tarafından ulaşılmasını sağlamak anlamına gelmektedir. Bütünlük (integrity); verilerin doğru ve yetki(li) dışında değişikliklerden veya istenmeyen müdahalelerden korunmasını sağlamak anlamına gelmektedir. Gizlilik (confidentiality) ise, (bilgisayarda) depolanan verilerin yalnızca erişim hakkı olanlar tarafından görülebilmesi anlamına gelmektedir.

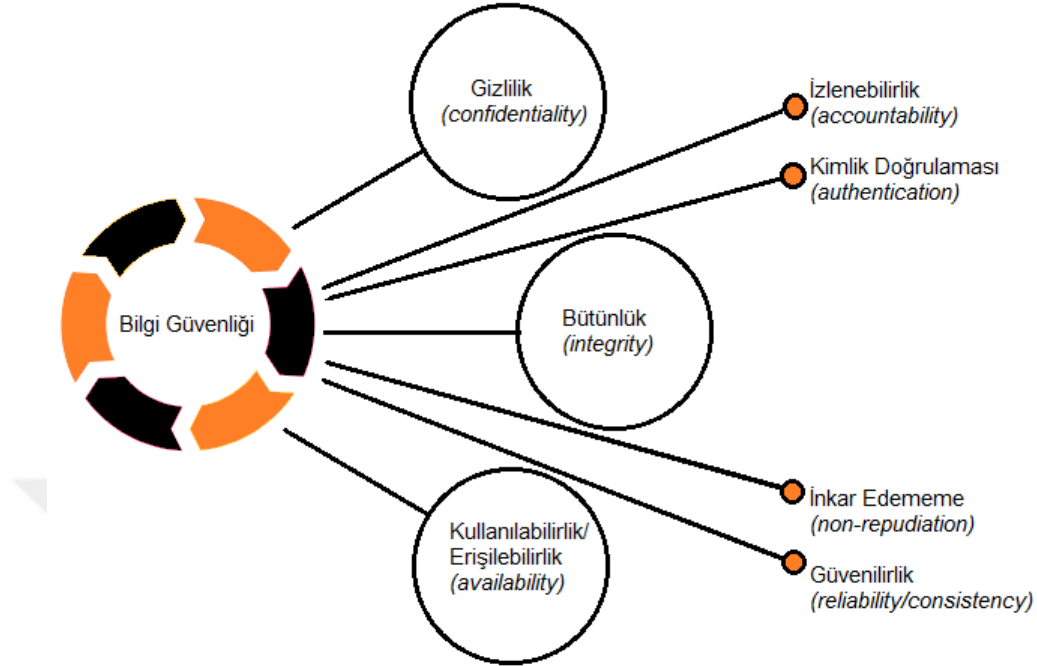
Şekil 21. Bilgi Güvenliği Üçgeni (AIC Triangle)



Kaynak: Pesen, 2015’den uyarlanmıştır.

Bilgi güvenliğinin yukarıda bahsedilen üç prensibine ek olarak aşağıdaki prensiplerden de ayrıca bahsetmek mümkündür. Bunlar; izlenebilirlik (accountability), kimlik doğrulaması (authentication), inkâr edememe (non-repudiation) ve güvenilirliktir (reliability/consistency) (Baktır, 2013, s. 116-117). Bu toplam yedi prensip Şekil 22’de görsel olarak ifade edilmiştir.

Şekil 22. Bilgi Güvenliğinin (Temel) Prensipleri



Gizlilik: Bilgilerin yalnızca yetkili kişiler tarafından kullanılmasını sağlamak, diğer bir ifadeyle yetkisiz kullanıcıların (izinsiz) erişimlerinin engellenmesidir. Gizlilik, verinin isteyerek ya da istemeyerek ifşa edilmesini engeller. Gizliliği sağlamak için parola, şifreleme, çeşitli erişim kontrolleri gibi aracı yöntemler kullanılır.

Bütünlük: Bilginin doğru, gerçek, değiştirilmemiş, bozulmamış ve güvenilir olmasının sağlanmasıdır. Aynı zamanda bilgi kaynağının doğru zamanda ve doğru kişi tarafından değiştirilmesini sağlar. Böylece her türlü ve özellikle kritik bilgilerin yanlışlıkla ya da isteyerek değiştirilmesinin (manipüle edilmesinin) ya da bozulmasının önüne geçilmiş olunur. Bütünlüğü sağlamak için özetleme algoritmaları, mesaj özetleri, sayısal imzalar vb. kullanılmaktadır.

Kullanılabilirlik/Erişilebilirlik: Veri ya da bilgiye yetkililer tarafından ihtiyaç duyulduğu anlarda her yerden ve her zaman erişilebilmesidir. Kullanılabilirlik için yedek sistemler, afet sistemleri, bakım, yedekleme, alternatif haberleşme kanalları vb. kullanılmaktadır.

İzlenebilirlik: Sistem üzerinde(n) gerçekleşen olayların/işlemlerin daha sonra analiz edilmek üzere kayıt altına alınmasıdır.

Kimlik Doğrulaması: Alıcının, göndericinin iddia ettiği kişi olduğundan emin olmasıdır. Bunun için özetleme algoritmaları, mesaj özetleri, sayısal imzalar ve güvenli sertifikalar kullanılmaktadır. Ayrıca iki faktörlü kimlik doğrulama (2FA - Two Factor Authentication) ve Blockchain teknolojileri de kullanılmaktadır.

İnkâr Edememe: Bilgiyi gönderen ya da işleyen kişinin yaptığı işi sonradan inkâr edememesidir. Bunun için sayısal (elektronik) imzalar ve işlem kayıtları (log) kullanılmaktadır.

Güvenilirlik: Sistemin planlandığı gibi çalışması ve her seferinde aynı davranışı sergilemesidir.

Kaynak: Pesen, 2015 ve Baktır, 2013, s. 116-117'dan uyarlanmıştır.

BG'den bahsedildiğinde ilk akla gelen kişisel BG olmakla birlikte, daha önemli olan kurumsal BG'dir. Kurumsal BG kişilerin (son kullanıcıların) BG'ni doğrudan etkilemektedir; her birey bilgi sistemleri üzerinden hizmet alırken

kurumsal bilgi varlıklarını doğrudan ya da dolaylı olarak kullanmaktadır. Kurumsal bilgi varlıklarının güvenliği sağlanmadan kişisel BG'nin varlığından bahsetmek zordur (Baktır, 2013, s. 117).

2.2 Tarihi Süreç

Bilginin korunması ve güvence altına alınması ile ilgili ilk bulgular MÖ 2000'li yıllara, Mısır toplumuna ait kalıntılarda kriptoloji (şifreleme bilimi) tarihinin ilk kayıtlarına rastlanmasına kadar dayandığı düşünülmektedir. Bu dönemde geliştirilen şifreleme yöntemleri arasında; sadece ilgili kişilerce anlaşılması istenilen simgelerin yazı içinde kullanıldığı, yazının *scytale* olarak bilinen şerit şeklindeki kağıdın belirli bir çaptaki silindire sarılarak yazılması, daha sonraları ise Roma imparatoru Sezar'ın yazılarında kullandığı her harfin alfabede kendisinden sonra gelen üçüncü harfle yer değiştirdiği gibi metotlar bulunmaktadır (Bilgem, 2013 Akt: Yiğitbaşı, 2015, s. 57).

1960'lar ve 1970'ler bilgisayar teknolojisinde hızlı bir teknolojik gelişme dönemi idi ve bunun yanında ortaya çıkan güvenlik açıklarından yararlanma fırsatları da doğmuş oldu. Etkileşimli bilgi işlem, zaman paylaşımı, kullanıcı kimlik doğrulaması, hiyerarşik dosya yapıları üzerinden dosya paylaşımı ve bilgisayar yardımcı program prototipleri 1960'larda bir teknik yenilikler dalgasının parçası oldu. Bu dalganın yanı sıra, erişim kontrolleri ve şifreler gibi nispeten basit güvenlik araçları kullanıldı. Gelecek on yılda, yerel alan ağlarının (LAN'lar), paket ağların (ARPANET) ve nesneye yönelik tasarımın, genel anahtar şifreleme, güvenlik doğrulama, şifreleme protokolleri ve şifreleme karmaşıklığı gibi bir şifreleme uygulamaları dalgası görüldü. Bilgi sistemlerinin gerekli bir özelliği olarak artan güvenlik bilinci, matematiksel güvenlik modellerinin uygulanmasına ve ispatlanabilir güvenli sistemlerin ilk kez uygulanmasına yol açtı (Denning ve Denning, 2016, s. 5 Akt: Hatfield, 2018, s. 106).

İnternetin keşfinin 1969 yılında olduğunu söylemek mümkündür. O yıllarda bilinen adıyla ARPA (US Advanced Research Project Agency) (şimdi DARPA olarak bilinmektedir) araştırmacıları Kaliforniya Üniversitesi ve Stanford Araştırma Enstitüsü arasında bir veri ağı kurmuşlardı. 1971 yılında bir tür e-posta oluşturuldu. 1973'te ise Londra Üniversitesi ağa bağlanarak kıtalar arası bağlantıyı gerçekleştirdi. Daha sonra diğer ülkelerde de ağlar oluşturuldu ve bunlar birbirlerine (bugün de hala

kullanılan) TCP/IP adı verilen sistemle bağlandı. Daha sonraları Berners-Lee bugün internet olarak bilinen World Wide Web (www) hizmetini geliştirdi. Hiper metin kullanılarak içerikler (kaynaklar) bir birleriyle bağlandı ve bunu takiben ilk web sayfası 1991’de yayınlandı. 1996 yılında Hotmail web tabanlı e-posta hizmetini, 1998 yılında ise Google arama motoru hizmetini geliştirdi. 2015 yılında İnternet Servis Sağlayıcıları (ISP) sayesinde kitlelere ulaşıldı (Løkke, 2018, s. 28). Bugün ise gelecek on yıl içerisinde Nesnelerin İnterneti (IoT) sayesinde bir birine bağlı elli milyar kadar cihazın olacağından bahsedilmektedir. Bu hızlı gelişim Intel’in kurucularından Gordon Moore’un belirlediği ve *Moore Yasası*⁹ olarak bilinen yaklaşıma göre, artışın benzer bir hızda (karşı çıkanlar olmakla birlikte) on yıl kadar daha devam edeceği öngörülmektedir.

Modern işletmeler büyük oranda bilişim sistemlerine bağımlıdır. Bu bağımlılık, işletmelerin bu bilişim sistemlerinin bozulmasına neden olan olaylara karşı savunmasız kalmalarına neden olmuştur. Sonuç olarak, bu sistemler için risk yönetimi, dünya çapındaki firmalar açısından büyük önem kazanmıştır. Ernst ve Young tarafından yapılan bir çalışma, şirketlerin küresel olarak %93’ünün siber saldırılara karşı artan tehditle mücadele etmek için siber güvenlik konusundaki yatırımlarını sürdürdüklerini veya artırdıklarını göstermiştir (Van Kessel ve Allan, 2013 Akt: Flores ve Ekstedt, 2016, s. 26). Günümüzde en önemli devrimler felsefe bölümlerinde, hatta parlamentolarda ve şehir meydanlarında değil, laboratuvarlarda, araştırma tesislerinde, teknoloji firmalarında ve veri merkezlerinde gerçekleştirilmektedir (Susskind, 2018, s. 7). Fiziksel dünyaya nüfuz etmenin yanı sıra, teknoloji, insanlar arasında, insanlar ve makineler arasında ve makinelerin kendi arasında bilgi alışverişini kolaylaştırarak daha fazla bağ kurmaya devam edecektir. Bin yılın başından bu yana, internete bağlı insanların sayısı 2000 yılında yaklaşık 400 milyondan 2016 yılına gelindiğinde 3,5 milyara yükseldi (Internet Live Stats Akt: Susskind, 2018, s. 45). Bu sayının 2021 yılına kadar yaklaşık 4,6 milyara yükselmesi bekleniyor (Cisco Akt: Susskind, 2018, s. 45). Sonunda, dünya nüfusunun çoğunun, yalnızca masaüstü bilgisayarlar üzerinden değil, akıllı cihazlar, akıllı telefonlar, tablet bilgisayarlar, oyun konsolları ve giyilebilir cihazlar aracılığıyla

⁹ **Moore Yasası:** 1965’lerde, teknolojik ilerlemelerden dolayı, her 18 ayda bir, işlemci hızının (mikroişlemciler içerisindeki transistör sayısının) iki katına çıkacağı öngörülmüştür. (Fazla ısınma sorunu yüzünden gelişme/artış [son zamanlarda] tam olarak bu şekilde devam edememiştir).

kablosuz internet tabanlı ağılara da bağlanacağı anlaşıyor. Facebook'un şu anda 2 milyardan fazla aktif kullanıcısı bulunmakta (Statista Akt: Susskind, 2018, s. 45). Twitter'ın beşte dördü mobil teknolojiden erişim sağlayan 313 milyondan fazla kullanıcısı bulunmakta (Twitter.com Akt: Susskind, 2018, s. 45). YouTube'da ise 1 milyardan fazla aktif kullanıcı yer almaktadır (YouTube for Press Akt: Susskind, 2018, s. 45).

2.3 Bilgi Toplama Yöntemleri

SM'de kullanılan sızma (penetrasyon) testlerinin elektronik ortamda yapılanları ve bunların benzerleri BG alanında bilgi toplama yöntemleri açısından birincil araç olarak kullanılabilir.

Bilgi toplama yöntemlerinde iki husus vardır (Aslanbakan, 2017, s. 21): Bunlar; aktif bilgi toplama ve pasif bilgi toplama yöntemi olmak üzere iki çeşittir. Aktif bilgi toplama; sistemle iletişime geçilerek bilgi toplama, pasif bilgi toplama ise sistemle iletişime geçmeden, iz bırakmadan bilgi toplama yöntemidir. Aslanbakan (2017)'a göre bilgi toplama tekniklerinden en çok kullanılan yöntemler/araçlardan bir kısmı şunlardır: Whois, Dnsdickt6, Dnsenum, TheHarvester, Wafw00f, Nmap, Ağ haritalama, NBTScan, Pipl, Traceroute, Bing.

Çeşitli yazılımlar aracılığıyla bilgisayar ya da akıllı telefonunuzun ön kamerası göz hareketlerinizi (izleyerek) kontrol ederek ekranın hangi noktasına baktığınızı tespit edebilmektedir. Örneğin, seyrettiğiniz bir video da ya da bakmış olduğunuz bir sayfada erkeğe mi kadına mı daha çok bakarak vakit geçirdiğinizden hareketle sizin cinsiyetiniz veya cinsel eğilimleriniz tahmin edilebilir ve devamında önünüze buna uygun içerikli reklamlar getirilebilir. İnsanlara takılacak olan çipler sayesinde ya da şimdiden var olan bileklikler (akıllı saatler, spor bantları) nabız atışlarınızı, tansiyonunuzu ve benzeri fizyolojik verilerinizi, tepkilerinizi (internet bağlantısı varsa anlık olarak) merkezden izleme, sınıflandırma ve/ya kontrol etme imkânı yaratabilmektedir. Örneğin X kişinin televizyondan yaptığı bir konuşma sonucunda toplanan bu verilerden yola çıkılarak ne kadar insanın (bunların demografik özellikleri, yaşadıkları şehir, ülke, mensubu oldukları üyelikler vb. onlarca veri ile birlikte) bu konuşmaya olumlu ya da olumsuz tepki verdiği (sinirlenip sinirlenmediği vb.) kolayca anlaşılabilecektir. Bu riskler karşısında Harari (2018) şu soruyu yöneltmektedir: Biyometrik sensörler aracılığıyla beden ve insan

beyninden toplanan veriler akıllı makinelere akıp durdukça, şirketlerin ve devletlerin bireyleri iyice tanıması, yönlendirmesi ve bireyler adına tercihler yapması kolaylaşacaktır. Bu durumda verinin sahibi kim olacak? DNA, beyin ve kişilerin hayatına ait veriler kişilere mi, devlete mi, bir şirkete mi, yoksa insanlığın tamamına mı ait olacak? (s. 86).

Teknolojinin pek çok faydası görülebilir fakat insan hayatında çok yer kaplarsa, insanlar onun gündemine esir düşebilir. İnsanlar binlerce yıl önce tarımı keşfetmiş ama bu teknoloji sadece bir avuç seçkini zenginleştirirken insanların çoğunu tutsak etmiştir. Çoğu insan kendini sabahtan akşama ot yolarken, kavurucu güneşin altında su kovaları taşıyıp mısır toplarken bulmuştur (Harari, 2018, s. 245). Kalabalıkları yönetmek için gruplar, grupları yönetmek için liderler gerekiyor. Sonuç olarak yönetenler ve yönetilenler var oldukça, çıkar ilişkileri bir şekilde devam edecektir. Yüksek popülasyon insanlık için sorun gibi gözüküyor. İnsan popülasyonundan daha kalabalık ama daha az sorunla yaşayabilen canlıları, yaşam formlarını araştırmak iyi (çözüm) olabilir. Günümüz bilgi çağında bu tür sorunların üstesinden gelebilmek için bilgi yönetimi ve bilgi güvenliğinin en üst sıralarda yer alması kaçınılmaz gözükmektedir.

2.4 Bilgi Yönetimi

Bilgi yönetiminde; bilgi elde etmeyi, depolamayı ve entelektüel değerleri birlikte ele almak gerekmektedir. Bilgi yönetimi; bir kurumda insan, teknoloji, süreç ve kurumsal yapıyı yeniden kullanmak (yenilemek) amacıyla belirgin sistematik bir koordinasyonun sağlanmasıdır (Yazıcıoğlu, Borat ve Kılıç, 2014, s. 9). Bilgi yönetimi, kurumsal bilginin çalışan tüm personele dengeli ve zamanında iletilmesini sağlayan ve aynı zamanda personel, bütçe, bilgisayar ve iletişim teknolojileri gibi birçok farklı unsuru bir arada barındıran sistemi ifade etmektedir. Bilgi yönetiminden hareketle bilgi yönetim sistemi ise; bilgi yönetimi disiplininin tasarımı, kurulması, uygulanması ve yenilenmesi sırasında personel, bütçe, yasal düzenlemeler, bilgisayar ve iletişim teknolojilerini oluşturan iletişim kanalları, web sayfaları, ağlar, veri tabanları, zaman-kalite yönetimi, sürekli eğitim gibi çok çeşitli unsurların bir arada ve uyum içerisinde kullanıldığı sistemi ifade etmektedir (Odabaş, 2005 Akt: Bakıoğlu, 2015, s. 88). İşletmelerin üretim süreçlerine katkılarında ise bilgi iki şekilde bulunmaktadır (Dinçmen, 2010, s.17), bunlar:

- **Açık bilgi** (*explicit, codified knowledge*): Kullanıma hazır, belirli bir formattaki bilgidir: Metin, teknik resim, formül, diyagram, grafik, tablo, bilgisayar programı, fotoğraf, film vb.
- **Örtülü bilgi** (*implicit, tacit knowledge*): Çalışanların kayda geçmemiş iş becerileri, yetenekleri ve iş yaparken gözlenebilecek, davranışlarını belirleyen beyinlerdeki bilgi kümesidir. İşletmelerin diğer kuruluşlar ve kayda geçmemiş deneyimleri ve ilişkileri de örtülü bilgi kapsamındadır.

Bilgi paylaşımında ve bilgi yönetiminde kullanılan bilişim araçları genel olarak şunlardır: Bilgi haritaları (knowledge map), intranet ve bilgi yönetimi portalları (knowledge management portals), veri mağazacılığı (data warehousing), veri madenciliği (data mining), belge yönetim sistemleri (document management systems), içerik yönetim sistemleri (content management systems), yerel ağlar (LAN: Local Area Network), geniş alan ağları (WAN: Wide Area Network) (Dinçmen, 2010, s. 23). Bilgi yönetiminde bilgi yönetimi araçlarının yanı sıra Öztemel (2010)'e göre bilginin yönetilebilmesi için birey düzeyinden kurum düzeyine geçilmesi önemlidir. Bireylerin sahip oldukları bilgileri bir araya getirerek kurumsal bilginin oluşturulması etkin bir şekilde yönetilmesi temel amaç olmalıdır. Kurumsal bilgiyi kurumun amaçlarını gerçekleştirebilmede kullanabilmek için modelleri oluşturmak ve uygulamaya koymak gerekmektedir. Kurumsal bilgiyi statik bir yapıda tutmak mümkün değildir. Başarılı bir yönetim için bu bilginin sınırlandırılmaması önemlidir. Kurum içinde üretilen veya kuruma dışarıdan gelen, o kurumla ilgili kayıtlı ya da kayıtsız her türlü bilgi kurumsal bilginin bir parçası olarak görülmeli ve yönetilmelidir (s. 2). Sınırlandırılmayan bilginin güvenliğinin sağlanması son derece önemlidir. Dolaşımda olan bilginin her türlü güvenliğini sağlamak kurumlar için prestij, güvenilirlik, iş yapabilirlik, iş sürekliliği, bilgi varlıklarının korunması, müşteriye ya da iş ortaklarına karşı (hukuksal) sorumluluk gibi bir çok önemli kavramı içinde barındırmaktadır. Bu ve benzeri nedenlerden dolayı BG'ne bütüncü bir yaklaşımla bakmak gerektiği bir kez daha doğrulanmış olmaktadır.

Bilgi yönetimi ayrıca, bilginin oluşturulması, saklanması, nakledilmesi ve uygulanması için örgüt içinde geliştirilmiş bir dizi iş sürecini ifade etmektedir. Bilgi

yönetimi, örgütün çevresinden öğrenme ve bilgiyi kendi iş süreçlerine katma kabiliyetini artırır. (...) Etkin bilgi yönetimi %20 teknoloji, %80 yönetim ve örgüt yönetimidir (Laudon ve Laudon, 2011, s. 419). Çevresel öğrenme sayesinde kazanılan edinimler iş süreçlerine aktarılırken örgütün kurumsal hafızası, önceki iş deneyimleri, örgüt kültürü ve örgüt politikaları gibi filtrelerden geçirilip rafine hale getirilerek uygulanmalıdır.

Bilgi yönetimi; veri madenciliği, uzman sistemler, yapay sinir ağları, bulanık mantık (fuzzy logic), genetik algoritmalar ve akıllı temsilciler (agent) gibi farklı akıllı teknikler grubunu da kapsar. (...) Akıllı teknikler; yapay zekâ ve veri tabanı teknolojisi kuruluşlarını bireysel ve anonim bilgileri elde etmek, bilgi tabanlarını genişletmek için kullanacakları birçok akıllı teknikler sunmaktadır. Uzman sistemler ile bulanık mantık ise daha çok örtülü bilgiyi elde etmek için kullanılmaktadır. Yapay sinir ağları ve veri madenciliği ise daha çok bilgi keşfi için kullanılmaktadır. Bu tür keşifler, yöneticiler tarafından kendi başlarına veya deneyimleri aracılığıyla bulamayacakları, Büyük Veri katmanlarının içinde yer alan örüntüleri (pattern), kategorileri, bağlantıları ve ilişkileri içermektedir. Genetik algoritmalar ise insan zekâsı ve onun düşünme hızı ve kapasitesiyle (herhangi bir yardım almadan ve araç kullanmadan) ortaya çıkarılması ve analiz edilmesi pekte kolay gözükmeyen karmaşık ve hacimli sorunlara çözüm üretmek için kullanılmaktadır. (...) Yapay sinir ağları çok sayıda verinin toplandığı karmaşık, az anlaşılmış sorunları çözmek, hacimli verilerde örnek ilişkiler keşfetmek için kullanılmaktadır. Yapay sinir ağları bu bilgileri insan beyni veya biyolojik modelle paralellik gösteren donanım ve yazılımları kullanarak keşfeder. Yapay sinir ağları bu modellemelerle veriler üzerinde incelemeler yaparak ilişkileri araştırır ve örnekler oluşturarak kendi hataları üzerinde tekrar tekrar düzeltme yaparak (en iyi optimizasyon ile) çok sayıda veriden öğrenme gerçekleştirir. Uzman sistemler uzman birinin problemi çözme yoluna benzetme veya modelleme yolları ararken, yapay sinir ağlarında çözüm planlanmadan sorunlara çözüm üretildiği öne sürülmektedir (Laudon ve Laudon, 2011, s. 421-437).

Bu bilgilerden hareketle uzman sistemler belirli bir soruna belirli bir yöntem ile çözüm ararken/üretirken, yapay sinir ağlarında amaç sistemin (sürekli döngü sayesinde en iyi optimizasyona ulaşarak) kendi kendine o an için (mevcut) en iyi sonucu elde etmesi, sistemin kendi kendine öğrenmeyi ve çözüm üretmeyi yönetebilmesidir. Bu yaklaşım aynı zamanda makine öğrenmesine de bir temel oluşturmaktadır.

2.5 Bilgi Güvenliğine Yönelik Saldırı ve Önlemler

Flores ve Ekstedt (2016) yapmış olduğu araştırmalarında BG konusunda şu sonuçları elde etmişlerdir: Dünya çapındaki firmalar, kurum çapında bilgi güvenliğini sağlamak için çok miktarda para harcamalarına rağmen BG tehditlerini yönetmeye ilişkin davranışsal girişimler halen yeterli değildir. Kuruluşların

çalışanlarının BG tehditleriyle ilgili inançlarını ve tutumlarını değiştirmesinin önemli olduğu görülmektedir. Çalışanların, bilgisayar sistemlerini korumalarının önemini, sosyal mühendislerin kötü niyetli davranışlarda bulunabilecekleri ve bunların uygulanmasındaki manipülasyon tekniklerinin farkında olmaları gerekmektedir. Ancak, tehditlere karşı sadece farkında olmak yeterli değildir. İnsanlar kendileri için iyi olmayan şeylerin farkında olabilirler, fakat bu onların davranışlarını değiştirecekleri anlamına gelmez (böyle olsaydı, bugün daha az sigara içen olurdu). Çalışanların saldırıları önlemeye yönelik tutumlarının değiştirilmesi gerekiyor. Çalışanların, BG davranışlarını değiştirmenin önemi ve yararları hakkında bir anlayış geliştirmeleri gerekmektedir. Çalışanların BG hakkında öğrendiklerinin hem kendi bireysel çıkarları hem de kurumları için olumlu sonuçlar doğuracağını anlamaları gerekmektedir. Bu nedenlerle, güvenlik eğitimi programlarında verilen bilgilerin somutlaştırılması ve kişiselleştirilmesi, eğitimi kişisel olarak ilgi çekici ve anlaşılır kılacaktır (s. 40).

IDS (Intrusion Detection System – Saldırı Tespit Sistemleri), akıllı olarak tanımlayabileceğimiz sistemlerden yalnızca birisidir. Ağ üzerinde konumlanan bu sistem, ağa yönelmiş olan tüm trafiği algılamakta, veri paketlerinin içeriğine bakmakta ve bir saldırı olup olmadığına karar vererek aksiyon almaktadır. Bu aksiyon bir cihazı ya da kullanıcıyı uyarmak, rapor vermek ya da gerekiyorsa tüm sistemi kesmek/kapatmak şeklinde işleyebilmektedir (Altınkaynak, 2018, s. 196). Gelecekteki birçok sistemin (yapay zekânın da desteği ile) IDS mantığına yakın bir yaklaşımla çalışılacağını düşünebiliriz. Zira, insan yönetiminde olan birçok sistem ve güvenlikle ilgili kontroller insani zafiyetlerden dolayı kolay kırılıma uğrayabilmekte ve bu durum sistemin işleyişine büyük zararlar verebilmektedir.

DNS (Domain Name System - Alan Adı Sistemi) saldırıları bir ülkeye karşı yapıldığında ülke genelinde önemli zararlara yol açabilmektedir. Nitekim bir ülkenin DNS sunucuları işlemez ve cevap veremez konuma gelirse, o ülkenin interneti de çalışmaz hale gelecektir. Ülkeye yapılacak en önemli saldırı, ülkenin en yetkili DNS sunucularına yönelik yapılan saldırılardır (Altınkaynak, 2018, s. 205). Bu tehlikelerin bilincinde olarak ulusal güvenlik için birincil düzeyde öneme sahip olan DNS sunucularının tespit edilerek özel bir düzenleme ile her türlü saldırı ve risklere karşı korunması bir devlet politikası haline getirilmesi gerektiği düşünülmektedir. BG için

alınacak önlemler bilgi teknolojilerinin gelişim hızına ayak uydurmak zorunda ve sürekli güncel tutulmak durumundadır. Zira, büyük bir ivme ile değişen teknoloji ve onun yapısal modifikasyonu yeni açıkları gündeme getirmekte ve yeni çözüm arayışlarını kaçınılmaz kılmaktadır. Bunun yanı sıra internet ve ağ teknolojisinin yapısı büyük oranda aynı kaldığı ve benzer altyapı donanımlarıyla hizmet verdiğinden dolayı, klasik olarak bilinen ve halen geçerliliğini büyük oranda koruyan yapısal (güvenlik ve protokol) katmanlarının kullanımı günümüzde de devam etmektedir. Bu katmanları kısaca şu şekilde hatırlatmak faydalı olacaktır:

Güvenlik duvarları (firewalls), önceden belirlenmiş güvenlik kurallarına göre gelen ve giden trafiği izleyerek ve kontrol ederek yerel bir ağı koruyan donanım veya yazılım cihazlarıdır. Yerel bir ağ ve internet arasında konumlanırlar. İzinsiz giriş algılama ve önleme sistemleri (IDPS-Intrusion Detection and Prevention Systems) de benzer şekilde çalışırlar, ancak daha fazla işlevselliğe sahiptirler. Yerel ağa veya ana bilgisayara (sunucuya) konumlanırlar ve sistemleri raporlar, algılar veya korurlar. Dijital imza, Genel Anahtar Altyapısının (PKI-Public Key Infrastructure) bir parçasıdır. İçeriğini ve gönderenin kimliğini doğrulamak için elektronik olarak iletilen bir belgeye eklenmiş bir kod olarak kendini gösterir. (...) Dijital sertifikalar da Genel Anahtar Altyapısının bir parçasıdır. Dijital sertifikalar, bir genel anahtar sahipliğini kanıtlamak için kullanılan elektronik belgelerdir. Sertifikanın içeriğini doğrulayan dijital imzanın yanı sıra, sahibinin kimliğiyle ilgili bilgiler de sertifikaya dâhil edilmektedir. (...) Genel Anahtar Altyapısına dayanan ve Netscape'in Güvenli Yuva Katmanı (SSL-Secure Sockets Layer) protokolünden geliştirdiği Aktarım Katmanı Güvenliği (TLS-Transport Layer Security) bir web sunucusu ile tarayıcı arasında şifreli bir bağlantı kurmak için en sık kullanılan güvenlik teknolojisidir (James, Bulajoul, Shehu, Li ve Obande, 2018, s. 126-128).

Şekil 23'de görüleceği üzere, literatürde yer alan BG'ne ait çeşitli sınıflandırmalara bakılacak olursa, karşımıza genel olarak en çok şu alt başlıkların çıktığını söylemek mümkündür:

Şekil 23. Bilgi Güvenliği Alt Başlıkları



- Güvenlik Yönetimi (*Security Management*)
- Ağ Güvenliği (*Network Security*)
- Sosyal Ağlarda Güvenlik (*Security in Social Networks*)
- Uç/Son Nokta Kullanıcı Güvenliği (*Endpoint Security*)
- Veri Güvenliği (*Data Security*)
- Uygulama Güvenliği (*Application Security*)
- Kimlik ve Erişim Yönetimi (*Idendity and Access Management*)
- Sanallaştırma ve Bulut (*Virtualization and Cloud*)
- İki Faktörlü Kimlik Doğrulama (*2FA - Two-Factor Authentication*)
- Fiziksel Güvenlik (*Physical Security*)
- Personel Güvenliği (*Personel Security*)
- Siber Saldırlara Karşı Güvenlik (*Security Against Cyber Attacks*)
- Felaketten Kurtarma (*Disaster Recovery*)

2.5.1 Güvenlik Yönetimi (*Security Management*)

BG alanında tehdit unsurları açısından bilgi sistemlerine (dolayısıyla kurum güvenliğine) zarar verebilecek üç tip tehdit bulunmaktadır. Kara (2018) bu üç unsuru şu şekilde açıklamaktadır; doğal tehditler, kasıtsız tehditler ve kasıtlı tehditler. Doğal

tehditler; daha ziyade insan faktöründen kaynaklanmayan, su taşkınları, yıldırım, deprem, yangın gibi doğa olaylarıdır. Kasıtsız tehditler; insan faktöründen kaynaklanan fakat bilinçli olarak yapılmayan davranış, tutum ya da işlem sonucunda ortaya çıkan tehditlerdir. Kasıtlı tehditler ise; yine kasıtsız tehditlerde olduğu gibi insan faktörü ile oluşan tehditleri kapsar ancak belirli bir amaca yönelik olarak yapılan, etki ve sonuçları bilinen bilinçli tehditlerdir (s. 27).

BG tehdit unsurları arasında (dolaylı ya da dolaysız) insan faktörü daha önce de ifade edildiği üzere SM ataklarında da olduğu gibi ön plana çıkmaktadır ve en zayıf halkalardan birini oluşturmaktadır. Kurumsal risk oluşumunda risk formülü; tehdidin olma ihtimali ile tehdidin etkisinin çarpımından elde edilmektedir ($Risk = \text{tehdidin olma ihtimali} \times \text{tehdidin etkisi}$). Risk formülünde yer alan bu iki belirleyici parametrede de insan faktörü etkisi oldukça yüksektir.

2.5.2 Ağ Güvenliği (*Network Security*)

Ağ güvenliği genel olarak şu alt başlıklar altında incelenmektedir (Pesen, 2015);

- İçerik Güvenliği (*Content Security*)
- Çevresel Savunma (*Perimeter Defense*)
- Ağ Erişim Kontrolü (*Network Access Control*)
- Kablosuz İletişim (*Wireless Communication*)
- İzleme (*Monitoring*)
- Yönetilir Hizmetler (*Managed Services*)

Güvenlik, ağlar için en az iki nedenden dolayı önemli bir konudur. Birincisi, ağlarda bulunan bilgiler eğitim, ticaret, sağlık hizmetleri, ulusal savunma ve diğer birçok alan için giderek daha fazla kullanılmakta ve bu tür bilgiler güvenlik açısından hassas olabilmektedir. İkincisi, bilgisayarlar evde, üniversitede, işyerinde veya devlet kurumlarında kullanılmakta ve eğer bir ağ üzerinden diğer bilgisayarlara bağlıysa, kaynaklar risk altındadır. Ağa bağlı bir bilgisayar dünyanın her yerinden on milyonlarca kullanıcıya erişim verebilir ve bu durum neredeyse herkesin ağ üzerindeki bilgisayara (veri ve bilgilere) ulaşabilmesi anlamına gelebilir (*Network Security*, s. 341).

Günümüzde işletmeler düzenli, verimli, üretken ve sürdürülebilir bir düzeyde bilgi üretme ve bilgi paylaşımında bulunmak için bilgisayar ve bilgisayar ağlarını kullanmak durumundadır. Kişisel kullanımdan (kişisel iş istasyonlarından) servis sağlayıcılara kadar geniş bir yelpazeyi ilgilendiren ağ güvenliği için teknik elemanlar kadar olmasa da belirli düzeyde güvenlik önlemlerini tanımak ve bilmek her kullanıcı için gerekli ve önemlidir. SM alanında geçerli olan en zayıf halka kavramı BG için de söz konusudur, saldırılar özellikle zayıf olan halkaya ya da o halka üzerinden sisteme yapılmak istenmektedir.

Bütüncü olmayan güvenlik sistemleri sonuç olarak istismar edilir. Güvenlik yönetimi ağ üzerinde çalışan her şeyin güvenliğini de içerdiğinden süreklilik gerektirmektedir (Altınkaynak, 2018, s. 188) ve güvenli iletişim için öne çıkan özellikler şunlardır: Gizlilik; gönderilen ve alınan paketlerin (bilgilerin) yalnızca ilgili taraflarca alınıp anlaşılması/yorumlanması, araya giren başka kişilerce bu bilgilerin ele geçirilememesi ve çözülmemesi gerekmektedir. Bütünlük; gönderilen paketlerin (bilgilerin) içerik değişimine uğramadan alıcısına ulaştırılması gerekmektedir. Erişilebilirlik; dolaşımdaki bilgilere ilgili veya tanımlanmış kişilerce ulaşılabilir olması gerekmektedir.

Bir haber sitesinin duyurmak istediği tüm haberleri dışarıya yayamaması ya da bu haberlerin manipüle edilmesi, bir fabrikanın network ürünlerinden birinin bozulması neticesinde, ünitelerin birbirleri ile yanlış ya da eksik iletişim kurması sonucunda ortaya çıkacak zarar büyük boyutlara ulaşabilir. Şu durumda gerek ev kullanıcıları gerekse kurumsal ağ kullanımlarından sıkı bir ağ güvenliği önlemi sağlanmalıdır (Altınkaynak, 2018, s. 189). Ağ güvenliği için (tek başına savunma sağlayamasa da) ilk sırada yer alan ve kolayca uygulanabilen güvenlik duvarı sistemleri yer almaktadır. Hunter (2013) güvenlik duvarlarını (firewalls), paketleri analiz ederek ve BT güvenlik politikaları tarafından belirlenen kuralları temel alarak, geçişlere izin verilmesini veya engellenmesini isteyip istemediklerini belirleyerek gelen ve giden veri trafiğini kontrol eden ağ güvenlik sistemi olarak tanımlamaktadır (s. 69). Güvenlik duvarları ağ güvenliğinde genellikle birinci sırada yer alır ve aynı zamanda saldırı tespit sistemleri (IDS-Intrusion Detection Systems) ile de sıkı işbirliği içerisinde çalışır. ADSReports (Kasım 2012)'un tahminlerine göre, küresel

kurumsal güvenlik duvarı pazarının % 11,1 oranında artarak (yıllık büyüme) beş yıl içinde 34,7 milyar dolarlık bir rakama ulaşması öngörülmektedir.

2.5.3 Sosyal Ağlarda Güvenlik (*Security in Social Networks*)

Sosyal ağların popülaritesi şu anda çok yüksek ve internet erişimi olan hemen herkesin en az bir hesabı bulunmaktadır. İnsanlar, bu ağlardaki kişisel bilgileri, arkasındaki kuruluşun verileriyle ne yapacağı konusunda endişelenmeden paylaşmaktadır. Bu veriler, Büyük Veri'nin güçlü analiz yeteneği ile birlikte, kişisel gizliliğimize büyük bir tehdit oluşturmaktadır. Bu gerçek, birçok hükümetin verilerin korunması ve gizliliği ile ilgili mevzuat hakkında endişelenmeye başlamasına neden olmaktadır (Zhao, Chellappa, Phillips ve Rosenfeld, 2003 Akt: Moreno, Serrano ve Fernández-Medina, 2018, s. 155).

Ana kaynağından (yani kişinin kendisinden, birinci elden) dağıtılan ve bu yüzden de doğruluğundan dolayı kıymetli olan her türlü bilgi sosyal ağlar ve internet üzerinde kontrolsüzce dolaşıma sokulmakta, güvenli olmayan ya da sahte (ikiz) sitelerden alış verişi yapılabilmekte, çekilen fotoğraflar (farkında olmadan GPS konum bilgisi de fotoğraflarla birlikte) paylaşmakta, kredi kartı/banka hesapları/kimlik bilgileri sms/e-posta vb. aracılığıyla dağıtılmakta, çift faktörlü doğrulama yapılmadan birçok işlem gerçekleştirilmektedir. Tüm bu işlemler kişi ya da kurumların SM saldırılarına uğramalarına ve bilgi güvenliklerini tehlikeye atmalarına sebebiyet verebilmektedir. Mümkün olduğunca bu işlemlerde azami dikkat gösterilmesi, kredi kartı yerine sanal kredi kartlarının (limit ve süre kısıtlı) kullanılması, katmanlı doğrulama araçlarının kullanılması, kırılması zor olan uzun ve karmaşık parolaların kullanılması, geride iz bırakmamak için daha güvenli olduğu düşünülen (?) VPN (Virtual Private Network: Sanal Özel Ağ) kullanılması gibi önlemler alınabilir.

2.5.4 Uç/Son Nokta Kullanıcı Güvenliği (*Endpoint Security*)

Uç/Son nokta kullanıcı güvenliği genel olarak şu alt başlıklar altında incelenmektedir (Pesen, 2015);

- Uç/Son nokta kullanıcı savunması (*endpoint defense*); anti malware, ana bilgisayar güvenlik duvarı (host firewall), ana bilgisayar tabanlı saldırı önleme sistemi (HIPS), uygulamalar için beyaz listeleme (application whitelisting)

- Disk Şifreleme (*Disk Encryption*)
- Cihaz Kontrolü (*Device Control*)
- Mobil Güvenlik (*Mobile Security*)
- Uzaktan Erişim / VPN (*Remote Access / VPN: Virtual Private Network*)

2.5.5 Veri Güvenliği (*Data Security*)

Veri, işlenmiş bilgilere verilen addır. Veri sayı, sembol, harf gibi ifadelerden oluşmakta ve tek başına bir anlam ifade etmemektedir (Ok, 2013, s. 20). Verilerin anlam kazanabilmesi için (yorumlanarak) enformasyona, enformasyonun da (işlenerek) bilgiye dönüşmesi gerekmektedir.

Her ne şekilde olursa olsun, öğrendiklerini kullanabilmek için öncelikle öğrenmek ve öğrenmenin olabilmesi için verilerin elde edilmesi, saklanması ve işlenmesi gereklidir. Dolayısıyla, her şeyin temelinde veri ve veri yönetimi bulunmaktadır (Yenisey, 2010, s. 138). Bu nedenle veri yönetiminin amacına uygun olarak icra edilebilmesi için veri güvenliğinin birinci derecede önemsenmesi ve ele alınması gerekli, hatta kaçınılmazdır. Tüm yapı, veri ve veri güvenliği üzerine kurulduğundan, veri güvenliği iyi planlanması ve yönetilmesi gereken bir süreçtir.

Son birkaç yılda, veriler neredeyse her alandaki kuruluşlar için en önemli varlıklar haline gelmiştir. Sadece bilgisayar bilimi endüstrisi alanıyla ilgili şirketler için değil aynı zamanda hükümetler, sağlık hizmetleri, eğitim veya mühendislik sektörü gibi kuruluşlar için de önemlidir. Hepsi için, veriler günlük faaliyetlerini yürütmek adına gereklidir ve yalnızca veriler değil, işletme yönetimlerinin hedeflerine ulaşmalarında ve elde edilen bilgiler temelinde en iyi kararları vermede yardımcı olabilmektedir (Zhao, Chellappa, Phillips ve Rosenfeld, 2003 Akt: Moreno, Serrano ve Fernández-Medina, 2018, s. 149).

Veri gizliliği muhtemelen sıradan insanların en çok endişe duyduğu konudur, ancak *büyük veri* tekniklerini kullanan kuruluşlar için de en büyük kaygılardan biri olmalıdır. Zira, *büyük veri sistemi* genellikle kuruluşların bu verilerden yararlanmak için kullandığı çok büyük miktarda kişisel bilgiler içermektedir. Dolayısıyla, kendimize bu bilgilerin kullanımına ilişkin sınırın nerede olduğunu sormak durumundayız (Zhao, Chellappa, Phillips ve Rosenfeld, 2003 Akt: Moreno, Serrano ve Fernández-Medina, 2018, s. 155). Veri güvenliği yanında daha yeni bir kavram olan veri yönetimi de gün geçtikçe daha önemli hale gelmektedir. Özellikle kişisel ve

kurumsal tüm veri (ve bilgi) kaynaklarının ağ, internet, mobil iletişim, büyük veri ve bulut sistemleri üzerinde gerçekleşmeye başladığı günümüzde bu durum daha da önemli bir hal almaktadır.

Veri toplama ve değerlendirme süreci, seçilen organizasyonun yapısı ve büyüklüğüne bağlı olarak planlanmalıdır. Bu süreçte alınacak her veri daha sonraki sonuçlara temel oluşturacağı için geriye dönük izlemeye izin verecek yapıda tasarlanmalıdır. Sonuçların kurum içerisinde paylaşımı sonrası kabul görmesi, iyileştirme hareketlerini başlatabilmesi açısından güvenilirliği yüksek bir grup tarafından ele alınması; bu tip proje ekibine üst yönetim desteğinin sağlanması unsurlarına da dikkat edilmelidir. (...) Bilgi yönetimi, sonuç olarak teknoloji kadar kültürel ve kişisel boyutları ile de dikkat çeken bir yapıyı tanıttığı için süreç içindeki kritik tüm kişilerle görüşülmesi ve destekleyici verilerin somut olarak edinilmesine özen gösterilmelidir (Köksaldı, Polat, Meydanlı ve Duman, 2010, s. 226). Veri yönetimi ise, bir işletmenin bilgi yaşam döngüsü ihtiyaçlarını etkin bir şekilde yönetmek için mimarinin, politikaların, uygulamaların ve prosedürlerin geliştirilmesi ve yürütülmesidir. Veri yönetimi, kendi başına önemli bir konudur ve bir şirketin yönetimi için kritik öneme sahiptir. (...) Veri yönetiminin temel bir özelliği de, verilerin yalnızca toplandığı değil aynı zamanda doğru olduğu güvencesinin verildiği usule ilişkin yöntemdir (Data Management, 2019).

2.5.6 Uygulama Güvenliği (*Application Security*)

Cihazlara indirilen ve kurulan yazılımlar (programlar, uygulamalar, aplikasyonlar vb.) eğer belirli güvenlik kontrolü aşamalarından geçirilmezlerse güvenlik açığına sebebiyet verebilir hatta kendileri direk tehdit unsuru olabilir. Bu nedenle özellikle cep telefonlarına Windows, IOS veya Android işletim sistemlerine sahip platformlar üzerinde çalışacak uygulamaların güvenliği için çeşitli katmanlardan oluşan güvenlik önlemleri bulundurulmaktadır. Bu platformlarda yer alan uygulamaların geliştiricileri çeşitli kimlik doğrulamaları ile önceden belirlenir, geliştirdikleri uygulamalarda zararlı içerik (kod) bulunup bulunmadığı test edilir (verify app vb. araçlarla), yükleme aşamasında ise yüklenen cihazda hangi alanlara erişim sağlayacağı belirtilir ve kişi uygun seçimleri yaparak kurulumu devam eder. Diğer taraftan cihazlarda kurulu olan uygulamaların her türlü isteğine erişim imkânı vermemek, *root* erişim korumasının kaldırılmaması, menşei belirli olmayan

üçüncü parti yazılımlardan sakınma gibi kullanıcının alabileceği basit ama etkili önlemler de mevcuttur.

2.5.7 Kimlik ve Erişim Yönetimi (*Identity and Access Management*)

Erişim kontrolü ve kimlik doğrulama bilgi sistemlerinde güvenliğin sağlanması için kaynaklara erişimi ve yetkilendirmeyi düzenler. Kişilerin kaynaklardan hangilerine ve hangi yetki düzeyinde erişim sağlayabileceğini belirler. Bu işlemler erişim matrisi, erişim kontrol listeleri ve rol belirleme gibi listeler aracılığıyla yapılır. (...) Erişim kontrolleri isteğe bağlı, rol tabanlı veya zorunlu erişim yöntemlerinden birisi ile belirlenebilir. Bu erişim kontrolleri önleyici ya da algılayıcı olabilmektedir (Kara, 2018, s. 70).

2.5.8 Sanallaştırma ve Bulut (*Virtualization and Cloud*)

Teknoloji değiştikçe güvenlik kapsamı da değişmektedir. Bilişim, ana bilgisayarlardan, PC'lere ve mobil cihazlara, Bulut ve Nesnelerin İnterneti'ne doğru geliştiğinden, hepsinin bir şekilde güvenliğinin sağlanması gerekmektedir. (...) Ayrıca bilinen tehditlerin yanı sıra, yeni teknolojiler yeni tehdit boyutları eklemektedir. Örneğin, büyük ölçekli veri sızıntısı veya hırsızlığı tehdidi, ya da *bulut bilişim* ile ilgili olup daha önceki teknoloji biçimlerine uygulanmayan saldırı tipleri gibi (Furnell, 2018, s. 32).

Bulut hizmetleri kullanıcılarının verilerini depolamak ve işlemek için kullanabilecekleri çok sayıda kaynak ve hizmet havuzu sunmaktadır. Kullanıcılar işletme giderlerini esnek bir şekilde kontrol edip azaltabilmekle beraber, buluttaki kullanıcı/müşteri verilerini hedefleyen saldırılarla ilişkili tehditleri, beklenmeyen ve pahalı maliyetleri göz önünde bulundurması gerekmektedir (Kumar, Chaisiri ve Ko, 2017, s. 1). Bulut bilişim sistemlerine hizmet sunma açısından bakıldığında oldukça mantıklı ve ekonomik gözüküyor olsalar da verilerin, bilgilerin uzakta (şirket dışında) olması, kontrolün de dışarıda olması anlamına gelmektedir. Birçok güvenlik önlemi ve taahhüt olsa da bu verilere kimlerin eriştiği ya da erişebiliyor olduğundan emin olmak tam olarak mümkün değildir. Diğer taraftan, bulut hizmet sağlayıcıları bir şekilde zarar görürse (doğal afetler, siber saldırılar, fiziksel saldırılar veya ekonomik iflaslar vb.), ilgili şirketler de bundan direkt zarar görebileceklerdir. (...) Bulut hizmetine geçilirken riskler ve fırsatlar etkin bir şekilde değerlendirilmeli ve ona göre karar verilmeli, uygun bulut servisi seçilmelidir (Kara, 2018, s. 108). Bulut

bilişim servis modellerinden daha çok altyapı servisi olarak bilinen IaaS bulut modeli diğerlerine göre daha esnek, güvenli ve hizmet alan şirket için daha fazla kontrol anlamına gelmektedir; güvenli bir fiziksel ortamda yedeklemeli, yangın korunaklı, yedek enerji sistemli kabinet sistemleri şeklinde hizmet sunumu verilir. Şirketler bu alanlara kendi sunucularını yerleştirerek onu istedikleri gibi yönetebilirler.

Bulut bilgi işlem, bilgi işlem kaynaklarına (bilgisayarlar, depolama cihazları, uygulamalar ve hizmetler) ağ üzerinden ulaşılmasını sağlayan bilgi işlem (ve erişim) modelini ifade etmektedir. Bu bilgi işlem kaynakları *bulutu*'na bağlanabilen herhangi bir cihaz veya konumdan ihtiyaca bağlı olarak giriş yapıp erişim sağlanabilir (Laudon ve Laudon, 2011, s. 170). *Bulut* burada bahsedilen bilgi işlem kaynaklarına genellikle internet üzerinden sanal ortamda yer ve zamandan bağımsız olarak erişimi ifade etmektedir. Hızlı ve esnek kaynak havuzu olarak da tanımlanabilir.

Sanallaştırma, fiziksel yapılandırmanın veya coğrafi konumlandırmanın sınırlarının olmadığı, tamamen ve her an erişilebilen bir dizi işlem kaynaklarını (sunucu ve depolama, yedekleme üniteleri gibi) hizmet olarak sunma işlemidir. Bir sunucu, üzerinde yer alacak sanal işletim sistemleri sayesinde, kullanıcıya birden fazla kaynakmış gibi hizmet verebilmektedir. Örneğin, aynı sunucu üzerinde Windows, Linux ve macOS işletim sistemleri hizmet verebilir (VMware uygulaması bunlardan biridir). Sanallaştırma bir işletmenin bilgi işlem ve depolama işlemleri için uzak noktalardaki bilgi işlem kaynaklarına da ev sahipliği hizmeti verebilir (Laudon ve Laudon, 2011, s. 182).

2.5.9 İki Faktörlü Kimlik Doğrulama (*Two-Factor Authentication - 2FA*)

Bazen iki aşamalı doğrulama veya çift faktörlü doğrulama olarak da adlandırılan iki faktörlü kimlik doğrulama (2FA), kullanıcının hem kullanıcı bilgilerini hem de kullanıcının kaynaklarını daha iyi koruyabilmelerini sağlamak için ve kendilerini doğrulamak için kullanılan bir güvenlik erişim sürecidir. İki faktörlü kimlik doğrulama, kullanıcının yalnızca bir faktör ile sağladığı kimlik doğrulamasına bağlı olan (genellikle bu bir paroladır) kimlik doğrulama yöntemlerinden daha yüksek düzeyde bir güvence sağlaması için kullanılmaktadır. İki faktörlü kimlik doğrulama yöntemleri, ikinci bir faktörün yanı sıra genellikle bir güvenlik belirteci, cep telefonu mesajı, parmak izi veya yüz taraması gibi bir biyometrik faktör de olabilir (Rouse, 2018b). Kullanıcı ve veri güvenliğini bir miktar daha arttırmak için

belirli bir süredir kullanılmakta olan 2FA, tam bir güvenlik sağlamasa da ikinci bir güvenlik katmanı içermesi açısından oldukça önemli ve gereklidir. Örneğin; kredi kartı ile alışverişlerde parola girilerek yapılan işlemlerden sonra onayın gerçekleşmesi için cep telefonlarına gelen ve bir defaya mahsus kullanılmak üzere üretilen doğrulama kodu en basit düzeyde de olsa bir 2FA kullanımıdır. Gerek SM uygulamaları gerek hackleme yöntemleriyle olsun kimlik hırsızlığı ve parolaları ele geçirmek (kişisel dikkat ve özen göstermemekten de kaynaklı) oldukça kolay bir hale gelmiştir. Bu tür ataklardan korunabilmek için 2FA'nın hangi kombinasyonu olursa olsun güvenlik duvarını bir kademe daha güçlendirmektedir. Rouse (2018b) 2FA kimlik doğrulama için sırasıyla en çok şu katmanların kullanıldığını ifade etmektedir;

- *Bilgi Faktörü*: Kullanıcının şifre, PIN veya başka türden sahip olduğu bir veri ya da bilgidir.
- *Sahip Olma Faktörü*: Kullanıcının kimlik kartı, güvenlik belirteci, akıllı telefon veya başka bir mobil cihaz gibi sahip olduğu bir şeydir.
- *Özgü Olma Faktörü*: Daha yaygın olarak biyometrik bir faktör olarak adlandırılan bir doğallık faktörü, kullanıcının fiziksel benliğinde doğal olan bir şeydir. Bunlar, bir parmak izi okuyucusunda doğrulanan parmak izleri gibi fiziksel özelliklerden eşleşen kişisel özellikler olabilir; yaygın olarak kullanılan diğer özgü faktörleri ise yüz ve ses tanıma olabilir. Ayrıca, tuş vuruş dinamikleri, yürüyüş veya konuşma düzenleri gibi davranışsal biyometrilere de içerebilmektedir.
- *Konum Faktörü*: Kimlik doğrulama girişimlerinin belirli bir konumdaki belirli cihazlarla sınırlandırılması veya daha genel olarak kaynak IP'ye dayalı bir kimlik doğrulama girişiminin coğrafi kaynağının izlenmesiyle uygulanabilmektedir. Ayrıca, kullanıcının cep telefonundan veya GPS verisi gibi başka bir cihazdan türetilmiş başka bir coğrafi konum bilgisi de olabilmektedir.
- *Zaman Faktörü*: Kullanıcı kimlik doğrulamasını, oturum açmaya izin verilen belirli bir zaman penceresinde gerçekleştirir.

Tüm bu araçların yanı sıra ikinci faktör olarak RFID, NFC, akıllı kartlar, dijital jetonlar da kullanılabilir. Günlük kullanımlarda 2FA uygulamaları

veri/işlem güvenliği açısından büyük oranda işleri kolaylaştırmaktadır. Bazı uygulamalarda (yüksek hassasiyetli veri içerikli işlemlerde) ise yukarıda bahsedilen 2FA faktörleri üçlü faktör setleri olarak da kullanılmaktadır.

2.5.10 Fiziksel Güvenlik (*Physical Security*)

Fiziksel güvenlik; yangın, su basması, deprem ve benzeri doğal afetlere karşı bilgi sistemlerini korumaya yönelik olarak alınan tedbirleri kapsamaktadır. Bunun yanı sıra yetkisiz kişilerin izinleri olmadıkları bir alana ya da bir makineye, cihaza, bilgiye erişimlerini engelleyecek çevre düzeneklerinin yapılandırılması söz konusudur. Fiziksel güvenliğin sağlanacağı öncelikli ortamlar; kurum binası ve çevresi, sunucu ve sunucu odaları ve ilgili çalışma alanlarını kapsamaktadır (Yiğitbaşı, 2015, s. 62). BG için SM'de olduğu gibi önem arz eden fiziki ortamlara erişimin koruma altına alınarak kontrollü ve kısıtlı erişimlerin sağlanması gerekmektedir. Fiziksel güvenliğin istenilen düzeyde sağlanabilmesi için fiziksel kontrol ve iyileştirme işlemlerinin de periyodik olarak yerine getirilmesi gerekmektedir. Kara (2018, s. 41) fiziksel kontrolü şu şekilde tanımlamaktadır: Fiziksel kontrol şirketin ve binanın fiziksel güvenliği ile ilgilidir. Kapıların kilitli tutulması, sunucuların ve ağ cihazlarının fiziksel olarak güvenli bir ortamda bulundurulması, kabloların korunması (harici girişlere karşı sürekli kontrollerinin yapılması), görevlerin ayrılması ve yedekleme işlemlerinin uygun şekilde ve düzenli aralıklarla icra edilmesi fiziksel kontrol olarak ele alınabilir.

Kritik önem arz eden bölgelere yetkisiz erişimlerin engellenmesi ve bilgi kaynaklarının yetkisiz kişilere karşı korunması adına alınan önlemler bütünü (Altınkaynak, 2018, s. 251) olarak değerlendirebileceğimiz fiziksel güvenlik için; bilginin korunması sürecinde korumalı binalar, kamera ve benzeri teknik ekipmanlar, biyometrik kontrollü geçişler, güvenlik görevlileri, sağır odalar, tempest¹⁰ korumalar vb. donanımlarla sağlanmaktadır. Altınkaynak (2018) güvenli bölgelerin oluşturulabilmesi adına genel tedbirler olarak aşağıda belirtilen güvenlik önlemlerinin alınabileceğini belirtmektedir:

- *Giriş Güvenliği*: Kritik alanlara sadece yetkilendirilmiş kişilerin giriş-çıkışını sağlamak üzere kontrol mekanizmalarının kurulması ve mümkünse NFC, RFID

¹⁰ TEMPEST: Telecommunications Electronics Material Protected from Emanating Spurious Transmissions (Elektromanyetik dinleme ve bu dinlemelerden korunma yöntemlerine verilen genel isim)

gibi kontrollerden kaçınılarak kopyalanması daha güç olan kimlik doğrulama yöntemlerinden (mümkünse çoklu katmanlardan oluşan) yararlanılmalıdır. Tüm giriş-çıkışların düzenli olarak kayıt altına alınması ve detaylı bir şekilde tutulması ve arşivlenmesi gereklidir.

- *Oda Güvenliği*: Kritik alanlara ait yönlendirici ve bilgilendirici işaretlerin kullanılmaması gerekmektedir. Kozmik bilgiler içeren odalar için ise tempest standartlarının korunması ve düzenli aralıklarla kontrol edilmesi gerekmektedir.
- *Afet Güvenliği*: Afet, acil durum ve olağan üstü haller için sistem ve sunucu yedeklerinin başka bir mekânda (başka şehir ve hatta başka ülke olabilir) mümkünse anlık, mümkün değilse düzenli aralıklarla yedeklenmesi gerekmektedir. Bu önlem özellikle büyük çaplı siber saldırılar için oldukça önem arz etmektedir.
- *Erişim Güvenliği*: Kritik alanlarda ve görevlerde çalışan personelin ilgili alanlara girişlerinde kayıt/görüntü vs. sağlayan cihazlarla girişlerine izin verilmemelidir. Sistem yöneticileri de dâhil bilginin açık halde görülmemesi sağlanmalıdır.
- *Ekipman Güvenliği*: Programlanabilir USB cihazlar, NFC ve RFID'li cihazlar, Hub'lar, Switch'lerin güvenlikleri sağlanmalıdır. Örneğin; kritik bilgi içeren bilgisayarların USB bağlantı portları (yuvaları) kaldırılabilir/iptal edilebilir.

Yukarıdaki başlıklara ek olarak güç sistemlerinden kaynaklanan bazı açıklar da başa çıkmak ve önlem almak gerekmektedir. Bunlar genellikle elektromanyetik dalgalanmalar (Elektro Manyetik Parazit - Electro Magnetics Interference [EMI] ve Radyo Frekans Paraziti - Radio Frequency Interference [RFI]) ile voltaj farklılıklarından meydana gelmektedir. EMI/RFI sebebiyle oluşan manyetik dalgalanmalardan dolayı dışarı bilgi kaçmasını engellemek için TEMPEST (Transient Electromagnetic Pulse Emanation Standards) standartları, voltaj farklılıklarına karşı önlem almak için ise ANSI (American National Standards Institute - Amerikan Ulusal Standartlar Enstitüsü) standartlarının uygulanması uygun olacaktır.

Fiziksel güvenlikle ilişkilendirilebilecek diğer bir konu ise kullanılmakta olan bilgi sistem cihazlarının işlerini gerektiği gibi yapıp yapmadıklarını yani güvenilir ve güncel oldukları konusunda uluslararası standartlara göre testlerinin gerçekleştirilmesi ve sertifikalandırılması oldukça faydalıdır.

2.5.11 Personel Güvenliği (*Personnel Security*)

BG'nin en önemli (ayrılmaz) parçalarından birisi personel güvenliğinin sağlanmasıdır. Bir kurumda ne kadar teknolojik güvenlik kontrolleri bulunursa bulunsun (SM bölümüne sıkça ifade edildiği üzere) herhangi bir sistemin en zayıf halkasının insan olduğu unutulmamalıdır. Bu yüzden BG'de personel güvenliğinin yer alması hayati önem taşımaktadır (Yiğitbaşı, 2015, s. 63-64). Yiğitbaşı (2015) yine personel güvenliği için alınacak önlemler açısından şu çalışmaların yapılması gerektiğini ifade etmektedir:

- İşe alımlarda personel özgeçmişi araştırmasının itina ile yapılması gereklidir (sabıka kaydı, kredibilitesi, sürücü geçmişi, referans kişiler vb.).
- İşe alımlarda kurumsal bilgi güvenliğine hanel gelmemesi için kurumsal bilgi güvenliği konularını içeren çeşitli gizlilik sözleşmeleri yapılabilir.
- Çalışanların şüpheli hareketleri izlenmeli ve rapor edilmelidir. Bunlar içerisinde internet veri trafiğinin izlenmesi, log kayıtlarına bakılması, ihtiyaç halinde telefon görüşmelerinin yasal yollarla takibi gibi konular yer almaktadır.
- Tatil ve izin zamanlarında kurumda göreve devam edenlerin kurum içi hareketlerinin izlenmesi gerekir.
- İşten ayrılma işlemleri yerine getirilirken dostça yaklaşma ve gizlilik sözleşmelerinin hatırlatılması gereklidir.

Ayrıca işten ayrılan kişiye tanımlanmış tüm erişimler (parola, tanımlı kimlik kartları, roller, fiziki geçişler, biyometrik geçişler vb.) kullanım dışı bırakılmalı, çalışanlar ve iş ortaklarına bu kişinin işten ayrıldığı bilgisi en kısa süre içerisinde iletilmelidir.

Erişim yönetimi başlığı altında ele alabileceğimiz diğer bir konu ise personel (sınırlı düzeyde erişim: klerans) yetki sınırlamasıdır. Özellikle bilgisayar programı kullanımında kullanıcının yetki tanımlarının doğru ve ölçülü yapılması

gerekmektedir. Gerektiği kadar erişimin üzerinde fazladan bir erişim hakkının tanımlanması BG'nin sağlanması açısından çeşitli olumsuzluklar doğurabilmektedir. Kara (2018) erişim haklarıyla ilgili olarak şu bilgilerin önemine dikkat çekmektedir: Örneğin, kullanıcının görevini yerine getirebilmesi için sadece (bilgiyi) okuması yeterli ise kullanıcıya ayrıca silme hakkının verilmemesi gerekmektedir. Gereğinden fazla erişim hakkı tanımanın bilginin kontrolsüz olarak yayılma riskini de beraberinde getirecektir. Bu tür standart bir uygulamanın hassas bilgi varlıkları ve bunları destekleyen bilgi teknolojileri kaynaklarının teşhir edilmesini sınırlandırmış olmakla birlikte, içerik ve alıcıları açısından duyarlı bilgi varlıklarının erişimi, değiştirilmesi veya dağıtımı üzerinde uygun kontrolleri sağlayacak bir yönetim yapısı sağlanmış ve böylece hassas bilgiye erişim veya bilginin dağıtımı sonucunda oluşabilecek zararlar en aza indirgenmiş olacaktır (s. 43).

2.5.12 Siber Saldırlara Karşı Güvenlik (*Security Against Cyber Attacks*)

Bilgisayar güvenliği veya BT güvenliği olarak da bilinen siber güvenlik, genellikle bilgisayar sistemlerinin hırsızlığa karşı korunması veya donanım, yazılım veya bilgilerin zarar görmesini engellemek için sağlanan hizmetlerin aksamadan devam ettirilmesi anlamında gelir (Singer ve Friedman, 2014 Akt: İslam, 2018, s. 216). Saldırganların kullandıkları PowerShell, VBS, VBA, Python, C# script ve Macro scriptler, RAT (Remote Access Trojans - Uzaktan Erişimli Truva Atı) ve diğer araçlara dair analizler düzenli olarak takip edilerek kurumsal bilgi güvenliğiyle ilgili birimlerce güncel önlemler alınmalıdır.

Ortaya çıkan bilgisayar ve bilgi teknolojisi uygulamaları ile birlikte, siber suç tüm dünyada önemli bir sorun haline gelmiştir. Her gün binlerce siber suçlu, internet üzerinden yasa dışı yollardan erişim sağlamak için bilgisayar sistemlerine saldırmaktadır. Her ay yüzlerce yeni bilgisayar virüsü ve spam, bilgisayar sistemlerine zarar vermek veya veri çalmak ya da yok etmek amacıyla yayılmaktadır (İslam, 2018, s. 215). Bu tür saldırılara karşı önlemler siber güvenlik çatısı altında ele alınmaktadır. Siber güvenlik; ağları, bilgisayarları, programları, verileri ve güvenlik açıklarını, saldırılar veya internet üzerinden siber suçlular tarafından yetkisiz erişime karşı korumak için tasarlanmış teknolojiler, işlemler ve uygulamalar anlamına gelmektedir (Lee, 2015 Akt: İslam, 2018, s. 216). Son zamanlarda siber saldırılarda kullanılan popüler yöntemlerden biri *fidyecilik* (ransomeware)

saldırılarıdır. Bilgisayarlara zararlı yazılımları bulaştırarak bilgileri şifreleyen yazılımlara *fidye yazılımlar* denmektedir. Bu atak türünde saldırganlar bilgisayardaki yazılım açıkları, e-posta ekinde gönderilen zararlı dosyalar ya da internetteki zararlı link gibi yöntemlerle kullanıcının bilgisayarına sızıp, kendi zararlı yazılımlarını kurbanın bilgisayarına kurarak bilgisayardaki tüm verileri şifreleyip, bilgisayarı kullanılamayacak hale getirmekte ve yeniden kullanılabilir hale gelebilmesi için kurbandan fidye ödemesi talep edilmektedir. İstenilen fidye şirketin büyüklüğü, prestiji, şifrelenen veri miktarı ve verinin niteliğine göre değişiklik gösterebilmektedir. Fidye için istenen ücretler 300 Amerikan dolarından başlamaktadır. 2017 yılında UBER'in dünya çapında 57 milyon müşterisine ait veriler çalınarak fidye istendi ve UBER şirketi fidye olarak 100 bin Amerikan doları ödemek zorunda kaldı (Kara, 2018, s. 149). Fidye saldırılarında diğer bir sorun; istenilen fidye miktarı ödense dahi, ekstradan ya da daha fazla miktarda bir paranın yeniden talep edilebileceği veya aynı bilgisayarlara (gerekli önlemler alınmaz ise) yeniden fidye saldırılarının düzenlenebileceğidir. *Fidye yazılım* satışı ve fidye için talep edilen paraların *bitcoin* gibi elektronik paralar üzerinden yapıldığında suçluların izlenmesi ve tespitleri ise oldukça zordur. Önlem olarak Siber Olaylara Müdahale Ekibi (SOME) kurulması bu tür olaylarda etkin izlemeler yapılabilmesi için kritik öneme sahiptir (Kara, 2018, s. 151). SOME ile ilgili detaylı bilgi (2.6.5) başlığı altında anlatılmıştır.

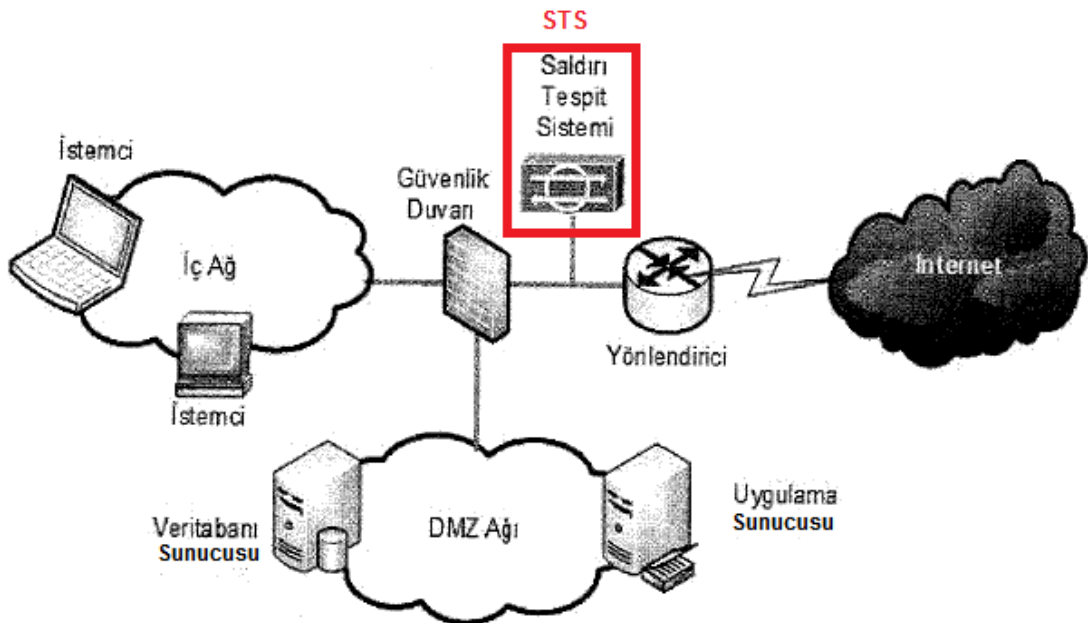
2.5.12.1 Bilgi Güvenliği Yönetim Sistemleri (*Information Security Management Systems - ISMS*)

Bilgi Güvenliği Yönetim Sistemleri (information security management systems - ISMS), hassas şirket bilgilerinin güvenli kalması için yönetilmesine yönelik sistematik bir yaklaşımdır. Bir risk yönetimi süreci uygulayarak insanları, süreçleri ve BT sistemlerini içerir. Herhangi bir sektördeki küçük, orta ve büyük işletmelerin bilgi varlıklarını güvende tutmalarına yardımcı olur (<https://www.iso.org/isoiec-27001-information-security.html>).

2.5.12.2 Saldırı Tespit/Önleme Sistemleri (*Intrusion Dedection System - IDS, Intrusion Prevention System - IPS*)

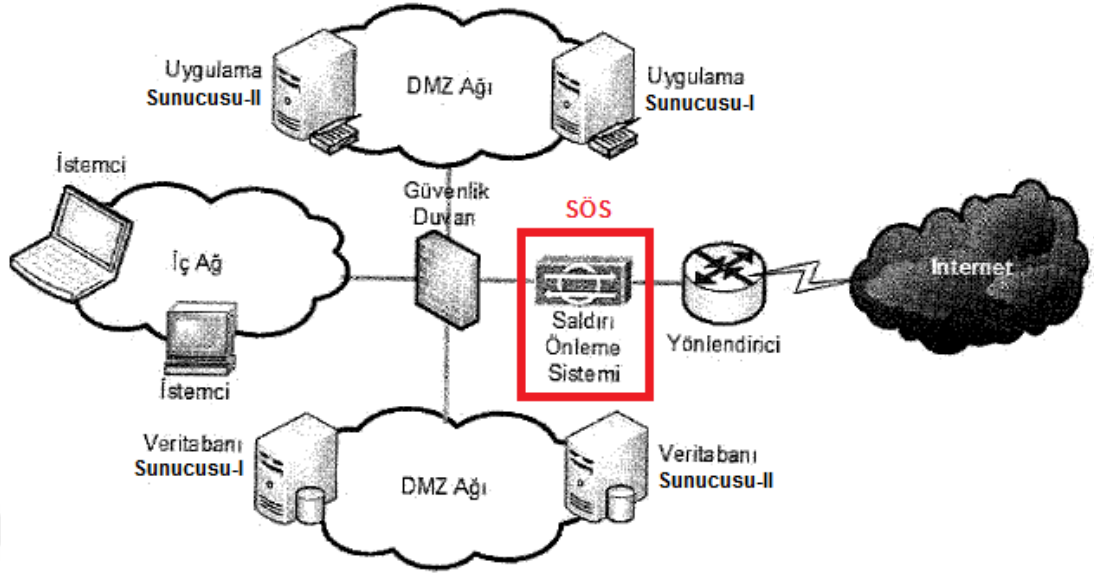
Saldırı Tespit/Önleme Sistemi (STS/SÖS) bilgi sistemlerinin güvenlik politikalarına uygun olmayan saldırıları ya da kötü niyetli erişim girişimlerini tespiti yarayan sistemlerdir (Kara, 2018, s. 204-205). STS'nin ağı önüne konularak atakları tespit eden ağ tabanlı (network based) türü ve sunucuların (server) üzerine kurularak atakları tespit eden sunucu tabanlı (host based) türü bulunmaktadır. Saldırıyı tespit etme yanında saldırıyı önleme yetenekleri de bulunan SÖS sistemleri daha çok tercih edilmektedir. SÖS'ler dışarıdan gelen atakları tespit etmenin yanı sıra içeriden (yerel ağlardan) gelebilecek saldırılara karşı da kullanılmaktadır. Saldırı, ağda bulunan sunucu(lar) tarafından yapılıyorsa saldırı SÖS'e ulaşmayacağı için tespit edilemez. Bu güvenlik açığını ortadan kaldırmak için sunucu tabanlı SÖS kullanmak gerekmektedir. STS ve SÖS'ler ağı çeşitli yerlerinde konumlandırılabilir. Bu karar şirketin yapısı, talebi, ihtiyacı ve ağ tipolojilerine göre değişebilmektedir. Şekil 24 ve Şekil 25'de STS ve SÖS'lerin ağda yaygın kullanım yerleri belirtilmiştir. Bu şekillerde yer alan DMZ (*Demilitarized Zone*); iç ağ (local area network) ile dış dünyayı birbirinden ayıran açık/sivil bölgeyi ifade etmektedir. DMZ, güvenlik katmanlarından biri olarak düşünülebilir.

Şekil 24. STS'nin Ağda Konumlandırılması



Kaynak: Kara, 2018, s. 205

Şekil 25. SÖS'ün Ağda Konumlandırılması



Kaynak: Kara, 2018, s. 206

2.5.13 Felaketten Kurtarma (Disaster Recovery)

İş sürekliliği ve BG açısından felaketten kurtarma çalışma ve planlamalarında aşağıdaki konuların her ne kadar BG uzmanı tarafından bilinmesi ve uygulanması gerekiyorsa da, yönetim tarafından da bilinmesi ve izlenmesi işletme sürekliliği ve güvenliği açısından gereklidir. Kara (2018, s. 244) “Kurumsal Bilgi Güvenliği” isimli çalışmasında bu konuları şu başlıklara ayırmaktadır:

- İş sürekliliği planı ve felaketten kurtarma planı
- Doğal kaynaklı ve insan kaynaklı felaketlerin farkı
- İş etki analizi aşamaları
- Felaketten kurtarım planının adımları
- Felaketten kurtarım planı testlerinin tipleri
- Yedekleme servisleri

İş sürekliliği planı ve felaketten kurtarma planı, bir organizasyonda büyük bir yıkımla karşı karşıya kalındığında normal (stabil) duruma (en kısa süre içerisinde) geri dönebilmek için yapılması gerekenlerdir. Bu plan; doğal ve insan kaynaklı yıkıcı etkileri, ağ problemlerini, enerji, iletişim ve bunlarla ilgili kesintileri, güncellemeleri, test ve ilgili hazırlıkları içerir. İş sürekliliği planı kritik bilgi işleme alanlarının

(LAN, WAN haberleşme altyapıları, ağ cihazları, kullanıcı bilgisayarları, yazılımlar, veriler, saklama ortamları ve üretim süreçleri) tamamına bakmalıdır. Güvenlik olayları doğal kaynaklı ve insan kaynaklı olmak üzere ikiye ayrılmaktadır. Bunlardan doğal kaynaklı olanlar; yangın, sel, su taşkınları, deprem, elektrik kesintileri vb., insan kaynaklı olanlar ise; sabotaj, saldırılar, grev, işini gerektiği gibi yapmama, görev başında bulunmama, bilinçli ya da bilinçsiz olarak iş yerine, makinelere ve iş süreçlerine verilen zararlar vb. İş etki analizi ise, iş birimlerinin, aksamaya sebebiyet veren olayın etkisini anlamaya yönelik çalışmalarını içerir. Bir işle ilgili felaket ya da kesintiler meydana geldiğinde bunun etkisinin ne olacağının anlaşılmasını sağlayacak bir belgenin ortaya konulmasıdır. Bu etki mali veya işlevsel olabilir. Felaketten kurtarma planı, vuku bulan olumsuz bir duruma çözüm üretebilmek için olayın gerçekleştiği ve devam ettiği süre boyunca uygulanacak çeşitli prosedürlerin uygulanması, destek, kurtarma ve koruma işlemlerini kapsamaktadır. Özellikle kritik iş süreçlerinin en az kesintiyle hizmete devam edebilmesini sağlamak önemlidir. Felaketten kurtarma plan türleri içerisinde kontrol listelerinin hazırlanması, yapısal incelemeler, simülasyon ve derinliğine inceleme, fonksiyonel derinlik ve paralel testler ve tam uygulama gibi girişimler bulunmaktadır (Kara, 2018, s. 244).

Yedekleme servisleri, iş sürekliliği ve felaketten kurtarma konuları içerisinde en önemli alanlardan birisini oluşturmaktadır. Özellikle bilişim alanında işletmeye ait veriler (kuruma ait veriler, müşterilere ilişkin veriler, satışlar, faturalar, raporlar, bilançolar vb.) sayısal ortamlarda (bilgisayar ve yedekleme araçlarında) tutulduğu ve ağ üzerinden kullanıldığı, sürekli güncellendiği için işletmenin varlık değerlerinin önemli bir kısmını oluşturmaktadır. Bu nedenlerle verilerin (kısa aralıklarla ve mümkünse eş zamanlı olarak) ikinci, üçüncü yedeklerinin tutulması gerekmektedir. Bu yedekler aynı şehir içinde başka bir bölgede, farklı şehirlerde hatta farklı ülkelerde olabilir.

2.6 Hukuksal Düzenleme ve Sorumluluklar

Ülkemizde bilginin suistimaline yönelik girişimler için çeşitli hukuksal önlemler alınmıştır. Bu önlemlerin başında Kişisel Verilerin Korunması Kanunu, Elektronik İmza Kanunu ve Türk Ceza Kanununda yer alan bazı maddeler yer almaktadır (Yiğitbaşı, 2015, s. 72).

2.6.1 Kişisel Verilerin Korunması Kanunu (6698)

07.04.2016 tarih ve 29677 Sayılı Resmî Gazetede 6698 numara ile yayımlanan (güncel) Kişisel Verilerin Korunması Kanunu'nda yer alan bazı önemli unsurları şu şekilde sıralamak mümkündür:

Bu kanunun amacı, kişisel verilerin işlenmesinde başta özel hayatın gizliliği olmak üzere kişilerin temel hak ve özgürlüklerini korumak ve kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esasları düzenlemektir. Kişisel verilerin işlenmesinde hukuka ve dürüstlük kurallarına uygun olma, güncel olma, meşru amaçlar için işlenme, işlendikleri amaç için gerekli olan süre kadar muhafaza edilme. Kanun, kişilerin ırkı, etnik kökeni, cinsiyeti, siyasi düşüncesi, felsefi inancı, dini, mezhebi, sendika üyeliği, sağlığı, cinsel hayatı ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri özel nitelikli kişisel veri olarak kabul etmektedir ve devamında özel nitelikli kişisel verilerin, kişinin açık rızası olmadan işlenmesinin yasak olduğunu ifade etmektedir. Ayrıca kişisel verilerin ilgili kişinin rızası olmadan yurt dışına aktarılamayacağı yer almaktadır. Haklar ve yükümlülükler bölümünde ise; kişilerin veri sorumlusuna başvurarak kendisiyle ilgili kişisel verilerin işlenip işlenmediğini öğrenme, işlenmiş ise buna ilişkin bilgi talep etme, işlenme amacının ne olduğu ve amacına uygun kullanılıp kullanılmadığını öğrenme, verilerin aktarıldığı üçüncü kişilerin kim olduğunu öğrenme, eksik ya da yanlış işlenmiş ise düzeltme talep etme hakkı bulunmaktadır (<http://www.mevzuat.gov.tr/MevzuatMetin/1.5.6698.pdf>).

İlgili Kanunun, kişisel verilerin korunması hakkında başlangıç seviyesinde olduğu, geliştirilmesi ve güncellenmesi gerektiğini düşünmekteyiz. Teknoloji çok hızlı geliştiği için ilgili kanunun güncel kalması açısından esas olanın genel çerçeveyi doğru çizmek olduğu, detaylara ise bağlı yönetmelik ve ilgili yönergelerde yer verilmesinin daha uygun olacağını söyleyebiliriz. Ayrıca soyut olan bazı ifadelerin çerçevelerinin açık ve net olmadığı gibi, subjektif düşünce içermesi olasılıkları da yüksektir. Bu tür ifadelerin kullanımından kaçınılmalıdır. Örneğin; “dürüstlük kurallarına uygun olma”, “belirli amaçlar için işlenme”, “sınırlı ve ölçülü olma” gibi tereddütlere yol açabilecek ifadelerden mümkün olduğunca uzak durulması gerekmektedir.

2.6.2 Elektronik İmza Kanunu

23.01.2004 tarih ve 25355 Sayılı Resmî Gazetede 5070 numara ile yayımlanan (2008 ve 2016 yıllarındaki değişikliklerle güncellenen) Elektronik İmza Kanunu'nda yer alan bazı önemli unsurları şu şekilde sıralamak mümkündür:

Bu Kanunun amacı, elektronik imzanın hukukî ve teknik yönleri ile kullanımına ilişkin esasları düzenlemektir. Güvenli elektronik imza; a) münhasıran imza sahibine bağlı olan, b) sadece imza sahibinin tasarrufunda bulunan güvenli elektronik imza oluşturma aracı ile oluşturulan, c) nitelikli elektronik sertifikaya dayanarak imza sahibinin kimliğinin tespitini sağlayan, d) imzalanmış elektronik veride sonradan herhangi bir değişiklik yapıp yapılmadığının tespitini sağlayan imzadır. Güvenli elektronik imza, elle atılan imza ile aynı hukukî sonucu doğurur. Elektronik imza oluşturma verilerinin, üçüncü kişilerce elde edilememesini, kullanılamamasını ve elektronik imzanın sahteciliğe karşı korunmasını, imzalanacak verinin imza sahibi dışında değiştirilememesini ve bu verinin imza sahibi tarafından imzanın oluşturulmasından önce görülebilmesini düzenlemektedir. İlgili kanunun gerektiği gibi uygulanmaması durumunda ise çeşitli yaptırımlar da getirilmektedir; Elektronik imza oluşturma amacı ile ilgili kişinin rızası dışında; imza oluşturma verisi veya imza oluşturma aracını elde eden, veren, kopyalayan ve bu araçları yeniden oluşturanlar ile izinsiz elde edilen imza oluşturma araçlarını kullanarak izinsiz elektronik imza oluşturanlar bir yıldan üç yıla kadar hapis ve elli günden az olmamak üzere adlî para cezasıyla cezalandırılırlar. Yukarıdaki ifadede belirtilen suçlar elektronik sertifika hizmet sağlayıcısı çalışanları tarafından işlenirse bu cezalar yarısına kadar artırılmaktadır

(<http://www.mevzuat.gov.tr/MevzuatMetin/1.5.5070.pdf>).

Tüm elektronik imzaların "nitelikli elektronik sertifika" unsuru altında icra edilmesi kalite/güven açısından, kanunda yer alan diğer tanımlamaların ise BG temel prensiplerinin referans alınarak hazırlanmasının ise uyumluluk açısından işlevsel olacağını düşünmekteyiz.

2.6.3 Türk Ceza Kanunda Yer Alan İlgili Maddeler

Türkiye'de bilişim hukuku ile ilgili yasaların bir kısmı 2004 yılında kabul edilen 5237 Sayılı Türk Ceza Kanunda, Onuncu Bölümde, Bilişim Alanında Suçlar

başlığı altında yer alan 243-244-245 ve 246 ncı Maddeler ile düzenlenmiştir. Bu Maddeler şu başlıklar altında tanımlanmıştır

(<https://www.mevzuat.gov.tr/MevzuatMetin/1.5.5237.pdf>):

- Madde 243: Bilişim sistemine girme
- Madde 244: Sistemi engelleme, bozma, verileri yok etme veya değiştirme
- Madde 245: Banka veya kredi kartlarının kötüye kullanılması
- Madde 246: Tüzel kişiler hakkında güvenlik tedbiri uygulanması

Kişisel verilere ilişkin suçlar bakımından 26/09/2004 tarihli ve 5237 sayılı Türk Ceza Kanununun 135 ila 140 ncı madde hükümlerinin uygulanacağı, bu kanunun 7 nci maddesi hükmüne aykırı olarak; kişisel verileri silmeyen veya anonim hale getirmeyenler 5237 sayılı Kanunun 138 nci maddesine göre cezalandırılacağı ifade edilmektedir.

“Elektronik İmza Kanununda tanımlanan suçlar dolayısıyla ilgili tüzel kişiler hakkında Türk Ceza Kanununun 60 ncı maddesi hükmüne göre tüzel kişilere özgü güvenlik tedbirlerine hükmolunur. İdarî para cezasını gerektiren eylemlerin işlendikleri tarihten itibaren geriye doğru üç yıl içinde üçüncü kez işlenmesi hâlinde Kurum tarafından elektronik sertifika hizmet sağlayıcısı tüzel kişinin faaliyet izninin iptaline karar verilir” denilmektedir.

2.6.4 5651 Sayılı Kanun

5651 Sayılı Kanun, internet ortamında yapılan işlemlerin düzenlenmesi, kayıt altına alınması ve bu yayınlar yoluyla işlenen suçlarla mücadele edilmesi hakkındaki kanundur. Bu kanunun amaç ve kapsamını başlıklar altında şu şekilde sıralamak mümkündür; içerik sağlayıcı, yer yağılayıcı, erişim sağlayıcı ve toplu kullanım sağlayıcı birimlerin yükümlülük ve sorumluluklarının yanı sıra, internet ortamında işlenen belirli suçlarla bu birimler üzerinden mücadele etmektir. 5651 sayılı Kanun toplu internet hizmeti sunan kurum ya da kişilere bazı sorumluluklar yüklemektedir. Bu sorumlulukların başında da “log tutma” işlemi gelir. Log tutma (loglama) işlemi; bir sistem üzerinde gerçekleştirilen hareketlerin (çeşitli veri ve içerikleri barındıracak yeterlilikte) düzenli bir şekilde kayıt altına alınmasıdır. Log tutma işleminin yerine getirilmediği durumlarda, ilgili internet erişimi üzerinden gerçekleştirilen tüm

işlemlerden hizmet sağlayıcısının sorumluluğu söz konusudur (<http://firelog.com.tr/5651-sayili-kanun-nedir/>).

2.6.5 Siber Olaylara Müdahale Ekipleri (SOME)

Bilişim suçlarının takip edilebilmesi ve gerekli (proaktif ve/ya reaktif) önlemlerin alınabilmesi için önemli hususlardan bir diğeri ise ulusal ve uluslararası düzeyde işbirliklerinin sağlanması ve geliştirilmesidir. Özellikle BG’ni tehdit eden bilişim suçları (daha çok siber saldırılar şeklinde ortaya çıkmaktadır) zaman ve mekândan bağımsız olarak dünyanın herhangi bir yerinden gerçekleştirilebilmekte ve saldırıyı düzenleyen ve saldırıya maruz kalan taraflar genellikle farklı ülkelerde bulunmaktadır. Bu tür ataklarda saldırıyı yapan kişinin izi sürülebilse de ülkelerin farklı hukuk düzenlemelerinden dolayı gerekli yasal işlemlerin yapılabilmesi adına uluslararası hukuksal işbirliklerine ihtiyaç duyulmaktadır. Bu işbirliklerini gerçekleştirebilmek için Siber Olaylara Müdahale Ekipleri (SOME) gündeme gelmiştir. Bu ekiplerin koordinasyon içerisinde çalışması hem ulusal hem uluslararası düzeydeki güvenlik saldırılarını ülkeler adına bertaraf edebilmek için (tıpkı terörle ortak mücadele, insan kaçakçılığını uluslararası düzeyde takipte, gümrük işlemlerinde ve İnterpol çalışmalarında olduğu gibi) oldukça etkili girişimlerdir.

Ülkemizde bu alanla ilgili çalışma Siber Güvenlik Kurulu’nun ilk toplantısında “Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı” olarak kabul edilmiş ve 20 Haziran 2013 tarihinde Bakanlar Kurulu Kararı olarak yayımlanmıştır. Söz konusu eylem planı çerçevesinde kamu kurum ve kuruluşları ve özel sektör bünyesinde Siber Olaylara Müdahale Ekipleri (Kurumsal SOME, Sektörel SOME) oluşturulması öngörülmüştür

(<https://www.bgasecurity.com/egitim/kurumsal-some-egitimleri/>).

2014 yılı Temmuz ve Kasım aylarında Haberleşme Genel Müdürlüğü, sırasıyla Kurumsal SOME Kurulum ve Yönetim Rehberi ile Sektörel SOME Kurulum ve Yönetim Rehberinin birinci sürümlerini yayımlamıştır.

2.6.6 Güvenli Veri Akışı Yaklaşımı (*Data Free Flow With Trust*)

2020 Japonya G20 zirvesi için “Data Free Flow With Trust” yaklaşımı için Cory, Atkinson ve Castro (2019) “Anahtar Teslim Paketler” başlığı altında şu önerilerde bulunmaktadır:

- Küresel dijital ekonominin temelinde çatlaklar oluşmakta. Açık, kurallara dayalı bir küresel ticaret sistemini destekleyen ülkelerin ortak bir çerçeveye üzerinde anlaşması gerekmektedir.
- Dijital ekonominin temeli, bazı ülkeler kendi kurallarını başkalarına dayatmaya çalışırken, bazıları da engel oluşturup içeriye doğru yönelmeye başladığından dolayı çatlıyor.
- Verilerin inovasyon ve verimlilik avantajlarını en üst düzeye çıkarmak için açık, kurallara dayalı bir ticaret sistemini destekleyen ülkelerin temel ilkeler ve ortak kurallar üzerinde anlaşmaya varması gerekmektedir.
- Ükelere verileri nerede depolayabileceklerini veya işleyebileceklerini söylemek yerine, depoladıkları veya işlediklerinden bağımsız olarak, ülkeler topladıkları verileri yönetmek için firmaları sorumlu tutmalıdırlar.
- Ülkeler, diğer yargı alanlarında saklanan verilere kolluk kuvvetlerinin erişimini düzenleyen verimsiz süreçleri ve eski yasal sözleşmeleri gözden geçirmelidir.
- Ülkeler, lisanssız içeriğin yasadışı dağıtımını içeren veri akışlarını engellemek için ISS'lerin uygun kontrolleri ve dengeleri olan politikaları benimsemelidir.
- Verilerin “güvende” akması için, ülkelerin gizliliklerini sağlamak için güven duydukları kişi ve işletmeleri desteklemeleri kilit teknolojiyi oluşturmaktadır.

Güvenli veri akışı yaklaşımı için yukarıda ifade edilen konuların tüm ülkelerde uygulanarak belirli bir standarda ulaşmada temel anahtar olduğu savunulmakta ve bu yönde güdüleyici ve yönlendirici bilgilendirme ve taleplerin 2020 Japonya G20 zirvesinin önemli bir bölümünü kapsayacağı düşünülmektedir.

2.6.7 Avrupa Birliği Genel Veri Koruma Yönetmeliği (EU General Data Protection Regulation - GDPR)

Avrupa Birliği Genel Veri Koruma Yönetmeliği, 25 Mayıs 2018'den itibaren, Avrupa genelinde veri gizliliği yasalarını uyumlu hale getirmek için tüm üye ülkelerde uygulanmaktadır (<https://gdpr-info.eu/issues>).

İlgili Yönetmeliğin Genel Hükümler (General Provisions) Bölümünde yer alan 1. Maddesinde, Konu ve Hedefler (*Subject-matter and objectives*) başlığı altında

şu ifadelerle yer verilmektedir: “Bu Yönetmelik, kişisel verilerin işlenmesiyle ilgili gerçek kişilerin korunmasına ilişkin kuralları ve kişisel verilerin serbest dolaşımına ilişkin kuralları ortaya koymaktadır. Bu Yönetmelik, gerçek kişilerin temel hak ve özgürlüklerini ve özellikle kişisel bilgilerin korunma haklarını korur. Birlik içindeki kişisel verilerin serbest dolaşımı, kişisel verilerin işlenmesiyle ilgili olarak gerçek kişilerin korunmasına bağlı nedenlerle kısıtlanmamalı veya yasaklanmamalıdır.” 4. Maddesi, Tanımlar (*Definitions*) kısmında ise kişisel verilerin tanımı şu şekilde yapılmaktadır: “Kişisel veriler, tanımlanmış veya tanımlanabilir bir gerçek kişiyle ilgili herhangi bir bilgi anlamına gelir; tanımlanabilir bir gerçek kişi, doğrudan veya dolaylı olarak, özellikle bir ad, bir kimlik numarası, konum verisi, bir çevrimiçi tanımlayıcı gibi bir tanımlayıcıya veya fiziksel, fizyolojik özelliklere özgü bir veya daha fazla faktöre atıfta bulunularak tanımlanabilen bir kişidir, bu gerçek kişinin genetik, zihinsel, ekonomik, kültürel veya sosyal kimliğidir”

99 Maddelik bu Yönetmeliğin tam metnine ve detaylarına gdpr-info.eu web adresinden ulaşmak mümkündür.

2.7 Bilgi Güvenliği ve ISO Standartları

Bilgi sistemleri üzerine yapılan güvenlik çalışmalarına ilk olarak 1970’li yılların başında başlanmış, 1972 yılında ABD hükümeti bilgisayar sistemlerinde aranacak güvenlik gereksinimlerini de tanımlayan bir rapor yayınlamıştır. Sonrasında, Güvenilir Bilgisayar Güvenliği Değerlendirme Kriterleri (Trusted Computer Security Evaluation Criteria–TCSEC) belgesiyle bilgisayar sistemlerinin güvenlik gereksinimlerini tanımlamıştır. Bu kriterler daha sonra Ortak Kriterlerin (OK) (Common Criteria) oluşturulmasında kullanılmıştır. OK günümüzde bilgi güvenliği değerlendirmesinde en önemli standartlardan birisidir (Kara, 2018, s. 221-222). TCSEC standartlarından hareketle geliştirilen ve *Turuncu Kitap* olarak da bilinen standartlar 1983 yılında yayınlanmıştır. Avrupa Komisyonu, ülkeler arasındaki farklılıkları kaldırarak ortak bir standart uygulamak maksadı ile 1991 yılında Bilgi Teknolojileri Güvenliği Değerlendirme Kriterleri (Information Technology Security Evaluation Criteria - ITSEC) standartlarını oluşturmuştur. 2006 yılında yayınlanan OK’in 3.1 sürümü daha sonra 2009 yılında ISO/IEC 15408

standardı olarak yayınlanmıştır (OK ile ilgili detaylı bilgilere www.commoncriteria.org adresinden ulaşılabilir).

ISO-International Standards of Organisations tarafından BG için geliştirilmiş/düzenlenmiş olan çeşitli standartlardan kısaca şu başlıklar altında bahsetmek mümkündür: TS ISO/IEC 17799 Bilgi Teknoloji - Bilgi Güvenliği Standardı, TS ISO/IEC 17799 Bilgi Teknoloji - Bilgi Güvenliği Standardı, BS7799, BS7799-1, BS7799-2, ISO ve IEC (27000-27001-27002-27005).

Türkiye’de BG standartlarıyla ilgili çalışmalar ve sertifikasyon işlemleri Türk Standartları Enstitüsü (TSE) tarafından yerine getirilmekte olup, bu çalışmalar daha çok ISO/IEC Standartlarının Türkçeye tercümesi yapılarak kazandırılması şeklinde icra edilmektedir.

2.7.1 TS ISO/IEC 17799 Bilgi Teknoloji - Bilgi Güvenliği Standardı

BG için bilinen/kabul edilen en iyi standart BG’ne yönelik yöntemlerin sıralandığı ISO standardıdır. Bilgi, diğer önemli ticari varlıklar gibi, bir işletme için değeri olan ve bu nedenle gerekli şartlar yerine getirilerek korunması gereken bir varlıktır. Bilgi uygun şekilde korunmalı ve şu üç kavramı içermelidir (<http://www.belgelendirme.com.tr/>);

- *Gizlilik*: Bilginin sadece erişim yetkisi verilmiş olan kişi veya kişilerce erişilebilir olduğunun temin edilmesi
- *Bütünlük*: Bilginin bir bütün olarak olduğu gibi korunmasını temin etmek
- *Elverişlilik*: Bilgiye gerek duyulduğunda erişim yetkisi verilmiş olan kişi veya kişilerce ilgili bilgi ve kaynaklara erişimin temin edilmesi

2.7.2 BS7799, BS7799-1, BS7799-2

BS7799 BG standardını, BS7799-1 ise BG’nin sağlanmasında kullanılacak kontrolleri, BS7799-2 British Standard tarafından belirlenen Bilgi Güvenliği Yönetim Sistemi (Information Security Management Systems) gereklerini içermektedir. ISO 27001 ise daha önceden kullanılmakta olan BS7799-2’nin yenilenmiş hali ve ISO’nun uluslararası sürümüdür.

2.7.3 ISO ve IEC

ISO (International Standards Organization) Uluslararası Standardizasyon Örgütü’nü, IEC (International Electrotechnical Commission) ise Uluslararası

Elektroteknik Komisyonu’nu ifade etmektedir. ISO veya IEC üyesi olan ulusal organlar, belirli teknik faaliyet alanlarıyla ilgilenmek için ilgili kuruluş tarafından oluşturulan teknik komiteler aracılığıyla Uluslararası Standartların geliştirilmesine katılım sağlarlar. ISO ve IEC teknik komitesi, karşılıklı ilgi alanlarında işbirliği yapar. Çalışmalara, ISO ve IEC ile bağlantılı olarak, resmi ve resmi olmayan diğer uluslararası kuruluşlar da katılmaktadır. Bilgi teknolojisi alanında, ISO ve IEC, ISO/IEC JTC 1 ortak teknik komitesini kurmuştur. ISO/IEC 272002, ISO/IEC JTC 1 Ortak Teknik Komitesi (Joint Technical Committee), Bilgi teknolojisi, SC27 Alt Komitesi, BT Güvenliği teknikleri tarafından hazırlanmıştır (<https://www.sis.se/api/document/preview/916656/>).

2.7.3.1 ISO/IEC 27000-27001-27002-27005

ISO/IEC 27000- Bilgi Güvenliği Yönetim Sistemleri ailesini tarif etmektedir:

ISO/IEC 27002, organizasyonun BG risk ortamlarını göz önünde bulunduran kontrollerin seçimi, uygulanması ve yönetimi dâhil olmak üzere, kurumsal bilgi güvenliği standartları ve BG yönetimi uygulamaları için kılavuz bilgiler içermektedir. ISO/IEC 27002, ISO/IEC 27001'e dayalı bir Bilgi Güvenliği Yönetim Sistemi uygulama sürecinde kontrollerin seçilmesi; yaygın olarak kabul edilen BG kontrollerinin uygulanması ve kendi bilgi güvenliği yönetim kurallarının geliştirilmesi için kullanılmaktadır (<https://www.iso.org/isoiec-27001-information-security.html>).

ISO/IEC 27001, BG'ne yönelik geliştirilmiş kurumsal bir standart, daha geniş anlamıyla bir “yönetim sistemi” standardıdır. Orijinal adı TS ISO/IEC 27001-Information Security Management System (ISMS), Türkçe olarak da TS ISO/IEC 27001-Bilgi Güvenliği Yönetim Sistemi (BGYS) olarak adlandırılır (Çubukçu, 2018, s. 20). Genel olarak; ISO/IEC 27000 BGYS terminolojisini, ISO/IEC 27001 BGYS gereksinimlerini, ISO/IEC 27002-27007 BGYS kılavuzlarını, ISO/IEC 27011-27799 BGYS ise sektörel kılavuzları kapsar.

ISO 27001 sertifikasyonunun işletmelere sağlayacağı çeşitli faydaları şu şekilde sıralamak mümkündür: Kuruluşun kendi bilgi varlıklarının farkına varması, risk faktörlerinin varlığın bilincinde olunması, güvenilirliğinin artması, müşteri memnuniyeti, anlaşmaların daha kolay icra edilebilmesi, yasal sorumluluklara ve düzenlemelere uyumluluk, iş sürekliliğinin daha kolay sağlanabilmesi.

ISO/IEC 27001 belgesini özellikle enerji sektörü, dış ticaret, elektronik imza servis sağlayıcıları, finans kurumları, hastaneler, sigorta şirketleri, gümrükleme ve e-ticaret ile uğraşan şirketlerin alması önerilmektedir (Çubukçu, 2018, s. 26-28). Bu listeye, güvenli sertifika sağlayıcıları, üniversiteler, IT kuruluşları gibi birçok sektör eklemek mümkündür. Türkiye’de yükümlü statüsüne sahip şirketlerin gümrükleme konusunda, Enerji Piyasası Düzenleme Kurulu lisans yönetmeliklerinde değişiklik yaparak ISO/IEC 27001 belgesini zorunlu hale getirmiştir.

Ayrıca, ISO 27001 açısından üzerinde durulması gereken belki de en önemli saldırı türlerinden biri “SM” saldırısıdır. Çünkü telefon yoluyla, e-posta ve doğrudan görüşmelerde “aldatmaya” yönelik girişimler söz konusudur. Bu durum için özellikle farkındalık eğitimlerinin düzenlenmesi önerilmektedir (Çubukçu, 2018, s. 13).

BG denetimleri için ISO Uygulama Kuralları veya kısaca ISO 27002 tarafından belirlenen öneriler dikkate alınmaktadır. Bu öneriler karşılıklı güven için ortak bir temel olması amacıyla, büyüklükleri ne olursa olsun iş sektöründeki tüm kuruluşlar için gerekli standardı sağlamayı amaçlamaktadır. Uygulama Kurallarının 2013 yılı baskısı, her biri farklı bir güvenlik yönünü ele alan 14 ana kontrol maddesine göre hazırlanmıştır (International Organisation for Standardisation):

- Bilgi Güvenliği Politikaları
- Bilgi Güvenliğinin Organizasyonu
- İnsan Kaynakları Güvenliği
- Varlık Yönetimi
- Erişim Kontrolü
- Şifreleme
- Fiziksel ve Çevre Güvenliği
- İşlem Güvenliği
- İletişim Güvenliği
- Sistem Toplama, Geliştirme ve Bakım
- Tedarikçi İlişkileri
- Bilgi Güvenliği Olay Yönetimi
- İş Sürekliliği Yönetiminde Bilgi Güvenliği Unsurları
- Uyumluluk

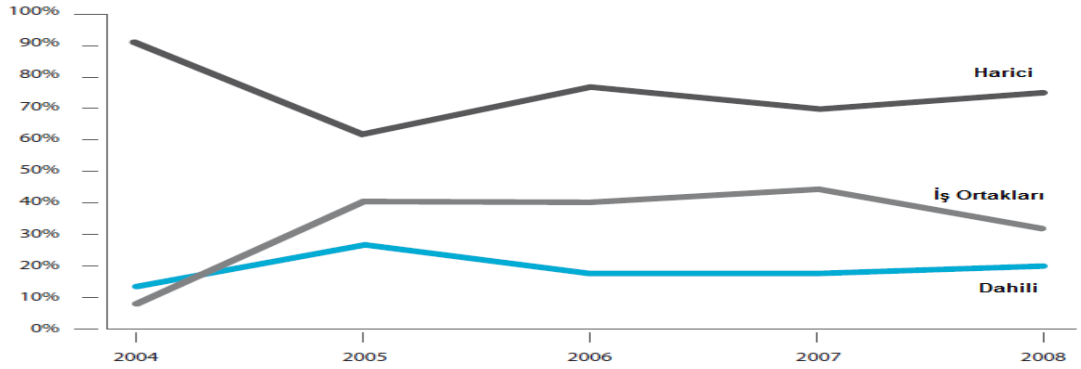
ISO/IEC 27005, risk deęerlendirmesi, risk iyileřtirmesi, risk izleme ve risk incelemesi konularında tavsiyeler de dâhil olmak üzere bilgi güvenlięi risk yönetimi rehberlięi sağlamaktadır.

2.8 Veri İhlali İstatistikleri

Bu başlık altında Verizon Business'ın 2009-2010-2011-2012-2013-2015-2016-2017-2018 yıllarını kapsayan veri ihlallerine ilişkin yapmış olduęu ve rapor halinde sunduęu arařtırmalardan faydalanarak çeřitli (istatistiksel) verilere ve bilgilere yer verilmiş olup, veri ihlalleri ile ilgili deęiřimin hangi yönde seyrettięinin ortaya konulması ve bu yönde ne tür eęilimlerin daha belirgin hale geldięinin tespit edilmesi amaçlanmıştır. Yine bu bilgiler ışığında aęırlıklı olarak hangi yönde korunma önlemlerine yer verilmesi gerektięi ile ilgili yönlendirici bilgilerin ortaya çıkartılması hedeflenmiştir.

- *2009 Veri İhlali Arařtırma Raporu İstatistikleri:*

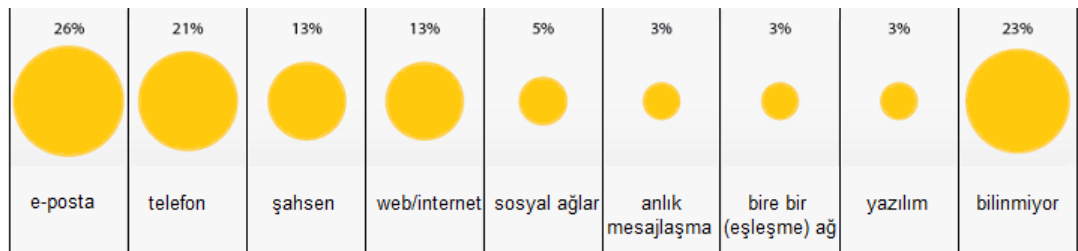
Veri ihlallerinin arkasında %74 oranında dıř kaynakların, %20 oranında ierdekilerin, %32 oranında iř ortaklarının ve %39 oranında ise birden ok tarafın bulunduęu ve bilgilere ek olarak tüm tehlikeye atılan kayıtların %91'inin organize suç gruplarıyla baęlantılı olduęu belirtilmektedir. Bu ihlallerin oluřmasına %67 oranında (kullanıcı kaynaklı) belirgin hataların yapılması, %64 oranında hackleme, %38 oranında kötü amaçlı yazılımların kullanılması, %22 oranında imtiyazların kötüye kullanılması ve %9 oranında fiziksel ataklar sebebiyet vermiştir. Bu saldırılarda kullanılan kişiselleřtirilmiş kötü amaçlı yazılımların yüzdesi 2008'e göre ikiye katlanmış, ancak 2008'e göre fiziksel saldırılarda pek fazla ihlal gözlenmemiřtir. Sektörlere göre veri ihlalleri ise řu řekildedir: %31 perakende, %30 finansal hizmetler, %14 yiyecek ve iecek, %6 imalat, %6 iř hizmetleri, %6 konaklama ve ikram, %3 teknoloji ve %3 dięer sektörler. 2004-2008 yılları arasında veri ihlallerinin kaynak daęılımı ise řekil 26'da gösterilmiştir:

Şekil 26. Veri İhlalleri Kaynak Dağılımı

Kaynak: Verizon 2009 Veri İhlali Araştırma Raporu, Erişim: 21.03.2019
(2009 Data Breach Investigations Report, <https://enterprise.verizon.com/>)

- *2010 Veri İhlali Araştırma Raporu İstatistikleri:*

Veri ihlallerinin arkasında %70 oranında dış kaynakların, %48 oranında içerdekilerin, %11 oranında iş ortaklarının ve %27 oranında ise birden çok tarafın bulunduğu ve bilgilere ek olarak tüm tehlikeye atılan kayıtların %98'inin organize suç gruplarıyla bağlantılı olduğu belirtilmektedir. Bu ihlallerin oluşmasına %48 oranında (kullanıcı kaynaklı) belirgin hataların yapılması, %40 oranında hackleme, %38 oranında kötü amaçlı yazılımların kullanılması, %28 oranında sosyal taktikleri ve %15 oranında fiziksel ataklar sebebiyet vermiştir. Sektörlere göre veri ihlalleri ise şu şekildedir: %33 finansal hizmetler, %23 konaklama ve ikram, %15 perakende, %6 imalat, %5 teknoloji hizmetleri, %6 iş hizmetleri, %4 devlet, %4 medya, %3 sağlık. 2010 yılında veri ihlallerinin kaynak dağılımı açısından sosyal taktikler oldukça artış göstermiş olup sosyal taktiklerin kendi içindeki dağılımları Şekil 27'de gösterilmiştir.

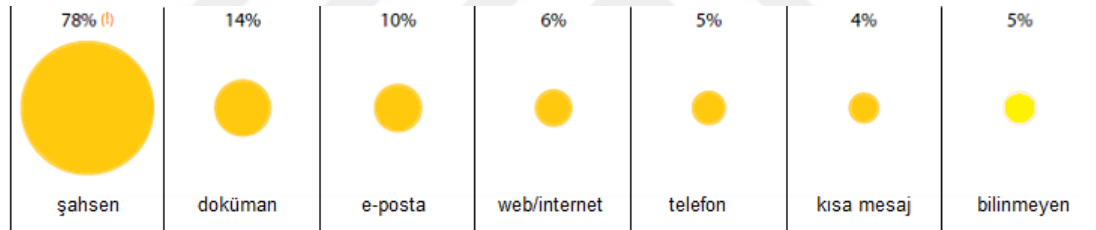
Şekil 27. Sosyal Taktiklerin Kendi İçerisinde Dağılımı - 2010

Kaynak: Verizon 2010 Veri İhlali Araştırma Raporu, Erişim: 21.03.2019
(2010 Data Breach Investigations Report, <https://enterprise.verizon.com/>)

- *Verizon 2011 Veri İhlali Araştırma Raporu İstatistikleri:*

Veri ihlallerinin arkasında %92 oranında dış kaynakların, %17 oranında içerdekilerin, %1 oranında iş ortaklarının ve %9 oranında ise birden çok (çoklu) tarafın bulunduğu ve bilgilere ek olarak tüm tehlikeye atılan kayıtların %98'inin organize suç gruplarıyla bağlantılı olduğu belirtilmektedir. Bu ihlallerin oluşmasına %50 oranında hackleme, %49 oranında kötü amaçlı yazılımların kullanılması, %15 oranında fiziksel ataklar, %17 oranında imtiyazların kötüye kullanılması, %11 oranında sosyal taktikler sebebiyet vermiştir. Sektörlere göre veri ihlalleri ise şu şekildedir: %40 konaklama ve ikram, %25 perakende, %22 finansal hizmetler, %4 devlet, %2 imalat, %2 teknoloji hizmetleri, %1 iş hizmetleri, %1 sağlık, %1 medya, %1 aşırma, %2 diğer. 2010 yılında veri ihlallerinin kaynak dağılımı açısından sosyal taktiklerin kendi içindeki dağılımları Şekil 28'de gösterilmiştir.

Şekil 28. Sosyal Taktiklerin Kendi İçerisinde Dağılımı - 2011



Kaynak: Verizon 2011 Veri İhlali Araştırma Raporu, Erişim: 21.03.2019
(2011 Data Breach Investigations Report, <https://enterprise.verizon.com/>)

- *2012 Veri İhlali Araştırma Raporu İstatistikleri:*

Veri ihlallerinin arkasında %98 oranında dış kaynakların, %4 oranında içerdekilerin, %1 oranında iş ortaklarının ve %58 oranında ise aktivist gruplarının bulunduğu belirtilmektedir. Bu ihlallerin oluşmasına %81 oranında hackleme, %69 oranında kötü amaçlı yazılımların kullanılması, %10 oranında fiziksel ataklar, %5 oranında imtiyazların kötüye kullanılması, %7 oranında sosyal taktikler sebebiyet vermiştir. Sektörlere göre veri ihlalleri ise şu şekildedir: %54 konaklama ve yemek hizmetleri, %20 perakende satışlar, %10 finans ve sigorta hizmetleri, %7 sağlık ve sosyal yardım hizmetleri, %3 enformasyon, %6 diğer. Sektörlere göre dağılımda büyük organizasyonlar (en az 1.000 çalışan) için veri ihlalleri dağılımı ise şu

şekildedir: %28 finans ve sigorta, %22 enformasyon, %12 perakende satış, %8 imalat, %7 kamu yönetimi, %5 taşıma ve depolama, %18 diğer.

- *2013 Veri İhlali Araştırma Raporu İstatistikleri:*

2013 yılı “perakendecinin ihlali yılı” olarak etiketlenebilir, ancak InfoSec risk ortamının daha kapsamlı bir değerlendirmesi, jeopolitik saldırılardan ödeme kartı sistemlerine doğru yönelen büyük çaplı saldırılara geçiş yılı olduğunu gösteriyor.

27 farklı ülkeyi kapsayan verilere göre finansal kuruluşlar %37, perakende ortamlar ve restoranlar %24, imalat, nakliye ve kamu hizmetleri %20, enformasyon ve profesyonel hizmet firmaları %20, büyük organizasyonlar ise %38 oranında veri ihlallerinden etkilenmiştir. Veri ihlallerinin arkasında %92 oranında dış kaynakların, %14 oranında içerdekilerin, %1 oranında iş ortaklarının, %7 oranında birden çok tarafın ve %19 oranında ise devlet bağlantılı aktörlerin bulunduğu belirtilmektedir. Bu ihlallerin oluşmasına %52 oranında hackleme, %76 oranında ağ üzerinden (zayıf veya çalınmış kimlik bilgilerine) yapılan ataklar, %40 oranında kötü amaçlı yazılımlar, %35 oranında fiziksel ataklar, %29 oranında sosyal taktikler ve %13 oranında imtiyazların kötüye kullanılması sebebiyet vermiştir.

- *2015 Veri İhlali Araştırma Raporu İstatistikleri:*

2015 yılında da bir önceki yılda olduğu gibi veri ihlallerinden en çok etkilenen ilk üç sektör; kamu, enformasyon ve finans sektörü olmuştur. Buradan şu sonucu çıkartmak mümkündür: Hiçbir endüstri güvenlik açıklarına karşı bağışık değildir. Sektörlere göre güvenlik ihlalleri (vuku bulan olay sayılarına göre) Tablo 8’de verilmektedir.

Tablo 8. Güvenlik Ataklarının Sektörel Dağılımı (Olay Sayısına Göre)

Sektörler	Toplam	Küçük Org.	Büyük Org.	Bilinmeyen
Kamu	50.315	19	49.596	700
Enformasyon	1.496	36	34	1.426
Finans Hizmetleri	642	44	177	421
İmalat	525	18	43	464
Perakende	523	99	30	394
Konaklama	368	181	90	97
Mesleki	347	27	11	309
Diğer Hizmetler	263	12	2	249
Sağlık	234	51	38	145
İdari	205	11	13	181
Eğitim	165	18	17	130
Kamu Hizmetleri	73	1	2	70
Taşıma	44	2	9	33
Eğlence	27	17	0	10
Maden	22	1	12	9
Emlak	14	2	1	11
Ticaret	14	10	1	3
Yönetim	4	0	2	2
İnşaat	3	1	2	0
Tarım	2	0	0	2
Bilinmeyen	24.504	144	1	24.359
	79.790	694	50.081	29.015

Kaynak: Veriler Verizon 2015 Veri İhlali Araştırma Raporu’ndan derlenmiştir.
 (2015 Data Breach Investigations Report, <https://enterprise.verizon.com/>) Erişim:
 21.03.2019

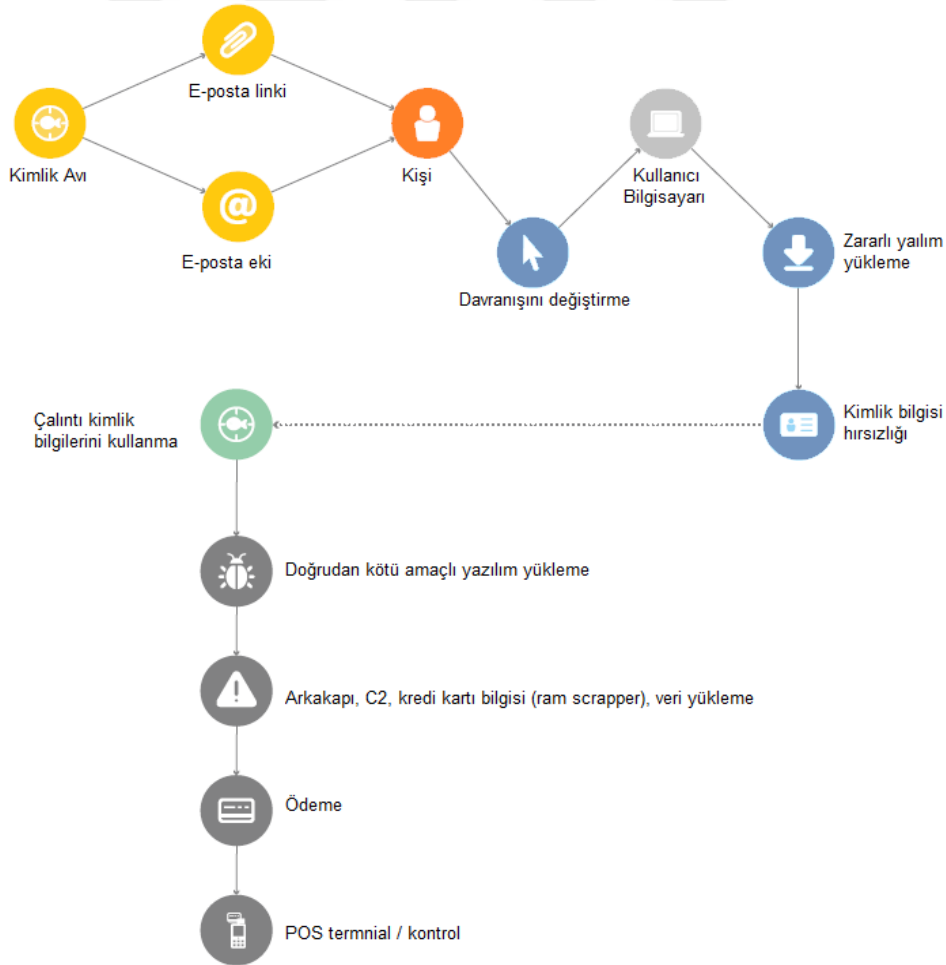
Tablo 8’deki verilere bakacak olursak en büyük veri ihlallerinin kamu sektöründeki büyük ölçekli organizasyonlara, enformasyon sektörüne, finans sektöründeki büyük organizasyonlara, imalat ve perakende sektörüne, konaklama sektöründeki küçük organizasyonlara karşı yapıldığı görülmektedir. Bunun yanı sıra, “Bilinmeyen” (tespit edilememiş ya da bildirilmemiş) tipteki sektör rakamının ve “Bilinmeyen” sütunundaki rakamların yüksekliği göz önünde tutulmalıdır.

- *2016 Veri İhlali Araştırma Raporu İstatistikleri:*

Fiziksel hırsızlıklar tekrar tekrar gördüğümüz bir problemdir ve bu olaylar en çok mağdurun kendi çalışma alanında (%39) veya çalışanın kişisel araçlarında (%33,9) meydana gelmektedir. Bu yılın verilerine göre kaybedilen varlıklar (asset), çalınan varlıklardan yüz kat daha fazla.

Kimlik bilgileri ve kimlik avı konularına odaklanmak, rakip tarafından yapılan işlemlerin tek bir yapıya özgü olmadığını göstermek 2016 raporlarında dikkat çekilen önemli konulardan birisidir. Özellikle SM’de sıkça kullanılan kimlik avı (phishing) ve kişiye doğrudan erişimin, kötü niyetli yazılımlar kullanmak kadar tehlikeli ve etkili olduğu ve bunun da veri/bilgi güvenliğini doğrudan etkilediği görülebilmektedir. Bu durum Şekil 29’da görsel olarak ifade edilmiştir.

Şekil 29. Bir Veri İhlalinin Ortaya Çıkışı ve Rotası



Kaynak: Verizon 2016 Veri İhlali Araştırma Raporu, Erişim: 21.03.2019
(2016 Data Breach Investigations Report, <https://enterprise.verizon.com/>)

- *2017 Veri İhlali Araştırma Raporu İstatistikleri:*

Veri ihlallerinin arkasında %75 oranında dış kaynakların, %25 oranında iç aktörlerin, %18 oranında devlete bağlı aktörlerin, %3 oranında çoklu tarafların, %2 oranında iş ortaklarının ve %51 oranında ise suç gruplarının bulunduğu belirtilmektedir. Bu ihlallerin oluşmasına %62 oranında hackleme, %51 oranında kötü amaçlı yazılımların kullanılması, %81 oranında çalınan ya da zayıf parolalar, %43 oranında sosyal ataklar, %14 oranında imtiyazların kötüye kullanılması, %8 oranında fiziksel ataklar sebebiyet vermiştir. Veri ihlallerinden etkilenenlerin %24'ünü finans kuruluşları, %15'ini sağlık kuruluşları, %12'sini kamu kuruluşları, %15'ini ise perakende ve konaklama sektörü (birlikte) oluşturmaktadır. Bu ihlallerin %66'sını zararlı yazılım içeren e-posta ekleri, %73'ünü finansal (maddi) motivasyon, %21'ini casusluk eylemleri oluşturdu ve bu ihlallerin %27'si üçüncü taraflarca fark edildi.

- *2018 Veri İhlali Araştırma Raporu İstatistikleri:*

Veri ihlallerin %76'sı finansal olarak motive edildi. Siber saldırıların neredeyse dörtte üçü (%73) dış kaynaklarca gerçekleştirildi. Yine de bütün saldırılar dış kaynaklı değil; çeyrekten fazla (%28) saldırı içeriden yapıldı. Organize suç gruplarının üyeleri tüm ihlallerin yarısının arkasında, devlet bağlantılı aktörlerin oranı is %12.

Sonuç olarak, veri ihlallerinde kategorilere göre belirtilen yüzdelik dilimlerin (yıllara göre değişen) yıllık artış ve azalışlarına bakılacak olursa, belirli bir tutarlılığın (doğrusal artış ya da azalış) görülmediği gözlemlenmektedir. Bunun çeşitli sebeplerinin olabileceği varsayılmaktadır. Örneğin; toplumsal olaylar (Arap Baharı, gösteriler, protestolar, ülkeler arası gerginlikler vb.), hacktivist girişimler, uluslararası organizasyonlara yönelik girişimler ve saldırı organizasyonların yıllara göre değişiklik göstermesi, diğer taraftan ise bir önceki yıl için tespit edilen açıkların fark edilerek en çok o yönde önlem alma girişimlerinin olabileceği düşünülmektedir. Özellikle son yıllarda göze çarpan bir diğer özellik ise SM ataklarının hızlı bir yükselişe geçmesi ve ayrıca veri ihlallerinin %28 gibi bir oranla içerden (kurum/kuruluş içi) kaynaklandığı görülmektedir.

ÜÇÜNCÜ BÖLÜM

3. ENDÜSTRİ 4.0

Endüstriyel devrim süreci geçmişten günümüze dörde ayrılmaktadır. Endüstri 1.0 olarak da adlandırılan birinci süreçte, su ve buhar gücü kullanımı ile çalışan mekanik sistemler bulunmaktaydı (ilk mekanik dokuma tezgahı-1784). Endüstri 2.0 olarak isimlendirilen ikinci süreçte ise elektrik enerjisinin kullanılmaya başlaması ile seri üretime geçildi (ilk hareketli bant sistemi mezbahane kullanımı-1870). Üçüncü ve şu an genel olarak yaşanan endüstri 3.0 süreci ise, elektronik ve bilişim teknolojilerinin birlikte kullanılması ile başladı (ilk programlanabilir yönetim sistemi SPS-1969). Henüz başlamış olan ve içinde bulunduğumuz dördüncü süreçte ise sanal ve fiziksel sistemlerin entegre bir şekilde kullanılması hedeflenmektedir. İnternete bağlı her nesnenin (sensör, bilgisayar, makine, cihaz vb.) üretim alanına daha fazla katkı sunması planlanmaktadır. Bu doğrultuda endüstriyel alanda köklü değişimler gerçekleştirecek olan ve “Dördüncü Endüstri Devrimi / Endüstri 4.0 (E 4.0)” olarak adlandırılan yeni bir süreç başlatıldı. İnternetin (ağırlıklı olarak Nesnelerin İnterneti’nin -IoT-) üretimde kullanılması, iş geliştirmeden mühendisliğe birçok yeniliği de beraberinde getireceği düşünülmektedir (GelecekHane, 2019).

Birinci Endüstri Devrimi 18. ve 19. yüzyıllarda gerçekleşerek buhar kazanları ve mekanik üretim gibi yenilikler getirmiş, İkinci Endüstri Devrimi ise 19. yüzyılın sonlarında ve I. Dünya Savaşından önce gerçekleşmiş telgraf ve endüstriyel dikiş makineleri gibi alanlarda çığır açmıştı. 1970’lerin sonlarında sanayideki yeniliklerin hızla devam etmesi Üçüncü Endüstri Devrimi olarak bilinen ve internet ve akıllı telefonlar gibi yenilikleri kapsayan dönemi getirmiştir. Dördüncü Endüstri Devrimi ise diğerlerine göre daha soyut olmakla birlikte yapay zekâ’nın her türden makine ile iletişim kurmasına ve makinelerin birbirlerinden öğrenmesine izin veren bir geleceği temsil etmektedir (Yılmazel, 2019, s. 159).

E 4.0 esas itibarıyla 2011 yılında Almanlar tarafından ülke kalkınmasına yönelik olarak hazırlanan proje önerilerinden sadece biriydi ve bilgi entegrasyonu temelli siber fiziksel sistemlerin üretilmesiyle ilgiliydi. Yapay zekâ destekli ve yüksek oranda otonom sistemlerin Nesnelerin İnterneti aracılığı ile bir birleri ile konuşan makinelerin Büyük Veri’den faydalanarak iş ve üretim süreçlerinin optimize edilmesiyle alakalıydı. Çabucak tüm dünyada kabul gören bu yaklaşım ülkelere göre

farklı algılanıp kendi tarzları ve yetenekleri doğrultusunda içi doldurulmaya çalışılsa da, esas olan üretim ve iş süreçlerindeki verimliliği, devamlılığı, doğru kararlar almayı, hızı ve kesintisiz işleyişi öne çıkartmaktır.

20. yüzyılın sonlarına doğru inanılmaz boyutlarda değişen teknoloji, iletişimin daha kolay ve daha hızlı yapılabilmesine olanak sağladı. Bu sayede, internetin sınırları kaldırması, tedarikçi, müşteri ve üreticilerin sanal platformlarda buluşması; küreselleşmeye, dünya ticaretinin artmasına ve sosyo-kültürel yapının değişmesine önemli katkılar sundu. Buna paralel olarak mikro elektronik alanındaki gelişmeler, sensör ve iletişim teknolojilerinin ölçek ekonomisi (kitle üretimi) kapsamında üretilmesine olanak sağlayarak, küçük boyutlarda ve düşük enerji tüketen sensörlerin (dolayısıyla bu sensörlerin kullanıldığı cihazların) uygun maliyetlerle üretilmesinin önünü açtı (Apilioğulları, 2018, s. 11). Sonrasında, Nesnelerin İnterneti'nin aracılık ettiği siber-fiziksel sistemlerin gelişmesi E 4.0 çatısını büyük bir oranda belirlemiş oldu.

Rekabetin akıllı ürüne doğru kayması, üretim süreçlerinin de gelişmesine etki ederek daha çok fonksiyonel ve özel ürünün, hızlı ve hassas toleranslarla üretilmesi amacıyla, firmalar yeni teknolojileri işletme süreçlerinde kullanmaya başladı. Sensör ve iletişim teknolojileri üretim süreçlerinin otomasyon yeteneklerini geliştirerek üst seviyelere taşınması akıllı ekipman (smart devices) kavramını ortaya çıkardı. Dolayısıyla, dijital dünya ile fiziksel dünyanın entegre edilmesi yani akıllı fabrika (smart factory) kavramını ortaya çıkarttı (Apilioğulları, 2018, s. 12-13).

İnterneti insana benzetirsek, internet altyapısını sağlayan ağları da insan beynindeki nöron ağına benzetebiliriz. İnsan hayatı düzensiz, beklenmedik gelişmelerle doludur. Hayatımızı yöneten beynimiz ise bu gelişmelere anında cevap verecek kadar esnek bir yapıya sahiptir. Geleceğin interneti de insanın her yaptığına uyum sağlamak üzere, nöron ağına benzer bir esnekliğe sahip olmalıdır. Geleceğin internetini tanımlarken, insan doğasına uygun olarak “organik” kavramının tercih edilmesi bu sebeptendir. İletişim ve bilgi alışverişi için bugün e-posta, mesajlaşma programları kullanılmakta iken, gelecekte ise işlerin yapılması için doğrudan işleri başlatacak, komutları verecek mesajlar yaratmak mümkün olabilecektir. 3B yazıcılara gönderilen tasarım dosyaları, sanal suretlerimizin bizim adımıza sosyal medya hesaplarımızı yönetmesi, uzaktaki bağlı nesnelerden gerçek zamanlı bilginin

toplanması, robotları uzaktan yönetmek gibi işlemler bir göz hareketi ile ya da sadece düşünce ile mümkün olabilecektir (Erbaşlar ve Dokur, 2016, s. 34-35). Tüm bu açıklamalar göz önüne alındığında, geleceğin internet altyapısı, Nesnelerin İnterneti, siber güvenlik gibi birçok başlık E 4.0 çatısı altında öne çıkmakta ve daha çok önem kazanmaktadır. Bu altyapıları yönetecek olan şirket ve kurumlar ise bu konular üzerindeki araştırmalarını daha derinleştirerek daha çok AR-GE ve yatırım harcaması yapma ihtiyacı duyacaktır.

Nesnelerin İnterneti, Büyük Veri ve bulut bilişim gibi gelişmekte olan bilgi teknolojileri ve yapay zekâ teknolojileri, E 4.0'ın akıllı fabrikasını uygulamaya yardımcı olmaktadır. Akıllı makineler, taşıyıcılar ve ürünler, birden fazla ürün çeşidinin esnek bir şekilde üretilmesi ve kendilerini yeniden yapılandırmak için birbirleriyle iletişim kurar ve müzakere ederler. Endüstriyel ağ, akıllı nesnelerden büyük miktarda veri toplar ve buluta aktarır. Bu, sistem performansını optimize etmek için Büyük Veri analizlerine dayalı sistem genelinde geribildirim ve eşgüdüm sağlar. Yukarıda bahsedilen kendi kendine organize edilen yeniden yapılandırma ve Büyük Veri tabanlı geri bildirim ve koordinasyon, akıllı fabrikanın çerçeve ve operasyonel mekanizmasını tanımlar (Wang, Wan, Zhang, Li, Zhang, 2016).

Gelecekte, etrafımızdaki dünyadaki algılayıcıların sayısında çarpıcı bir artış bekleyebiliriz. Bunlar bir arada kullanıldıklarında tespit edebilecekleri birçok şey olacak ve büyük bir gelişme kaydedecekler. Bu, giderek artan *hassas* bir teknolojidir. Avuç içi cihazlarımızda sesi ölçmek için mikrofon, konum belirlemek için GPS yongaları, görüntüleri yakalamak için kameralar ve başka başka birçok sensör bulunmaktadır. Fiziksel dünya ile etkileşime girmek için giderek artan bir şekilde etrafımızdaki bu cihazlar radar, sonar, lidar (üzerinde bulunan bir lazer ışını sayesinde etrafında bulunan cihazlarla arasındaki mesafeyi ölçmeye yarayan sistem), hareket sensörü, barkod tarayıcıları, nem göstergeleri, basınç sensörleri, manyetometreler, barometreler, ivmeölçerler ve diğer algılama araçlarını kullanacaktır (Susskind, 2018, s. 49). Mobil cihazlarda ya da giyilebilir teknolojilerde ihtiyaç duyulacak olan sensörler bunlarla sınırlı kalmayacaktır. Yukarıda bahsedilen sensörlerin yanı sıra havadaki nemi ölçmek, sıcaklık değişikliklerini anlık gözlemlemek, ses şiddetini takip etmek, hava kirliliğini, havadaki oksijen azot ya da karbon monoksit değerlerini ölçmek, etrafımızdaki

kimyasal maddeleri belirlemek, kokuları algılamak biyometrik ölçümleri (kan basıncı, şeker, nabız, tansiyon, stres düzeyi vb.) takip etmek, araçlar için boş park yerlerini tespit etmek ve buna benzer onlarca veri akışını gerçek zamanlı takip ederek önce enformasyon daha sonra bilgi olarak kullanılmak üzere frekans, medyan, korelasyon vb. değerlendirmelere tabi tutulacaktır. Etrafımızı çevrelemiş olan tüm bu veri ajanları (Nesnelerin İnterneti) sayesinde birbirleri ile konuşabilen/iletişim kurabilen cihazlar arasında cereyan eden veri alış verişi ışık hızıyla hareket ederek, saniyeler içerisinde terabaytlar (1 trilyon bayta denk gelen bilgisayar depolama kapasite birimi) düzeyinde bir yerden başka bir yere akacaktır.

Çoğu kişinin düşündüğünün aksine E 4.0 yalnızca durmaksızın 7/24 çalışan akıllı robotlarla doldurulmuş çok pahalı ve tamamen otomatize edilmiş bir işletme demek değildir. “Akıllı” bir işletme, mevcut fiziksel donanımı, veri toplayan Nesnelerin İnterneti cihazlarına bağlayarak ve veri analizi yapacak yazılımlar (analitikler) kullanarak da E 4.0 alanında başarılı olabilir. Bu yeni veri yapısı, tasarım ve üretim çözümlerini kolaylaştıracak ve işletmelerde iyileşmeler sağlayacaktır (Banger, 2018a). “Akıllı” işletmelerin yanı sıra E 4.0’ın işletmeler/kurumlar için dikkat çeken bir diğer özelliği ise dijitalleşme ve uzaktan erişim alanlarındaki gelişmelere olan katkıları olacaktır.

DigitalEurope’un hazırlamış olduğu raporda Avrupa üretim endüstrisinin dijitalleşmesi ile 2030 yılında büyümenin %15’ten %20’lere çıkması öngörülmekte, Birleşik Krallık’ta doğrudan sağlık sektörünü etkileyebilecek diğer bir istatistiğe göre ise sağlık girişimlerinin hâlihazırda %90’ının yüz yüze gerçekleştiği ve bu oranın sadece %1 azaltılması ile 200 milyon Sterlin kadar bir maliyetin azaltılabileceği ifade edilmektedir. Yaratıcı endüstrilerde dijitalleşme ile 2013 yılında %47 olan gelir artışının 2015 yılında %57 olduğu gösterilmiştir. Uzaktan eğitim endüstrisinin 15 kat daha fazla büyüyerek sonraki on yıl içinde toplam eğitim sektörünün %30’unu işgal etmesi beklenmektedir (Özdoğan, 2018, s. 21-22).

Deloitte (2017b) “Revolution” başlıklı raporunda E 4.0 için şu ifadeler yer vermektedir: Girişimin temel yapısındaki en son ve muhtemelen en önemli devrim. E 4.0, bilgi işlem, veri, yapay zekâ ve evrensel bağlantıların birleşmesinden kaynaklanıyor. Bu devrim her sektörü yeni baştan şekillendiriyor. Ekonominin bu değişimin dönüştürücü etkisinden korunmuş bir yönü yoktur. Bazı endüstriler

diğerlerinden daha hızlı deęiřecek, ama sonunda hepsi deęiřecek. Ancak deęiřim zordur. Teknoloji her zaman dost deęildir. E 4.0 iřletmelere verimlilik ve i gr iin ok byk fırsatlar sunuyor, fakat aynı zamanda yeni rakipler yaratıyor, eski alıřma yntemlerini tehdit ediyor ve gvenlik ve itibar iin yeni riskler yaratıyor.

Bu blmde genel olarak E 4.0'ın tanımı, bileřenleri, avantaj ve dezavantajları, olumlu ve olumsuz yanları ile gelecek iin neler vaat ettięi zerinde durulacaktır. Ayrıca, iřletmelerin bu yndeki deęiřimi ve E 4.0'ın nndeki engeller aıklanmaya alıřılacaktır.

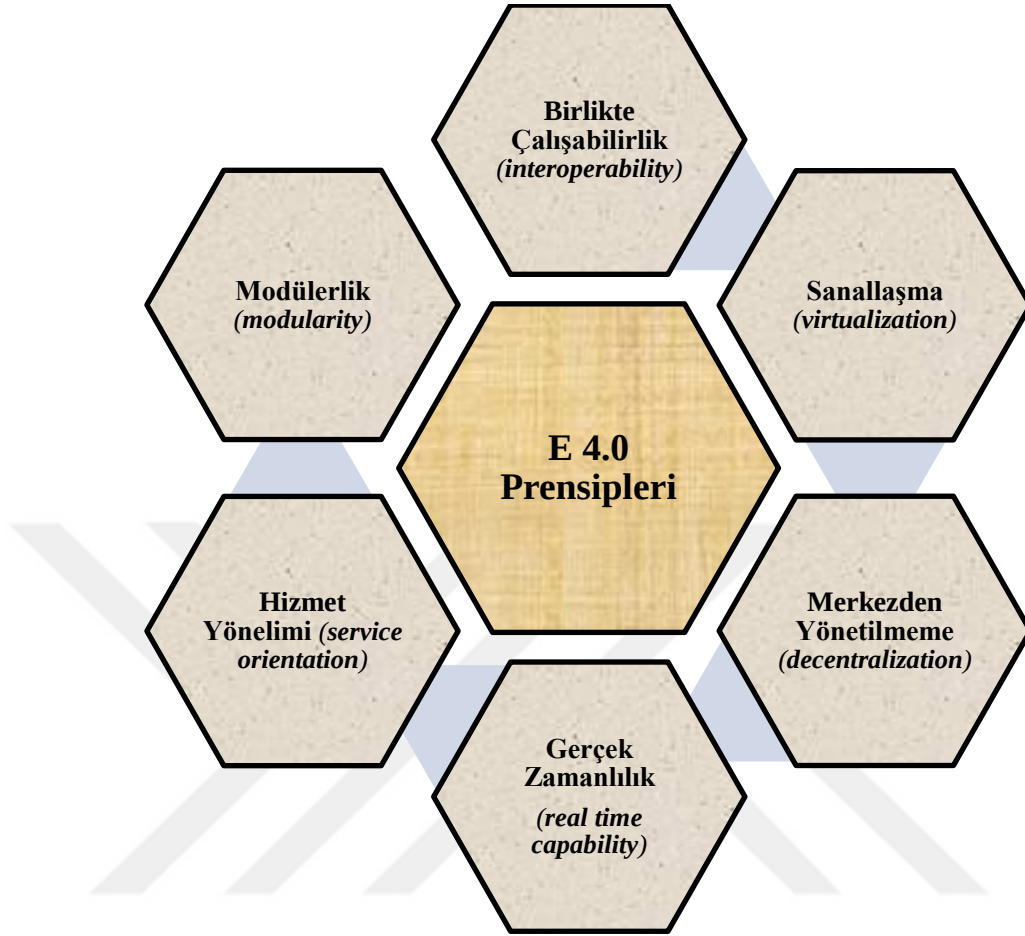
3.1 Tanımı

E 4.0 terim olarak Drdnc Sanayi Devrimi anlamına gelmektedir. Sevin (2018)'e gre E 4.0 en son ve ileri teknolojiyi, otomasyonu, veri alıřveriřini ve retim teknolojilerini kolektif bir yapı ierisinde kullanmayı iermektedir. Bylece siber-fiziksel sistemlerin kendi kendine (self) optimizasyonun saęlanmasını ngrmektedir. Bu kapsamda E 4.0'ı, geleneksel sanayiye bilgisayarlařma ynnde teřvik eden ve yksek teknolojiyle donatmasını ieren proje olarak tarif etmek mmkndr. E 4.0, altı temel prensip zerinde ykselmektedir. Bunlar; birlikte alıřabilirlik (*interoperability*), sanallařma (*virtualization*), merkezden ynetilmeme (*decentralization*), gerek zamanlılık (*real time capability*), hizmet ynelimi (*service orientation*) ve modlerlik (*modularity*) dir. řekil 30'da bu altı temel prensip grsel olarak da ifade edilmiřtir.

Marr (2016) E 4.0'ı, bilgisayarlar ve otomasyonun tamamen yeni bir řekilde bir araya gelerek ortaya ıkarttıęı bir yapılanma olarak tanımlamaktadır. Makine ve robotlara insan mdahalesinin ok az olduęu, robotik ęrenmenin n planda olduęu ve makinelerin birbirlerine uzaktan eriřim saęladıęı bir sistem olarak tarif etmektedir.

Esas olarak Alman hkmetinin imalat gibi geleneksel sanayisini bilgisayarlařma ynnde teřvik etmek ve yksek teknolojiyle donatma projesi olarak planlanıp hazırlanan ve sunulan E 4.0 yeni bir sanayi devrimi nitelięi tařıdıęı iin, uygarlıęın getięi ilk  devir (Birinci, İkinci ve nc Sanayi Devrimleri) sonrası gelen drdnc ařama olarak adlandırılmıřtır (Mobilya Dekorasyon, 2016).

Şekil 30. Endüstri 4.0 Prensipleri



Kaynak: Sevinç, 2018'den uyarlanmıştır.

E 4.0'da dijital imalat (otomasyon, veri alış verişi, üretim teknolojileri), entegre iletişim ağı (Nesnelerin İnterneti – IoT), siber fiziksel sistemler, akıllı fabrikalar (esneklik, hız ve verimlilik) ve ayrıca verilerin yorumlanarak (Büyük Veri, yapay zekâ ve algoritmalar sayesinde) anlamlı çıkarımlarda bulunmak (iş zekası) üzerine bir yapılanma söz konusudur (Öztemel, 2018, s. 81). E 4.0; bilişim, iletişim ve internet teknolojilerinin üretim süreçlerini yoğun biçimde etkilemesi ve dönüştürmesi ile ortaya çıkan yeni bir durumdur. Bilişim ve iletişim teknolojilerinin (BİT) operasyonel teknolojiler (OT) ile bütünleşmesi ve buna bağlı olarak yeni iş modellerinin ortaya çıkması olarak da ifade etmek mümkündür (Banger, 2018a). E 4.0 kendi üretimini, kapasitesini ve tedarik zincirini planlayabilen yeni nesil endüstridir; fiziksel sistemler ile siber sistemlerin konuştuğu bir dünyadır (Özdoğan, 2018). Nesnelerin İnterneti, bulut bilişim, otonom sistemler, veri analitiği, yapay

zekâ ve makine öğrenmesi ile bu alt yapı günümüz koşullarında kısmen de olsa oluşturulmuş bulunmaktadır.

E 4.0 temel olarak Üçüncü Sanayi Devrimi'ndeki sistemlerin daha akıllı olmasına ve otomasyona dayanan bir kavramdır. Teknoloji ve siber sistemlerin üretim kapasitelerini arttırmaya yöneliktir. Akıllı fabrikalardan esas kasıt budur. Bütün sistemlerin dijitalleştirilmesi ve uzaktan takip edilebilmesidir. E 4.0 ayrıca, bu sistem içerisinde yer alacak yeni nesil robotların kusursuzca çalışmaları yanı sıra birbirleri ve insanlarla iletişim halinde olmasını ve robotların kullanacağı sistemlerin yapay zekâ aracılığı ile öğrenen algoritmalara sahip olmasını da içermektedir. Akıllı fabrikalara ek olarak otonom araçlar, uçabilen cihazlar, üç boyutlu yazıcılar üretimin daha verimli ve fabrikaların tam kapasite ile çalışabilmelerine destek olacaktır (Özdoğan, 2018, s. 28).

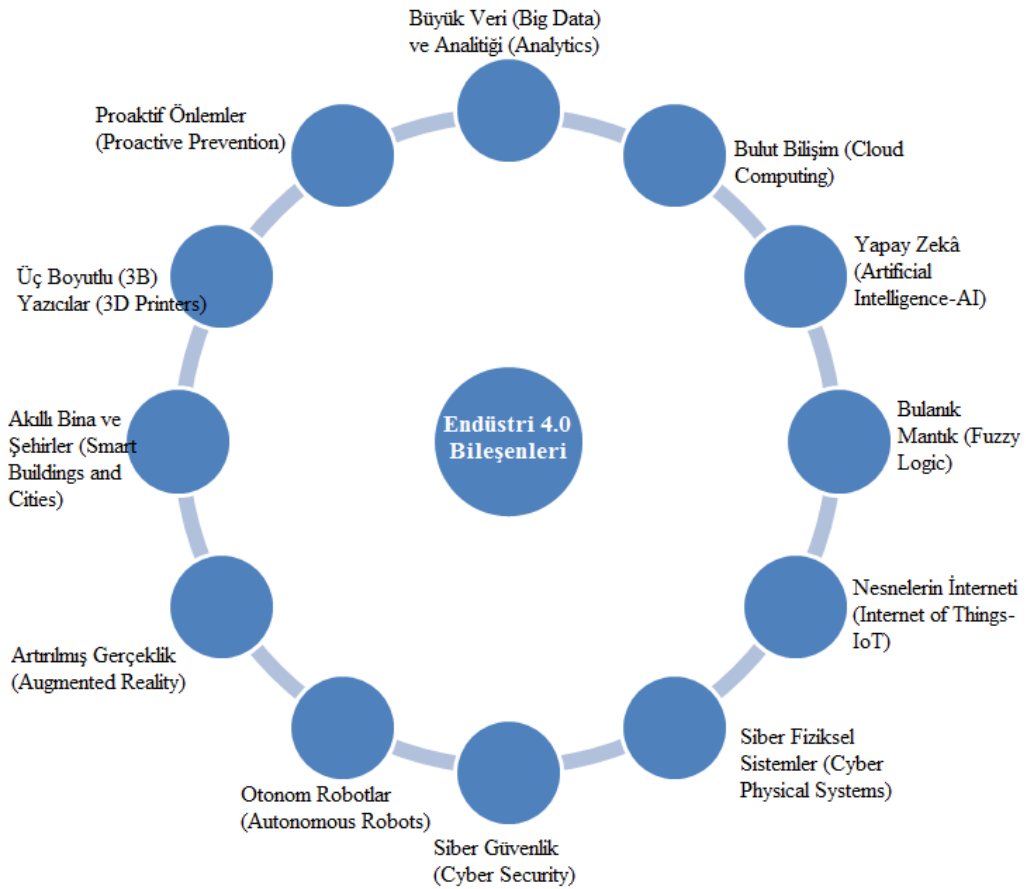
3.2 Endüstri 4.0'ın Bileşenleri

İngiliz filozof Jeremy Bentham 1770'lerin sonuna doğru, eski Yunancada “bütünü gözlemlemek” anlamına gelen *panoptikon* düşüncesini (yeni tip) hapisaneler ya da kurumlar inşa etmek amacıyla ortaya atmıştır. Bu fikre göre pasta dilimi şeklinde demir parmaklıklar ve çemberin tam ortasında da bir nöbet kulesi olacaktı. Tüm mahkûmlar buradan gözetlenebilecek ancak gözetlendiklerini bilmeyeceklerdi. Panoptikon düşüncesiyle “görünmez her şeye kadir olması” duygusunun oluşturulması hedeflenmişti. Bu kavrama *nesnelerin interneti*'nin gelişiminden daha iyi bir örnek verilemez. Bu teknolojinin vatandaşa verilen hizmetin gelişiminde faydası çoktur fakat esas mesele mahremiyetin nasıl korunacağıdır (Løkke, 2018, s. 31). Aynı şekilde BG, gözetlenmenin sınırlarının nerelere dayanabileceği, merkez gücün kimin elinde toplanacağı, idarenin bu gücü hangi yönde ve nasıl kullanacağı vb. konularda şimdilik cevaplanabilmesi oldukça zor birçok soru da gündeme gelmektedir.

E 4.0'ın temel bileşenlerini genel olarak şu başlıklar altında toplamak mümkündür; Büyük Veri, bulut bilişim, yapay zekâ, bulanık mantık, Nesnelerin İnterneti, siber fiziksel sistemler, siber güvenlik, otonom robotlar, sanal gerçeklik, akıllı bina ve şehirler, üç boyutlu yazıcılar, proaktif önlemler. Bu listeye elbette daha bir çok başlık (yatay ve dikey sistem bütünleştirilmesi, nano teknoloji, makine öğrenmesi, sanal gerçeklik, kripto paralar ve blockchain vb.) ilave etmek mümkün

olmakla birlikte E 4.0'a ait temel bileşenleri genel hatları ile kavramak için bu bölümde yer alan başlıkların (Şekil 31) yeterli olacağı düşünülmektedir. Her ne kadar bu bileşenler tekil başlıklar şeklinde ele alınarak aşağıda açıklanmış olsa da, görüleceği üzere hiçbir başlık bir diğeri ya da diğerlerinden bağımsız değildir. Bu nedenle bileşenleri kavramak için ikili üçlü gruplar şeklinde yaklaşımlarda bulunmak daha doğru bir tercihtir. Örneğin, bulanık mantığın yapay zekâdan, bulut bilişimin Büyük Veriden, Nesnelerin İnternetinin siber fiziksel sistemlerden, akıllı bina ve şehirlerin artırılmış gerçeklik ve otonom robotlardan ayrı düşünülmesi söz konusu değildir. Konu içerikleri ve açıklamalar incelenirken bu durum kolayca fark edilebilecektir. Her bir alan müstakil bir konu gibi gözükse de yukarıdaki gerekçelerden dolayı E 4.0'ın ana çatısı altında toplanmaktadır. Öte yandan, yine "sistem yaklaşımı"ndan hareketle, E 4.0'ın bu yaklaşıma uygun olarak, alt birimlerinin toplamından daha fazla şey ifade ettiği dikkatlerden kaçmamalıdır. Burada kast edilen şey "büyük resmi" görebilmektir.

Şekil 31. Endüstri 4.0'ın Temel Bileşenleri



3.2.1 Büyük Veri (*Big Data*) ve Analitiği (*Analytics*)

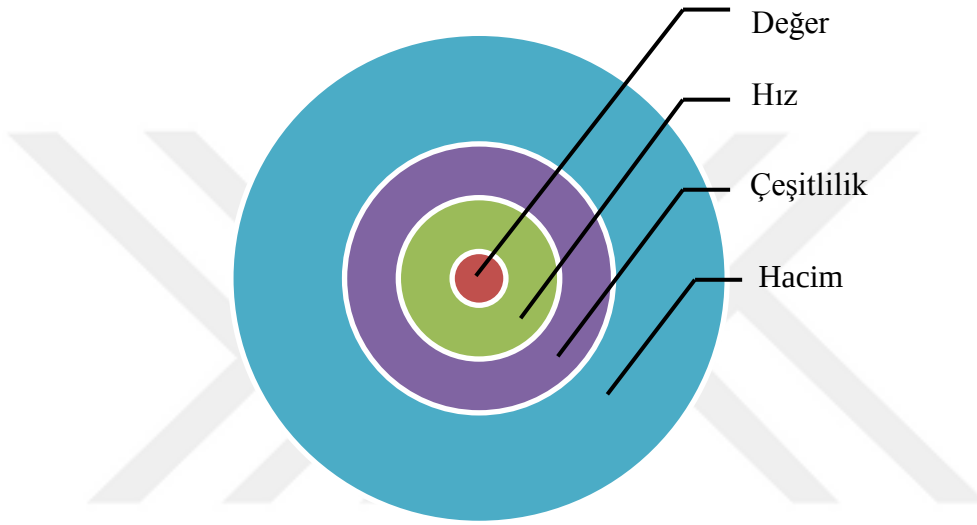
Büyük Veri, “V” harfi ile başlayan İngilizce üç terimin baş harflerinden oluşmaktadır ve 3V olarak tanımlanmaktadır. Bunlar; Volume (hacim), Variety (çeşitlilik), ve Velocity (hız)’dır. Sosyal medya, sensör verileri, Nesnelerin İnterneti (IoT) gibi seri halde ve sürekli veri üretebilen teknolojilerin sayesinde veri hacmi gün geçtikçe artmaktadır. Veri hacminde o kadar büyük artışlar yaşanmaktadır ki, yalnızca son iki yılda üretilen veriler dünya üzerinde şimdiye kadar üretilmiş verilerin %90’ını kapsamaktadır (Marr, 2018 Akt: Yılmazel, 2019, s. 159). Yılmazel (2019) Büyük Veri’nin temel bileşenleri olan üç V’yi şu şekilde açıklamaktadır;

- *Volume* (Hacim): Verilerin üstel büyümesi sayesinde ve yalnızca metin verilerinin değil birçok tipteki verinin saklanması/depolanmasından dolayı büyük hacimler oluşmaktadır. Yüksek kalitede ve detaylı videolar, müzikler, görsel malzemeler veri boyutlarını Terabayt ve Petabayt mertebelerine ulaştırmıştır. Veri büyüdükçe veriyi desteklemek için inşa edilen mimari altyapı ve bu altyapı üzerinde çalışan uygulamaların sık sık gözden geçirilmesi gerekmektedir. Büyük hacim, bu boyutuyla Büyük Veriyi temsil etmektedir.
- *Variety* (Çeşitlilik): Farklı veri formatları, veri semantiği ve veri yapı türlerini ifade etmektedir. Çeşitlilik, Büyük Veri içerisindeki veri çeşitliliğini çözümlemek ve yönetmek için farklı teknikler sağlamaya yöneliktir. Geleneksel olarak yapılandırılmış tek tip verilerin ve veritabanlarının yanı sıra artık web sayfaları, sosyal medya siteleri, e-postalar, belgeler ve sensör cihazları verileri gibi yarı yapılandırılmış veya yapılandırılmamış veri çeşitliliği de mevcuttur.
- *Velocity* (Hız): Veri yoğunluğu ve içeriklerin çok hızlı bir şekilde değişmesinden dolayı veriyi artık anlık olarak takip etmemiz gereken bir süreçteyiz. Veri hareketlerinin gerçek zamanlı olması gerekliliği veri güncellemesini saniyeler mertebesine indirmektedir (s. 162).

Bu üç bileşen için herhangi bir öncelik ya da üstünlük sıralaması bulunmamaktadır. Her bir bileşen kendi başına önemlidir ve Büyük Veri’yi tanımlamaktadır. Büyük Veri’den verimli bir şekilde yararlanabilmek için temel

oluşturan bu üç bileşenden mümkün olabildiğince en üst seviyede ve eş zamanlı fayda sağlamak gerekmektedir. Şekil 32’de görüleceği üzere, bazı çalışmalarda 3V’ye ilaveten dördüncü bir V (Value = Değer) önerilmektedir. Burada geçen dördüncü V’yi “değer” içermesi ve verinin kıymetli olması sebebiyle *veri-enformasyon-bilgi-bilgelik* piramidi sıralamasındaki bilgelik katmanına denk düştüğünü söylemek mümkündür.

Şekil 32. Büyük Veri’nin Bileşenleri



Kaynak: Marr, 2018 Akt: Yılmazel, 2019, s. 159’den uyarlanmıştır

Büyük Veri’nin günümüzde hangi boyutlara ulaştığını genel olarak anlayabilmek için Marr (2018b)’ın derlemiş olduğu şu verilere bakmak uygun olacaktır:

- Yaklaşık 3,7 milyardan fazla insan interneti kullanmaktadır.
- Google her saniye ortalama 40.000’den fazla arama işlemektedir. Bu, günde 3.5 milyar arama demektir. Diğer arama motorları ile bu rakam 5 milyara çıkmaktadır.
- Dakikada 16 milyon kısa mesaj gönderilmektedir.
- Dakikada 156 milyon e-posta gönderilmektedir. 2019 yılında, dünya genelinde 2,9 milyar e-posta kullanıcısı olması beklenmektedir.
- Dakikada yaklaşık 100 milyonun üzerinde istenmeyen e-posta (*spam*) gönderilmektedir.

- Dakikada 150 bin'in üzerinde Skype görüşmesi gerçekleştirilmektedir.

Domo'nun *Data Never Sleeps 5.0* Raporuna göre ise *her bir dakikada*;

- Snapchat kullanıcıları 527.760 fotoğraf paylaşmaktadır.
- 120'den fazla kişi LinkedIn'e katılım sağlamaktadır.
- Kullanıcılar 4.146.600 YouTube videosu izlemektedir.
- Twitter'da 456.000 tweet gönderilmektedir.
- Instagram kullanıcıları 46.740 fotoğraf paylaşmaktadır.

Facebook istatistiklerine bakacak olursak;

- Facebook'un 2 milyar kullanıcısı bulunmaktadır. Bunlardan 1.5 milyarı günlük olarak aktiftir.
- Her saniye 5 yeni Facebook hesabı açılmaktadır.
- Günlük 300 milyon fotoğraf yüklenmektedir.
- Dakikada 510 bin yorum yazılmaktadır.

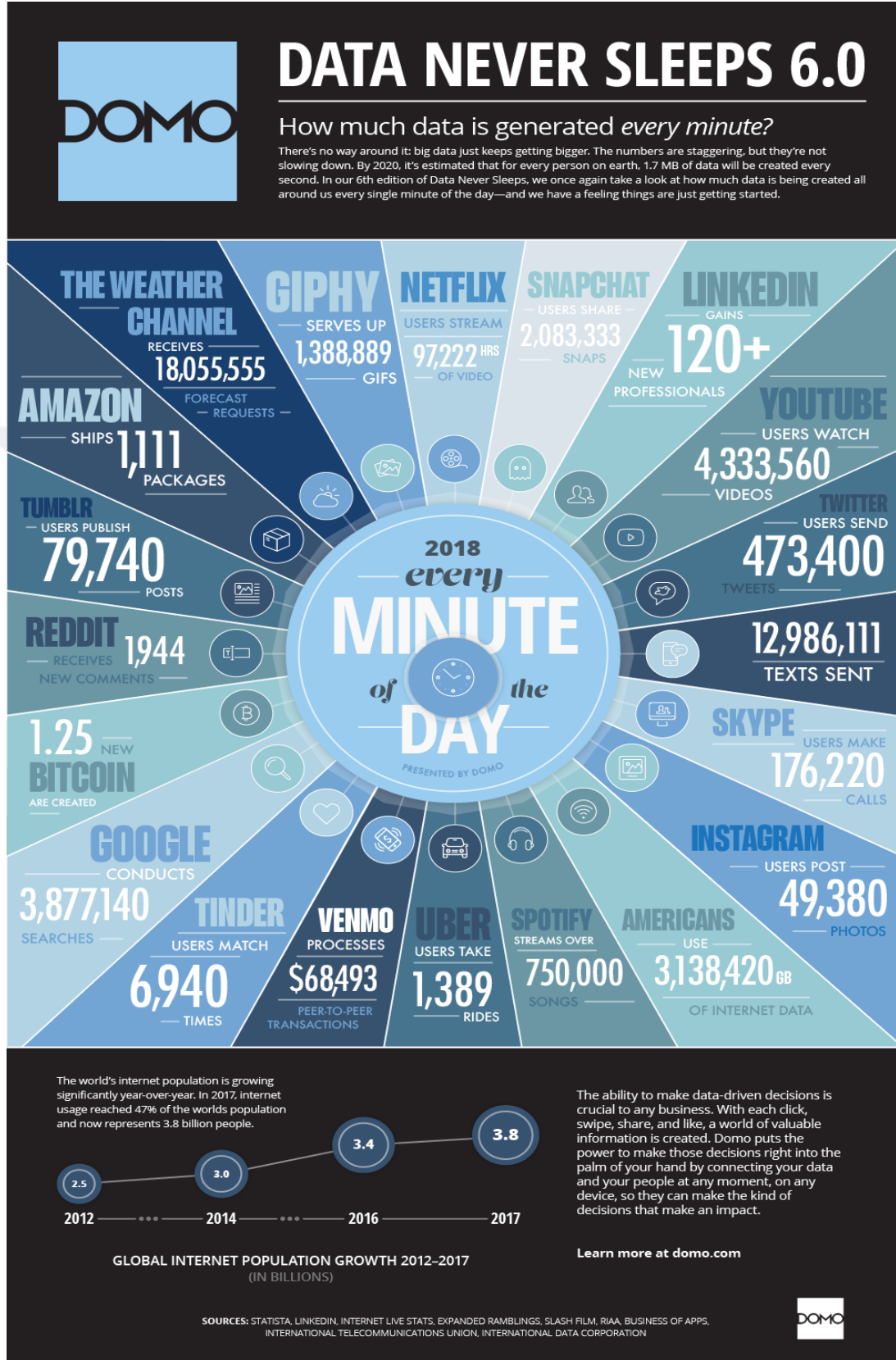
Instagram verilerine bakacak olursak;

- 600 milyon Instagram kullanıcısı bulunmaktadır. Bunlardan 400 milyon kadarı günlük olarak aktiftir.
- Instagramda günlük 95 milyon resim ve video paylaşılmaktadır.
- Instagram'ın "hikâyeler" kısmını günlük olarak 100 milyon kişi kullanmaktadır.

Yukarıda istatistik rakamları verilen ve ağırlıklı olarak sosyal medyayı kapsayan bu veriler Büyük Veri'nin oluşumunda yalnızca bir bölümü temsil etmektedir. Bunlara ilave edilecek olan sensör verileri, GPS verileri, makinelerden üretilen veriler (örneğin uçuş esnasında yaratılan uçuş verileri) ve daha saymakla bitmeyecek yüzlerce veri kaynağını düşünecek olursak, Büyük Veri'nin gerçekten "Büyük" olduğu gözlerden kaçmamalıdır. Veri analitiği ve bu verilerin yorumlanması ise bir sonraki adımı oluşturmaktadır.

Şekil 33'de Domo'nun 2018 yılına ait *Data Never Sleeps 6.0* Raporuna göre *bir dakikada* üretilen verilere yönelik istatistiksel rakamlar yer almaktadır.

Şekil 33. Data Never Sleeps 6.0 Raporu



Kaynak: <https://www.domo.com/learn/data-never-sleeps-6>, Erişim: 08.05.2019

Büyük Veri analitiği, bireylerin daha iyi kararlar almasına yardımcı olacak bilgileri sağlamanın ötesine geçecektir. Yakında, Endüstriyel Nesnelerin İnterneti (IIoT) analitiği karar veren makineler ile daha fazla otomasyon içerecek, insanlar ise süreçleri izleyerek gerektiğinde müdahalede bulunacak (Moskvitch, 2018, s. 70).

Analitiğin her zaman üç tipi olmuştur, bunlar; geçmiş hakkında bilgi veren *açıklayıcı analitik*, geleceği tahmin etmek için geçmiş verilere dayalı modeller kullanan *öngörücü analitik* ve optimal davranış ve aksiyonları belirlemek için modeller kullanan *normatif analitik*'tir (Davenport, 2014, s. 215). E 4.0 çatısı altında Büyük Veri analitiği (Analitik 3.0) ise bu üç analitiğin tamamını kapsamaktadır. Analitik 3.0'ın bu şekilde kullanımı işletmelere planlama, karar verme ve uygulama aşamalarında büyük katkılar sunmaktadır. Davenport (2014)'a göre Büyük Veri (dolayısıyla onun üzerinde konuşlanan veri analitiği) sadece daha iyi ve hızlı kararlar ile maliyet tasarrufu için değil, aynı zamanda müşteriler için veriye dayalı yeni ürün ve hizmet yaratmak için de kullanılmaktadır. Bu beceriler, liderlik, örgütsel yapı, teknoloji ve mimaride değişim anlamına gelmektedir (s. 216).

Klasik manada *analitik*; pazarlama, satış ve hizmet gibi süreçleri anlamak, düzenlemek, yönetime bilgi vermek ve yönetimi aykırılıklara karşı uyarmak amacıyla kullanılıyordu. Bu doğrultuda şirketler, performansları değerlendirip iyileştirmeler planlıyor ve bu iyileştirmeleri aylara ve yıllara yayılan teknoloji projeleriyle hayata geçiriyordu. Oysa Büyük Veri bu durumu tam tersine çevirerek sürekli bir değişim ve akış halindeki veriyi hızlı bir şekilde takip ederek tepki veriyor ve kuruluşları avantajlı hale getiriyor. Büyük Veri araçları ve teknolojileri ile çalışan veri bilimciler, görülmemiş bir ölçek ve hızda hem var olan mevcut veri kaynaklarını hem de yeni kaynakları sürekli araştırarak fırsatları yakalamaya çalışıyor (Davenport, 2014, s. 25). Büyük Veri yığınları, karışık ve karmaşık yapılar içermesi nedeniyle geleneksel veri tabanı ve dosya sistemlerinden farklılaşmaktadır. Bu yığınların analiz edilmesi, ayıklanması ve işlenmesi amacıyla “analitikler” adı verilen özel analiz ve yorumlama yazılımları kullanılmaktadır (Banger, 2018b, s. 40). Davenport (2014, s. 135) bu yazılımlardan bazılarını şu şekilde listeliyor:

Apache Pig ve Hive, Hadoop kullanarak uygulama kodlarında MapReduce fonksiyonlarının yürütülebilmesi için üst seviye bir dil sağlayan iki açık kaynaklı betik¹¹ dildir. Pig veri okumak, filtrelemek, dönüştürmek, birleştirmek ve yazmak gibi işlemleri tarif etmek için bir betik dil sunuyor; bu Java'dan daha üst seviyede bir dil ve programlamada daha fazla üretkenliğe olanak tanıyor. Diğer bazı kuruluşlar bunun için açık kaynaklı Python betik dilini kullanıyor. Hive aynı işlevleri daha fazla toplu işlem (batch) yönelimiyle gerçekleştiriyor ve veriyi Yapılandırılmış Sorgu Dili (Structured Query Language - SQL) sorgularına uygun ilişkisel formata çevirebiliyor. Bu Hive'i SQL sorgu diline hâkim analistler için işlevsel hale getiriyor.

Google'ın üretmiş olduğu Dremel isimindeki Büyük Veri analiz aracı ile yapılan test çalışması sonucunda 35 milyar satırın bir indeks kullanılmadan yalnızca saniyeler içerisinde tarandığı belirtilmiştir. Müşterilerin hangi ürünlere talep göstereceği, kasko yaptıran müşterinin ne zaman kaza yapabileceği, şirket satışlarının dönemsel artış ya da azalışları gibi pek çok sorunun yanıtı R ve benzeri araçlar kullanılarak yanıtlanabilmektedir. Makine öğrenimi ile elde edilen öngörülerle de suistimal yönetimi, mevcut donanımlarda oluşabilecek arızaların önceden tahmini, metin tabanlı duygu analizi, kredi puanlama ve fiyatlandırma modelleri gibi senaryolar geliştirilebilmektedir (Özdoğan, 2016, s. 41-44).

Büyük Veriyi kimler kullanıyor diye baktığımızda yelpazenin oldukça geniş olduğunu görebiliyoruz; duygusal paylaşımların araştırılmasından elektrik tribünlerinin verimlilik optimizasyonuna kadar kullanıldığına şahit oluyoruz. Davenport (2014)'un bu konuyla ilgili olarak vermiş olduğu örneklerle bakacak olursak; Google veri bilimcileri, temel arama ve reklam yerleştirme algoritmalarını ilerletmek için, Netflix, şirketin müşterilerine sunduğu film önerilerini optimize etmek için, sınav şirketi Kaplan, müşterilerine etkin öğrenme ve sınavlara hazırlanma stratejileri önermek için (s. 23), *duygu analizi* uygulaması bloglarda, tweetlerde ve Facebook sayfalarında bir kuruluşun marka ürünleri hakkında yapılan yorumların nette olumlu veya olumsuz olduğunun belirlenmesi için, BM'nin Global Pulse inovasyon laboratuvarında gerçekleştirdiği Hunch Works aracıyla izlemeye yönelik kullanımını (s. 24) görmekteyiz. General Electrics ise Büyük Verinin önde gelen kullanıcılarından; şirket izlenen tribünlerde en az %1 verim artışı elde edebileceğini,

¹¹ Betik Dil: Web sayfalarında dinamik içerik sağlamak için kullanılan ve istemci (client) tarafında çalışan bir dildir.

bunun gelecek on beş yılda 66 milyar dolarlık yakıt tasarrufuna denk gelebileceğini tahmin etmektedir (s. 32).

Büyük Veriyi değerli kılan unsur, milyonlarca bireysel katılımcı ve kaynaktan gelen, analiz edilebilen benzerlikleri bulmak, anlamlandırmak ve sorunları çözmek için kullanılabilen veri ve enformasyonlardır. Dağıtık ve işbirlikçi bir toplumda kolektif bilgi hazinesine verileriyle katkıda bulunan milyonlarca insan, verilerinin belli bir azınlık tarafından kontrol edilen ve fikri mülkiyet hakkına tabi bir meta olmasındansa açık ortak kaynaklar üzerinde herkesin faydalanabileceği şekilde paylaşılmasını giderek artan bir ısrarla talep etmektedir (Rifkin, 2015, s. 196). Bu talep için, Blockchain teknolojisinin dağıtık ve büyük oranda merkezi olmayan yapısıyla benzer özellikler taşıdığını söylemek mümkündür. Yeni teknoloji ve üretim süreçlerinin maliyetleri minimize etmesinin yanı sıra insanlığın ortak faydasına sunabileceği katkılarının da olmasını ummak bireysel ve toplumsal talepler açısından oldukça değerli ve ayrıca gereklidir.

Büyük Veri'nin endüstriyel kullanım sektörü olarak; bankacılık, iletişim, medya, eğlence, havacılık, savunma, otomotiv, sağlık, eğitim, adalet, spor, üretim ve kamu gösterilebilir. Veri nerede yoğun ise Büyük Veri'nin kullanımı orada söz konusudur (Özdoğan, 2018, s. 83). Davenport (2014) ise Büyük Veri'nin sektörel kullanımının şu sektörler daha uygun olduğunu ifade etmektedir; sağlık hizmetleri, firmadan firmaya hizmet veren şirketler, firma aracılığı ile müşteriye hizmet veren şirketler, endüstriyel ürün firmaları, telekom firmaları, medya ve eğlence firmaları, bankalar ve elektrik sağlayıcıları (s. 51-58). Şekil 34'de bu sektörler görsel olarak da verilmiştir. Kritik iş birimleri dikkate alındığında ise Davenport (2014) sıralamayı şu başlıklar altında topluyor ve açıklıyor; pazarlama, satış, tedarik zinciri, üretim, insan kaynakları, strateji ve finans (s. 59-63).

Pazarlama: Pazarlama amacıyla kullanılan yeni veri kaynakları arasında müşterilerin sosyal, mobil ve konum verileri.

Satış: Müşteri ilişkileri yönetimi (CRM) ve çağrı raporlama, toplam satış tahminleri, satış sorumlularının vakitlerini nasıl geçirdikleri.

Tedarik Zinciri: GPS takibi ile kargo takipleri ve kesin varış zamanlarının izlenmesi, RFID ve telematik algılayıcılar ile konum takibi, nem, doluluk oranları,

ışık, sıcaklık, eğim açısı, paketlerin açılıp açılmadığının kontrolü gibi değişkenlerin izlenmesi.

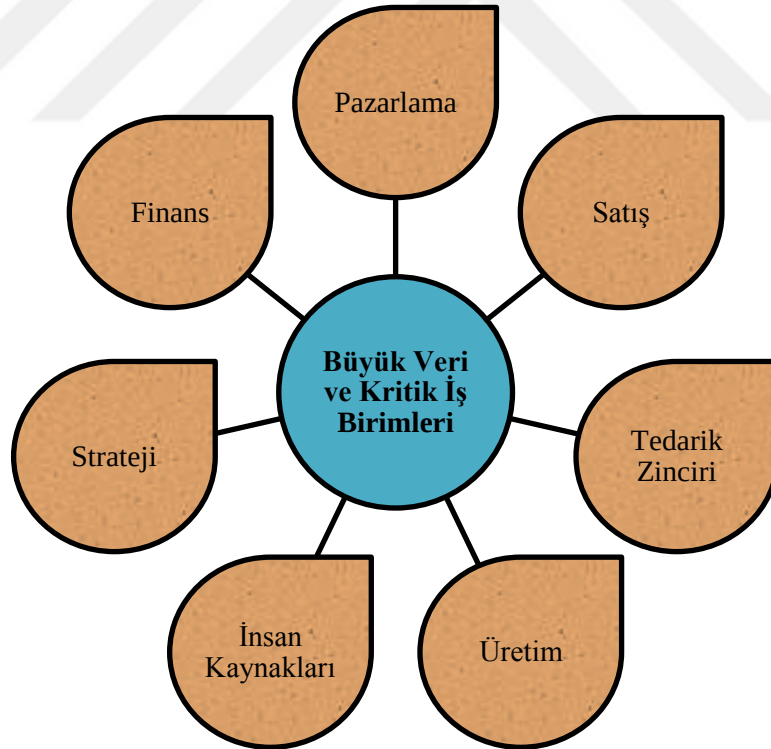
Üretim: Algılayıcılar (sensörler) sayesinde mekanik işleme, lehimleme cihazları ve robot aygıtların performans ve kendi bakım ihtiyaçları hakkında raporlama.

İnsan Kaynakları: Çalışanların konum ve iletişim verilerinin analizi, çalışanların iş birliği ve iletişim faaliyetlerinin analizi.

Strateji: Stratejik kararlar alınırken artık büyük ölçekli dış veri kullanmamak stratejik hata olarak kabul ediliyor ve değerlendiriliyor. Sadece kendi tecrübe ve kurum içi bilgilerine güvenilmesi bir strateji uzmanı için yetersizlik demektir.

Finans: Borsacılar ve risk yöneticileri alım satım fırsatlarını belirlemek veya yatırım ve varlıkların değer kaybetme ihtimalini değerlendirmek için muazzam miktarda veri işleyerek finansal korumayı sağlayabilmektedir.

Şekil 34. Büyük Veri ve Kritik İş Birimleri



Kaynak: Davenport (2014, s. 59-63)'dan uyarlanmıştır

3.2.2 Bulut Bilişim (*Cloud Computing*)

E 4.0 teknolojilerinden bir diğeri bulut bilişimdir. Bulut bilişim, internet tabanlı bir bilgi işlem yaklaşımı olup, işlerin ve iş süreçlerinin büyük bir ağ üzerinde paylaşılarak, verileri depolama görevi ve istenilen bilgilerin (zamandan ve mekândan bağımsız olarak) istenilen yerde elde edilmesini, yani yetkili erişimini sağlamaktır. E 4.0'ın temel özelliklerinden bir diğeri de veri ve bilgilere ulaşmada ve onları kontrol etmede sınırları kaldırmasıdır. Bulut bilişim işte bu işleyişin gerçekleşmesinde önemli araçların başında yer almaktadır (Öztuna, 2017, s. 121).

Bulut bilişim'i (bulut) yalnızca verilerin tutulduğu ortak ve kapsamlı mekânlar olarak görmemek gerekir. Bulut, veri tabanlarının tutulmasının yanı sıra çeşitli servis hizmetleri de sunmaktadır. Bulutu çözüm ortaklığı olarak görmek de uygundur. İşletmelerin yalnızca donanımsal ihtiyaçları değil aynı zamanda yazılım ve uygulama (software & application) ihtiyaçları da bulut üzerinden çözüme kavuşturulabilmektedir. Kendi başına ve bağımsız olarak teknolojik ihtiyaçlarını (maddi ve insan kaynağı yönünden) karşılayamayacak olan işletmeler, özellikle KOBİ'ler için çözüm ortaklığı sunan bulut'u, Büyük Veri için veri ambarı, kesintisiz hizmet, veri yedekleme, veri tabanlarının kiralanması, ERP gibi çeşitli yazılımların kullanımı için aracı hizmet sağlayıcısı olarak da görmek gerekir. Bulut'a, işletmeler için bir tür dış kaynak kullanımı (outsourcing) aracı da diyebiliriz. Bulut ile ilgili olarak yazılım ve veri güvenliği ise henüz netlik kazanmış bir konu değildir. Şöyle ki; donanımsal ve yazılımsal yeterliliği itibarıyla bulut üzerinden yapılan hizmetler ve veri güvenliği, işletmelerin kendi başlarına sağlayacaklarından çok daha verimli olabilir fakat buna karşın kurumsal ve müşteri ile ilgili verilerin dışarıda (üçüncü parti) tutuluyor olması akıllara güvenlik açığı ile ilgili soruları getirmektedir. Özellikle bu bağlamdaki güven sorunu yeterince aşılabılırsa bulut kullanımının daha da yaygınlaşabileceğini söylemek mümkündür.

Bulut bilişimde en önemli noktalardan bir diğeri, işletmenin ihtiyacı olan bir hizmeti hızlı bir şekilde kullanıma geçirebilmesidir. Normalde haftalarca sürecektir bir donanım tedarikinin ardından bu donanıma bir işletim sisteminin kurulması, üzerinde uygulama çalıştırmak ve bu uygulamayı ilgili kullanıcılara açmak (Özdoğan, 2018, s. 84) ve ayrıca çeşitli güvenlik testlerinden geçirerek yeterliğini onaylamak çok uzun zaman alabilmektedir.

Bulut bilişim için göze çarpan avantaj ve dezavantajlar genel hatları ile Şekil 35’de düzenlenmiştir.

Şekil 35. Bulut Bilişim’in Avantaj ve Dezavantajları



2014 yılının başlarında Google, bulut depolama hizmetlerinin fiyatını neredeyse %70 oranında düşürerek gigabayt başına fiyatı 0,026 dolara çekti. Bu hamle endüstride şok etkisi yaratırken, Amazon ve Microsoft gibi diğer depolama devleri de fiyat düşürme savaşına katıldılar. Böylesine uygun fiyatlı kaynakların kolaylıkla erişilebilir hale gelmesi ve SaaS (Hizmet olarak Yazılım) uygulamalarının da gün geçtikçe artması, kişisel verimlilik, girişimcilik ve inovasyon alanlarında birçok olumlu etkiler yaratmayı başardı. Bu gelişmeler ise bulut bilişime doğru kaçınılmaz geçişi hızlandırdı. Ancak tüm verileri buluta taşıma hareketi, beraberinde her zaman olduğu gibi yeni riskler de getirdi. Sonuç olarak yüz milyonlarca hesabın çalınması, sadece verilerin tek bir sanal ortamda tutulması sebebiyle meydana geldi.

Bulut, bireyler ve kurumlar için olduğu kadar suçlular için de oldukça kullanışlı bir platform oluşturdu (Goodman, 2016, s. 13).

3.2.3 Yapay Zekâ (*Artificial Intelligence - AI*)

Zekâ, sınırlı kaynaklarla sorun çözme becerisi olarak tanımlanabilir ki, buradaki en önemli kaynak zamandır. Zekâ, insanın hayatta kalma mücadelesi için faydalı olduğundan evrimleşmiştir. Kendi türümüz tarafından uygulandığı gibi bu beceri sadece gezegenimize hâkim olmamızı değil, hayatımızın kalitesini sabit bir şekilde artırmamızı da sağlamıştır (Kurzweil, 2019, s. 238). İnsanoğlunun zekâ konusundaki beklenti ve öngörülerini benzer bir şekilde yapay zekâ için de söylemek mümkündür.

Yapay Zekâ (YZ), doğal sistemlerin yapabildiği her bilişsel etkinliği yapay sistemlere, daha da yüksek başarımlı düzeylerinde nasıl yaptırabileceğimizi inceleyen bilim dalıdır (Say, 2018, s. 83). YZ, makineler tarafından sergilenen zekâ türüdür. YZ, bir bilgisayarın veya bilgisayar denetiminde çalışan bir makinenin çeşitli faaliyetlerini zeki canlılara benzer şekilde yerine getirme yeteneğidir. YZ genel olarak insanın düşünme biçimini taklit ederek bunlara benzer yapay yönergeleri geliştirme üzerine kurulmuştur (Banger, 2018b, s. 35). Genel olarak YZ'nin amacı; makineleri daha akıllı ve daha yararlı duruma getirmek ve zekânın ne olduğunu anlamak şeklinde sınıflandırılabilir (Yılmaz, 2017, s. 5).

E 4.0'ın temel niteliklerinden olan toplumsal dönüşüm ve insansız imalat ortamının oluşturulabilmesindeki en büyük etkenlerden birini YZ çalışmaları oluşturmaktadır. YZ teknolojisinin temel amacı bilgiyi anlayabilen, işleyebilen, olaylar arasında ilişki kurabilen ve kendi başına (otonom) kararlar verebilen, örgüleri öğrenebilen, planlama ve muhakeme yapabilen, problemlere kendi sahip olduğu ve olmadığı (yapay sinir ağları sayesinde) bilgileri kullanarak çözümler üretebilen algoritmalarla bilgisayar sistemleri oluşturmak olarak tanımlanabilir (Öztemel, 2018, s. 82).

YZ insanlar için başka işler yaratılmasını (şu ana kadar var olmayan yeni iş kollarının ortaya çıkmasını) da sağlayabilir. İnsanlar YZ ile yarışmak yerine YZ'nin idame edilmesi ve desteklenmesine odaklanabilir. Örneğin insan pilotların yerini insansız uçakların almasıyla bazı meslekler yok olurken bakım, onarım, uzaktan kumanda, veri analizi ve siber güvenlik alanlarında yeni iş olanakları doğabilir. ABD

silahlı kuvvetleri insansız uçakların uçurulmasında uçak başına otuz kişiye ihtiyaç duyuyor ve uçuşların sonucunda topladıkları bilgilerin analizi için en az seksen kişi daha gerekiyor (Harari, 2018, s. 43). Bu durum tek başına yeterince açıklayıcı bir örnek olmasa da benzer durumlar başka alan, uygulama ve meslekler için de geçerli gözüküyor. Sonuç olarak, yok olacak birçok mesleğin yanı sıra şimdiden hayal edilemeyecek onlarca yeni mesleğin türeyeceği mümkün gözükmektedir. Ancak, Harari (2018) insanlar için pek çok yeni meslek ortaya çıksa da “işlevsiz” bir sınıfın doğmasına tanıklık edebileceğimiz görüşünde ve bu durumun iki yönlü bir sorun teşkil edeceğini öne sürmektedir. Bir tarafta yüksek işsizlik sorunu diğer tarafta ise nitelikli eleman sıkıntısı (s. 44) olacağını öngörmektedir. Bu yaklaşımın doğru olabileceğini varsayacak olursak, genç nesillerin BT ile daha çok içli dışlı olmaları gerekecektir hatta bu durum bir zorunluluk haline gelebilecektir. “Eski model” insanların yeni yüzyılda ıskartaya çıkabileceği riski her zaman mevcut gözükmektedir. Bu durum insanları yeni bir sınıflaşma sorunu ile karşı karşıya bırakabilir.

Stockfish 8 adlı program 2016 yılının bilgisayar şampiyonu ilan edildi. 2017 yılında ise Google’ın AlphaZero programı Stockfish 8’i yendi. İnsan ve bilgisayar satranç deneyimini kullanabilen Stockfish saniyede 70 milyon satranç hamlesi yapabilirken AlphaZero sadece 80 bin hamle yapabiliyordu. AlphaZero’nun yaptığı, en son makine öğrenmesi prensiplerini kullanmasıydı. Satrancı kendi kendine oynayarak öğrenmişti ve buna rağmen Stockfish karşısında yüz oyundan yirmi sekiz galibiyet, yetmiş iki beraberlik ve sıfır yenilgi ile ayrılmayı başarmıştı (Harari, 2018, s. 45). YZ, daha güçlü bilgisayarlar, daha gelişmiş ve daha hızlı hesap gücü demek değildir. Bu fark etmemiz gereken önemli bir ayrıntıdır. Moore Yasası’nın sekteye uğraması YZ’nin önünde bir engel gibi durmamakta.

İnsanların çoğu, özellikle eğitilmiş ve tecrübeli kişiler kendi kararlarından hiç şüphe etmemektedir. Yapılan araştırmalara göre, yeni restoran açan girişimcilerin %81’i kesin başarıya ulaşacaklarını düşünmektedir. Oysaki restoran işinde başarı oranı sadece %5’tir. Amerika’daki bazı büyük hastaneler artık doktorların sadece kendi bilgi ve tecrübelerine dayanarak teşhis koymalarına müsaade etmemektedir. Çünkü dünyada tıp ve teknoloji alanındaki tüm gelişmeleri takip etmek için bir doktorun haftada 48 saat literatür okuması gerekmektedir. Bu nedenle IBM’in

Watson ismindeki YZ algoritmaları bu hastanelerde kullanılmaya başlandı. Gerekli tüm tetkik ve tahlil sonuçları bilgisayara yüklenerek Watson'un en güncel bulguları da taraması sayesinde en uygun tedavi için doktorlara tavsiyelerde bulunuyor (Pağda, 2018, s. 107). YZ'deki ilerlemeler bir taraftan verimlilik ve üretkenliği arttırırken diğer taraftan insan emeğine olan ihtiyacı azaltabildiğinden artık birçok farklı alanda ve meslekte kullanılabiliyor. EDiscovery adında bir bilgisayar yazılımı milyonlarca hukuki belge içinde tarama yaparak davranış kalıplarını, fikir silsilelerini, kavram ve benzeri şeyleri o kadar yüksek hızda yapabiliyor ki en iyi avukatları gölgede bırakabiliyor. Bu program insan gözünden kaçan ayrıntıları yakalayabiliyor ve yüksek oranda emek tasarrufu sağlıyor (Rifkin, 2015, s. 140).

YZ'nin ana hedeflerinden birisi öğrenebilmedir. Öğrenerek elde edilen tecrübeyi simüle edebilmektir. Kapsamlı veri üzerinde kullanılan algoritmalar sayesinde artık makinelerin öğrenmesi sağlanabiliyor. Öğrenmenin yanı sıra muhakeme, problem çözme, algı, dil işleme gibi insana özgü becerilerin makinelere taşınabilirliği de bu alana girmektedir (Özdoğan, 2018, s. 91-92). YZ ve öğrenmeye diğer bir destek ise yapay sinir ağları aracılığı ile sağlanmaktadır. Karmaşık ve doğrusal olmayan problemlerin çözümünde kullanılan yapay sinir ağları özellikle büyük (hacimli) verilerin yorumlanmasında önemli avantajlar içermektedir. Tek doğru çözüm yerine mevcut durum için en doğru (optimal) ve en hızlı çözümü üretebilen yapay sinir ağları makine-insan ara yüzü için önemli bir destek sağlamaktadır. Kuantum bilgisayarların işlem gücü (hızı) ve teknikleri ile yapay sinir ağlarının birlikte kullanılması yakın gelecekte hesaplamaların daha kolay, hızlı ve güvenilir yapabileceğini söylemek mümkün. İnsan faktörü kısa ve orta vadede karar alma aşamasında halen var olacak olsa da YZ, yapay sinir ağları ve kuantum bilgisayarların “yeni sürece” vereceği destek büyük bir boşluğu dolduracak, yarı otonom sistemlerden tam otonom sistemlere ve otonom robotlar dönemine geçişin ön evresini oluşturacaktır.

Hastanın elini tutup onu hastalığıyla nasıl mücadele edeceği konusunda bilgilendirirken yüreklendirme sanatı gibi tıbbın insan dokunuşuna olan ihtiyacı (Say, 2018, s. 148) hâlâ devam ediyor olsa da, yakın gelecekte bu durum büyük oranda YZ lehine değişecektir.

3.2.4 Bulanık Mantık (*Fuzzy Logic*)

Klasik mantık var olan her veriyi 0 ya da 1 olarak ifade ederken, bulanık mantıkta bu ifadeler 0 ile 1 arasındaki ara değerlerden oluşmaktadır. Kesinlik içermeyen çıkarım ve durumlarda bulanık mantık devreye girerek dilsel kavrayışa, gündelik yaşama ve insanın karar verme süreçlerine daha yakın olduğu düşünülen bir yaklaşım ortaya koymaktadır.

İki değerli kümeler kesin (*grips*) kümeler olarak adlandırılmaktadır. Bilgisayarlar iki değerli kümeyi kullanarak ikili mantıktan yararlanır. Fakat gerçek hayatta bir nesnenin hangi kümeye ait olduğu tam kesinlik göstermeyebilir. Örneğin; bir masanın üzerinde bir tabak elma olduğunu farz edelim. Bu durumda, “tabaktakiler elma mı?” sorusuna “evet”; “tabaktakiler armut mu?” sorusuna ise “hayır” cevabı verilecektir. Peki, tabaktaki elmaların arasında bir veya bir kaç tane armut olduğunu varsayalım. O zaman yukarıdaki sorulara kesin küme teorisi açısından nasıl cevap verileceği açık değildir. “Tabaktakiler elma mı?” sorusuna “belki tam değil”, “çoğunluğu elmadır”, “bir tanesi armut, diğerleri elmadır”, “bir kaç tanesi armut, diğerleri elmadır” gibi cevaplar verilebilir (<http://farabi.sutef.gen.tr/bulanik/bulanik/bolum02.htm>), işte bu şekilde tanımlama bulanık mantık yaklaşımıdır.

Bulanık mantıkta, çoğu zaman, gerçek fiziksel dünyada karşılaşılan nesnelerin sınıflarının tam olarak tanımlanmış üyelik kriterleri yoktur. Örneğin; hayvan sınıfı net bir şekilde köpekler, atlar, kuşlar vb. içerirken, kayalar, sınırlar, bitkiler vb. nesneleri kati bir şekilde içermez. Ancak, denizyıldızı, bakteri gibi bazı nesneler ise belirsiz bir statüye sahiptirler (Zadeh, 1965). Bu bulanıklığı gidermek için Zadeh, örneğin denizyıldızını biraz hayvanlar biraz bitkiler sınıfına sokmayı önermekte. İnsan beyninin çalışma sisteminin benzetimi çalışmaları sonucunda ortaya çıkan ve YZ’nın alt dallarından biri olan bulanık mantık, bulanık küme teorisine dayanan matematiksel bir sistemdir (Eğrisöğüt ve Kazan, 2007).

Bulanık mantık; görüntü işleme, zaman serilerinde tahmin yapma, haberleşme, mühendislik, tıp, sosyoloji, psikoloji, kavşak sinyalizasyonu, işletme, ulaştırma ve YZ gibi alanlarda kullanılmaktadır (Gürel, 2017, s. 130).

Bulanık (fuzzy) mantık, sözel ifadelerle karar verebilme mekanizmasının kati olmayan sınırlar çerçevesindeki işleyişini matematiksel olarak modellemede

kullanılmaktadır. Burada yer alacak kümeler kesin (*grips*) olmayan kümelerden oluşacağından bu kümeler bulanık (*fuzzy*) olarak adlandırılmaktadır. Çeşitli aşamalardan geçirilen bu süreç sonunda anlamlı sonuçlar elde edilebilmektedir. Bulanık mantıkta işlem süreci genel olarak şu şekilde sıralanmaktadır;

- Fuzzification (*Bulanıklaştırma*)
- Defuzzification (*Durulaştırma*)
- Tanımlama (*Bulanık Önermeyi İşleme*)

Birinci aşama bulanık olmayan değişkenlerin üyelik fonksiyonlarının ve operatörlerinin belirlenerek bulanık kümeyi oluşturmak için bulanıklaştırılmasından oluşur. İkinci aşama olan durulaştırmada ise, ilk aşamada oluşturulan bulanık sayı veya bulanık küme tam sayılara dönüştürülür ve bulanık sayılardan kesin sonuçlar oluşturularak karar vermede kullanılmak üzere hazır hale getirilir. Son aşamada ise, hazır hale getirilen bu sayılar kullanılmak üzere sisteme aktarılır. Eğer hazır hale getirilen bu sayılarda tek bir sonuç elde edilemediyse elde edilen en yüksek değerlerin ortalaması alınır ya da oluşan çözüm alanına ait ağırlık merkezi alınarak çözüm değeri üretilir.

Bulanık mantık işlem sürecini daha somut olması açısından başka bir örnekle şu şekilde de açıklayabiliriz. Bulanıklaştırma aşaması, elemanın üyelik fonksiyonundaki yerini kesin olmayan hatlarla belirlemedir. Örneğin: 25 yaşında olan birisi, büyük bir oranda “yetişkin”, kısmi bir oranda da “genç” kümesinin elemanıdır. Bu durum yüzde olarak da belirtilebilir: %80 “yetişkin”, %20 “genç” vb. Bulanık karar verme aşaması, bulanıklaştırma aşamasındakine benzer ve mantık çerçevesi içerisinde sınıflamayı biraz daha daraltır; *IF <bulanık mantık> THEN <bulanık mantık>* şeklinde ifade edilebilir. Durulaştırma aşaması ise makine dilinin anlayabilmesi için sözel değerlerin tekrar sayısal değerlere veya değer aralıklarına çevrilmesi sürecidir. Durulaştırma işlemleri çeşitli yöntemler ve fonksiyonlar kullanılarak yapılmaktadır. Örneğin; gravity, ağırlık merkezi fonksiyonları vb. Genel olarak *ağırlık merkezi* dikkate alınır (Özmen, 2018).

Bulanık mantık'ın kullanımı bizler çok farkında olmasak da günlük yaşamdan endüstrinin çeşitli alanlarına kadar girmiş bulunmakta ve insan yaşamını daha konforlu hale getirmek, verimlilik, maliyetlerin düşürülmesi, güvenlik, stratejik karar verme ve yapay zekâ gibi birçok alanda kullanılmaktadır. Bulaşık makinelerinde bulaşık miktarına ve kirlilik seviyelerine göre hesap yaparak ne

şekilde yıkama yapılacağına karar vermede, fotoğraf ve fotokopi makinelerinde en iyi odaklanma ve görüntü almasında, metrolarda trenlerin daha az sarsıntıya sebebiyet verecek şekilde frenleme sistemlerinde, arabalarda otomatik vites şanzımanlarında geçiş zamanı ve sürelerinin ayarlanmasında, nükleer reaktörlerdeki soğutma ünitelerinde, yapay pankreas ünitelerinin insülin düzeyini belirleme ve daha onlarca alanda kullanılmaktadır. E 4.0 bileşenlerinden bir çoğuna, özellikle yapay zekâ'ya önemli katkılar sunan bulanık mantığın ilerleyen zamanlarda daha fazla kullanılacağı düşünülmektedir. Bulanık mantığın, yapay zekâ, yapay sinir ağları, otonom süreçler ve robotikte daha fazla kullanımı E 4.0 çatısı altında gerçekleşecek gözükmemektedir. Bu nedenle bulanık mantık yaklaşımı özellikle E 4.0 kapsamında daha fazla irdelenip değerlendirilmelidir.

Yılmaz (2017, s. 20-21), bulanık mantığın avantajlarını şu şekilde özetlemektedir;

- Günlük hayatta karşılaşılan durumlardaki gibi karmaşık, belirsiz, zamanla farklılaşan, eksik tanımlı sistemlerin çözümünü basitleştirir.
- Geniş bir uzaydaki giriş sinyalleri bile az sayıda üyelik fonksiyonu ile tanımlayabildiği için küçük bir yazılımla bile problemi çözebilir.
- Kural tabanı az sayıda kuraldan oluştuğu için, sonuca daha hızlı ulaşır.
- Doğrudan kullanıcı girişlerine ve uzman bilgi ve tecrübelerinden yararlanabilmesine olanak sağlar.

3.2.5 Nesnelerin İnterneti (*Internet of Things - IoT*)

Nesnelerin İnterneti; çeşitli haberleşme protokolleri sayesinde birbirleri ile haberleşen ve birbirine bağlanarak iletişim kurarak bilgi aktarabilen veya paylaşabilen akıllı bir ağ oluşturmuş cihazları temsil etmektedir. Kevin Ashton tarafından 1999'da ortaya atılan bu kavram ilk başta RFID etiketleri sayesinde radyo frekansı üzerinden birbirleriyle haberleşen cihazları kapsamaktayken gelişen teknolojik altyapı ve teknolojiler sayesinde konsept çok daha geniş bir vizyona sahip oldu. Bu konsept sadece evlerdeki eşyaları ya da yoldaki trafik ışıklarını değil, fabrikalarda üretim yapan makine parkurlarını da kapsamaktadır (Erbaşlar ve Dokur, 2016, s. 80). RFID teknolojisinin yanı sıra yakın zamanlarda NFC teknolojisi, barkodlar ve QR kodlar ve sensörler gibi yeni teknolojiler sayesinde Nesnelerin İnterneti kablosuz internet ve kablosuz haberleşme desteğiyle daha kapsamlı bir hal

almakta ve artık birçok cihaz akıllı mobil cihazlardan kolayca yönetilebilmektedir. Nesnelerin İnterneti sayesinde tüm bu cihazlar bir orkestra edasıyla hareket edebilmekte, yani eşgüdümlü çalışabilmektedir. Akıllı algoritmalar ve YZ sayesinde bu orkestra yakın gelecekte başlarında bir şef'e ihtiyaç duymadan da çalışmalarını devam ettirebilecektir.

Nesnelerin İnterneti (IoT), internet üzerinden veri toplayan ve ileten aygıtlara atıfta bulunur ve akıllı telefonlar, akıllı saatler, bileklikler, hatta televizyon ya da buzdolabındaki her veri ve iletişimi kapsar. IoT son yıllarda muazzam bir büyüme sağlamış durumdadır ve bu süreci daha işin başlangıcı olarak görmek mümkündür. Bugün internete bağlanan yaklaşık 13 milyar cihaz bulunmaktadır. 2020 yılı itibariyle bu rakamın 20 milyarın üzerine çıkacağı tahmin edilmektedir. Sadece akıllı telefon kullanıcılarının 2020 yılına kadar 6 milyardan fazla olacağı tahmin ediliyor. Akıllı cihazlar dünyayı, arabaları, evleri ve işleri değiştiriyor. 2020'ye gelindiğinde, çeyrek milyar kadar aracın internete bağlanacağı ve otomatik sürüş de dâhil olmak üzere tüm araç içi hizmetleri sunacağı öngörülüyor (Marr, 2018a, s. 4). Büyük Veri entegrasyonu ve analitiğinden de yararlanacak olan Nesnelerin İnterneti her türlü veri akışını kullanarak elektronik cihazların (makinelerin) birbirleri ile haberleşmesini (iletişimini) sağlayacak. Ayrıca, giyilebilir teknolojiler, sensörler, manyetik veri aktarımları, GPS, NFC ve benzeri uygulamalar da Nesnelerin İnterneti'nin parçasını oluşturmaktadır.

Birleşik Devletler Ulusal İstihbarat Yönetim Ofisi ve İç Güvenlik Departmanı, 2017 Kamu-Özel Analitik Değişim Programı, *Fidye Yazılım ve Sosyal Mühendisliğin Geleceği* başlıklı çalışmasında Nesnelerin İnternetini “akıllı” veya internete bağlı ortak veya ev tipi cihazları ifade eder şeklinde tarif ediyor. Akıllı telefonlar, kahve makineleri, giyilebilir cihazlar, çamaşır makineleri, tıbbi cihazlar ve araçları da buna örnek olarak gösteriyor.

Gartner'a göre Nesnelerin İnterneti, içsel durumları veya dış ortamlarıyla iletişim kurmak ve bunları algılamak veya etkileşime girmek için gömülü teknolojiyi içeren fiziksel nesneler ağıdır (Cisco, 2016). Cisco'ya göre, 2030 yılına kadar 500 milyar cihazın internete bağlanması bekleniyor. Her cihazın veri toplayan, çevre ile etkileşime giren ve bir ağ üzerinden iletişim kuran sensörleri bulunmaktadır. Nesnelerin İnterneti (IoT), bu bağlı cihazların ağıdır. Bu akıllı, bağlı cihazlar, IoT

uygulamalarının daha bilinçli kararları ve eylemleri yönlendirmeye yardımcı olmak için bir araya getirmek, analiz etmek ve içgörü sunmak için kullandığı veriler üretmektedir.

Nesnelerin İnterneti çatısı altında bir birlerine bağlı olan cihazlar artık bir birlerine karşı “sorumluluk” taşımak zorundalar çünkü SM’de olduğu gibi teknolojik saldırılar da genellikle en zayıf halkaya, insana yapılmaktadır. Örnek verecek olursak internete bağlı cihazlar arasında parola koruması en zayıf olan aygıtlardan birisi yazıcılardır ve bu nedenle son zamanlarda saldırıların büyük bir kısmı yazıcılara ve/veya yazıcılar üzerinden gerçekleştirilmektedir. Hürriyet Gazetesi’nin 18 Temmuz 2018 tarihli ve “Hacker’lar özellikle neden yazıcılara saldırıyor?” başlıklı yazısında şu bilgilere yer veriliyor: Bitdefender Antivirüs’ün Kuzey Amerika’daki 2000 evden topladığı istatistiklere dayanan bir araştırmaya göre internete bağlı cihazlar arasındaki en zayıf şifreler %50 oranla yazıcılara ait bulunmaktadır. (...) Yazıcılar aracılığıyla güvenlik önlemlerinin aşılması ve yazıcılarla aynı ağı kullanan diğer sistemlere saldırılması da potansiyel bir tehdit olarak karşımıza çıkmaktadır. Yine aynı gazetenin 21 Temmuz 2018 tarihli ve “Dünya Kupası boyunca futbolseverler siber saldırıya maruz kaldı” başlıklı yazısında sesli asistanlar üzerinden de teknolojik saldırıların gerçekleştirildiği ve rahatsız edici boyutlara ulaşabildiğine dair kanıt olarak şu bilgileri aktarıyor:

Müzik dinlemek, trafik durum bilgisi almak, bankacılık işlemleri gerçekleştirmek gibi pek çok uygulamada kullanılan akıllı cihazlardaki sesli asistanlar da siber saldırganların hedefi haline geliyor. Seslerin içinde komut gizlenmesi, insan duyma eşiği üzerindeki frekansların kullanımı ve seslerin kodlanması yoluyla komut gönderimi sesli asistanların istismar edilebileceği zafiyet alanlarını oluşturuyor. Gizli komutlarla gerçekleştirilebilecek saldırıların başında zararlı kod indirip çalıştırmak, gizli sesli/görüntülü aramayla casusluk faaliyeti yapma ve istenmeyen e-posta gönderme geliyor. Sesli asistanların istismarıyla oluşacak saldırıların kullanıcılara gerek maddi gerekse manevi hasar verecek seviyelere ulaştığı belirtiliyor.

Günümüzde kablosuz ve Nesnelerin İnterneti uygulamalarının artması *bluetooth* haberleşme teknolojisinin kullanım alanlarını da arttırmaktadır. Gelecekte akıllı evlerde Nesnelerin İnterneti uygulamalarında bluetooth kullanımının daha da yaygın bir şekilde kullanılması beklenilmektedir. Fakat bluetooth cihazlarının işlemci gücünün sınırlı olması, basit şifreleme sistemlerini kullanıyor olması, iletişim

esnasında aradaki haberleşmenin dinlenebiliyor olması gibi dezavantajları (güvenlik açığı olarak da değerlendirilebilir) barındırdığından (Kara, 2018, s. 106-107) Nesnelerin İnterneti, dolaylı olarak E 4.0'ın güvenliğini riske edecek bir özellik olarak değerlendirilmeli ve yeni protokoller ya da bluetooth'un görevini üstlenecek yeni teknolojilere ihtiyaç duyulabileceği gözden kaçırılmamalıdır.

Nesnelerin İnternetini anlamaya çalışırken, Büyük Veri ve Veri Analitiği ile Bulut Bilişim'i de aynı resim içerisinde değerlendirmekte fayda var: Nesneler, makineler, cihazlar, sensörler ve birçok yerden toplanacak veriler Bulut Bilişim altyapısını kullanarak Büyük Veriyi oluşturacak ve veri analitiği (bulanık mantık, yapay zekâ, yapay sinir ağları ve otonom algoritmalar vb.) desteği ile iletişimi ve nesneler arası haberleşmeyi gerçekleştirerek karar verme ve iş süreçlerini yönetebilecektir.

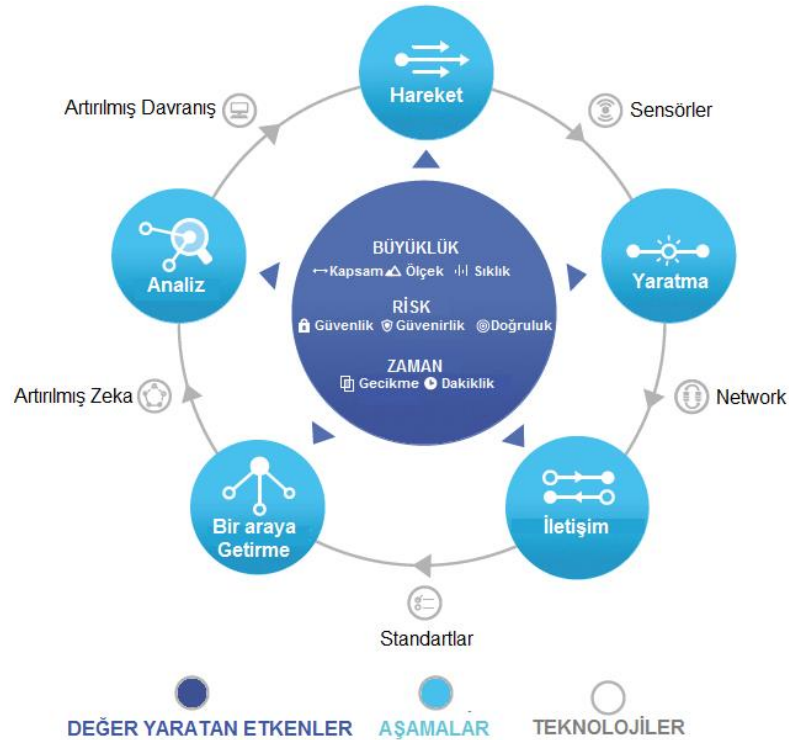
Trend Micro BT'nin dünya genelinde 1.150 kişinin katılımı ile Nesnelerin İnterneti (IoT) konusunda gerçekleştirmiş olduğu araştırmanın sonucuna göre birbirleriyle bağlantılı cihazlardaki sayının artmasıyla birlikte, işletmeler siber saldırılara karşı daha açık hale gelmektedir. BT ve güvenlik konusunda karar verenlerin %43'ü IoT projelerinin uygulanmasında güvenliğin ikinci plana atıldığını ifade ediyor (Hürriyet Teknoloji, 27 Ağustos 2018). Aynı araştırmaya göre müşterinin güveni kaybetme korkusu %52 ile işletmeler açısından birinci derecede önem arz ederken bunu %49 ile para kaybı, %32 ile kişisel bilgilerin kaybı, %31 ile yasal cezalar ve %28 ile veri güvenliği kurallarının ihlali takip ediyor. Bu demek oluyor ki, Nesnelerin İnterneti'ni kullanmak iş süreçlerini hızlandırırken ve daha verimli hale getirirken diğer taraftan güvenlik açıkları doğurmakta ve bu durum aşağı yukarı yarı yarıya göz ardı edilmektedir. IoT altyapısını kullanmadan önce işletmelerin güvenlik ve sızma (pentest) testlerini yeterince yapmadığı/yaptırmadığı görülmekte ve bu konun önemi bir kez daha doğrulanmaktadır.

World Economic Forum'un 6 Şubat 2019 tarihli ve "Internet of Things, Robotics and Smart Cities" başlıklı yazısında, bugün dünyada yaşayan insan sayısından daha fazla birbirine bağlı cihazın var olduğundan söz edilmektedir. Genelde, Nesnelerin İnterneti olarak bilinen bu cihazlar, enerji kullanımını izleyen ve yöneten akıllı bina teknolojilerinden, potansiyel çarpışmaları önlemeye yardımcı olan araçlara kadar uzanan sonsuz bir biçimde vücut bulmaktadır. 2020 yılına kadar,

devam eden teknolojik gelişmeler ve hesaplama, depolama ve bağlantıların, maliyetlerin düşmesiyle de IoT cihazlarının sayısının 20 milyarı aşacağı tahmin ediliyor. IoT teknolojileri günlük yaşamın tüm yönlerine yayılmaya devam ettikçe ve hatta insan vücuduna yerleştirildikçe, veri mülkiyeti, doğruluk ve mahremiyet koruması ile ilgili sorular daha büyük önem kazanacaktır. Benzer şekilde, elektrik şebekelerinin, kamu altyapısının, araçların, evlerin ve iş yerlerinin uzaktan erişilebildiği ve kontrol edilebildiği birbirine bağlı bir dünyada var olacaktır. Elbette bu gelişmeler eş zamanlı olarak siber güvenlik konusunu da gündeme getirecektir.

E 4.0 içerisinde yer alan Nesnelerin İnterneti, siber güvenliğin yanı sıra özellikle işletmeler ve devletler tarafından dikkatlice takip edilmesi gereken alanların başında gelmektedir. Deloitte (2017a, s. 4) “Guiding the IoT to Safety” başlıklı raporunda Nesnelerin İnterneti etrafındaki belirsizliği ve riski azaltmanın ilk adımının, ne olduğu ve devlet kurumlarının bununla nasıl etkileşime girmesi gerektiğine dair daha iyi bir fikir edinmekten geçtiğini belirtiyor. IoT’un, fiziksel dünyadaki dijital bilgileri oluşturmak, iletmek, birleştirmek, analiz etmek ve hareket etmek için gereken teknolojilerin mimarisi ve takımı olduğunu ekleyerek bunu Şekil 36’da yer alan görselle açıklıyor:

Şekil 36. Enformasyon Değer Döngüsü

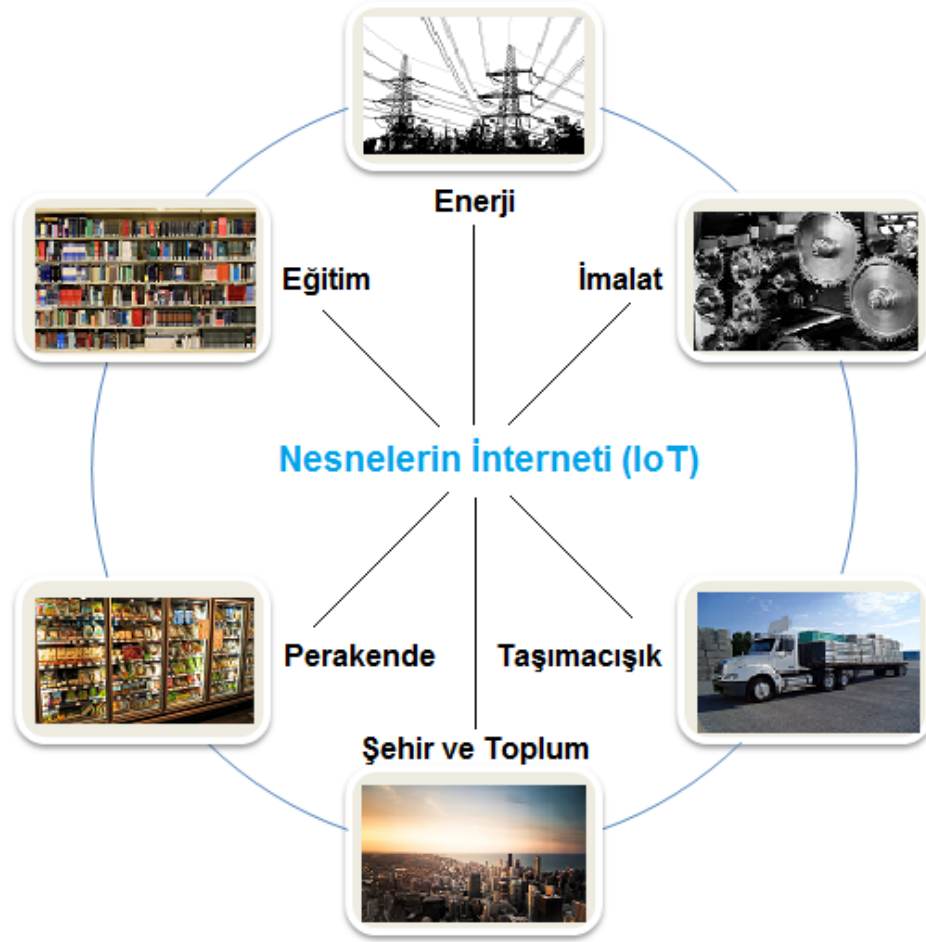


Kaynak: Deloitte Analysis, Deloitte, 2017a, s. 4

BT ve ağ konusunda dünya liderlerinden olan Cisco, işletmeler için Nesnelerin İnterneti (IoT) alanında en çok şu alanlarda hizmet ve çözüm üretmektedir (<https://www.cisco.com>); enerji, imalat sanayi, taşımacılık, şehirler ve toplum, perakende ve eğitim. Bu alanlar Endüstri 4.0'a dönüşüm sağlanması için en temel sektörleri ifade etmektedir. Şekil 37'de görsel olarak da belirtilen bu sektörleri kısaca şu şekilde açıklamak mümkündür:

- *Enerji sektörü için;* karar vermeyi hızlandırmayı, üretimi artırmayı, maliyetleri düşürmeyi ve işçi güvenliğinin artırılmasını
- *İmalat sanayi için;* makinelerin kolayca birbirlerine bağlanmasını, cihazların uzaktan izlenmesi, yönetilmesi ve üretim verilerinin gerçek zamanlı analizinin alınmasını
- *Taşımacılık sektörü için;* filo operasyonlarının optimize edilmesi ve servis maliyetlerinin düşürülmesini. Bağlantılı araçlar sayesinde, karayolları ve transit sistemler için yol koşulları ve önleyici bakım özellikleri için gerçek zamanlı görünürlük elde edilmesini
- *Şehirler ve toplum için;* akıllı şehir çözümleriyle altyapının geliştirilmesini, daha uygun maliyetli belediye hizmetlerinin oluşturulmasını, toplu taşıma araçlarının iyileştirilmesini
- *Perakende sektörü için;* yenilikçiliğin hızlandırılmasını, işlemlerin optimize edilmesini, maliyetlerin düşürülmesini
- *Eğitim sektörü için;* öğrenci çıktılarını geliştirmeyi, güvenliği artırmayı ve yerleşke izlemeyi iyileştirmeyi ifade etmektedir.

Şekil 37. Nesnelerin İnterneti (IoT) ve Sektörler



Kaynak: Cisco verilerine dayanılarak uyarlanmıştır. (<https://www.cisco.com>),
Erişim: 15.05.2019. Fotoğraflar <https://pixabay.com> sitesinden alınmıştır, Erişim:
15.05.2019

Nesnelerin İnterneti, üretkenliği artırıyor ve birçok ürün ve hizmeti üretmenin marjinal maliyetini (*üretim miktarı 1 birim arttırıldığında toplam maliyette meydana gelen değişim*) sıfıra yakın bir seviyeye çekiyor. Bunun sonucunda şirket karları erimeye başlıyor, fikri mülkiyet hakları zayıflıyor ve ürün kıtlığına dayalı ekonomi yerini yavaş yavaş bolluğa dayalı bir ekonomiye bırakıyor. (...) Şirketler mal ve hizmetlerin akışını izlemek için ticari koridorları boyunca sensörler yerleştiriyorlar. Örneğin UPS kargo şirketi Büyük Veriyi kullanarak ABD'deki 60 bin aracını anlık olarak takip ediyor (Rifkin, 2015, s. 19-20). Daha doğrusu 60 bin aracı izleyerek Büyük Veriyi elde ediyor ve bunu yorumlayarak ortaya çeşitli faydalar koyuyor. Alışveriş merkezlerinde ise sensörler, satış ve pazarlama departmanlarına, müşterilerin ağırlıklı olarak hangi ürünlere baktıklarına ve hangi ürünle

ilgilendiklerine, hangilerini ellerine alıp incelediklerine, hangilerini rafa geri koyup hangilerini satın aldıklarına dair birçok bilgi sağlıyor. Perakendeci ve tüketicilere gönderilen ürünlerin nerede olduğu da sensörler aracılığıyla takip ediliyor. Sensörler, ne miktarda atığın geri dönüştürülüp tekrar kullanım için işlendiğini de bildiriyor. Büyük Veri 7/24 analiz edilerek tedarik zinciri stokları, üretim ve dağıtım süreçleri duruma göre yeniden ayarlanıyor ve analiz sonuçları ışığında değer zinciri üzerinde verimlilik ve üretkenliği artırmak amacıyla yeni kurumsal uygulamaları hayata geçiriyor (Rifkin, 2015, s. 20-21).

2012 yılının sonlarında Endüstriyel İnternet terimini kullanan ve dijital sanayi şirketleri arasında önde gelen GE şirketi “Industrial Internet” başlığı altındaki yazısında Nesnelerin İnterneti (IoT) ve Endüstriyel Nesnelerin İnterneti (IIoT) -IoT’un endüstriyel pazarlarda kullanılması- için şu bilgilere yer veriyor: Endüstriyel İnternet’in 2020 yılına kadar 2,125 milyar dolarlık bir piyasasının olabileceği, Endüstriyel İnternet devriminin 2030 yılına kadar Avrupa GSYİH’sına 2.8 trilyon Euro ekleyebileceği tahmin ediliyor. Bu, Euro Bölgesi ekonomisinin mevcut büyüklüğünün dörtte birine yakın. IIoT aynı zamanda havacılık, demiryolu, enerji ve enerji üretimi ve sağlık hizmeti sunumu gibi çeşitli endüstrilerde dünya genelinde Avrupa rekabet edebilirliğini arttırırken daha fazla verimlilik ve hız yaratabilecektir. Endüstriyel İnternet, Avrupa’nın bugün karşı karşıya olduğu enerji zorluklarını azaltarak enerji verimliliğini de sağlayabilir. Gazla çalışan enerji üretiminde yalnızca %1’lik tasarruf sağlamanın bile, önümüzdeki 15 yıl boyunca yakıt tasarrufunda küresel olarak 66 milyar dolar, Avrupa’da 15 milyar dolar olacağı ifade ediliyor. Gartner, Nesnelerin İnterneti’nin 2020 yılına kadar yaratacağı katma değeri 1,9 trilyon dolar olarak öngörüyor (<https://www.ge.com/europe/industrial-internet>).

Nesnelerin İnterneti dünyasında tüm olumlu ilerlemelerin yanı sıra bazı soru işaretleri de bulunmaktadır. Bu sorulardan en başta geleni ise Rifkin (2015)’e göre şunlardır; herkes ve her şeyin birbirine bağlandığında kişinin mahremiyetinin korunması için sınırlar nasıl belirlenecek? Sorun şu ki Nesnelerin İnterneti üzerinde gerçekleşen veri akışına erişme becerisine sahip, gelişmiş yazılımlar kullanan şirketler, kendi amaçları ve çıkarları doğrultusunda sömürmenin yeni yollarını aramak için küresel sinir sisteminin her katmanını delebilirler. Siber hırsızlar, ticari kazanç elde etmek için -bu çalışmada yer alan SM ve BG bölümlerinde de ifade

edildiği üzere- kimlik bilgilerini çalabilir, sosyal medya siteleri karlarını artırmak için verileri reklam verenlere ve pazarlamacılara satabilir, politik kampanya organizatörleri önemli bilgileri yabancı devletlere aktarabilirler (s. 84). Şu an öngörülemeyen birçok olumsuzluğun gelecekte ortaya çıkacağına hiç şüphe yok fakat olumlu yanları açısından bakılacak olursa IoT ve onun sağlayacağı faydaları göz ardı etmek mümkün gözüküyor.

3.2.6 Siber Güvenlik (*Cyber Security*)

E 4.0 ile birlikte, siber güvenlik çok daha önemli bir konuma gelmiştir. Dijitalleşmenin ve robotların çalışma dünyasında çok daha fazla yer alması, Nesnelerin İnterneti, yapay zekâ, akıllı fabrikaların varlığı işletmelerde çeşitli riskler oluşturmaktadır. Bu risklerden biri de siber tehditlerdir. Yapay zekâ teknolojisinin özellikle savunma endüstrisinde kullanılmaya başlamasıyla birlikte siber tehditler daha çok konuşulmaya başlanmıştır (Öztuna, 2017, s. 68).

T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı'nın 2012 yılında Bilgi Güvenliği Derneği ile birlikte hazırlamış olduğu "Ulusal Siber Güvenlik Stratejisi" raporunda siber saldırı; "hedef seçilen şahıs, şirket, kurum veya devletin bilişim sistemlerinin işleyişinin engellenmesi, bozulması veya değiştirilmesi yoluyla iş, ticaret, yönetim veya toplumsal hayat üzerinde olumsuz etki oluşturacak girişimlerdir. Ulusal veya uluslararası düzeyde ticari, politik veya askeri amaçlı olarak, planlı ve eşgüdümlü bir faaliyet olarak gerçekleştirilebileceği gibi çeşitli kişi ve gruplar tarafından çok değişik amaçlar için de gerçekleştirilebilir" şeklinde, siber güvenlik ise; "Siber saldırılara karşı alınan tedbirler bütünüdür. Kurum, kuruluş ve kullanıcıların varlıklarını korumak amacıyla kullandığı araçlar, geliştirilen politika ve uygulamalar; yazılı belgeler, elektronik ortam dokümanları, etkinlikler, eğitimler ve bilişim alanında kullanılan güvenlik teknolojilerinin tamamı siber güvenliğin unsurları arasındadır" şeklinde tanımlanmaktadır. Yine aynı raporda kritik altyapının zarar görmesinin toplumsal düzenin devamı için çeşitli seviyelerde güçlükler yaratacağı, bunun ise can güvenliğinden ekonomik faaliyetlerin sürdürülmesine kadar birçok alanı etkileyeceği belirtilmektedir. Siber güvenlik bağlamında kritik altyapının ise şu başlıkları kapsaması gerektiği önerilmektedir; kamu güvenliği, savunma, nükleer-biyolojik-kimyasal tesisler, ulaşım, gıda, su, sağlık, bilişim, enerji

ve mali işler. Bu başlıklara nüfus bilgileri ve tapu kayıtlarını da eklemek bizce mümkündür.

Siber saldırılar kişilere, kurumlara ya da devletlerin tüm sektörlerine uygulanabildiği, kaotik ve hayati durumlar yaratabildiği için dikkatli ve anlık olarak izlenmesi gereken konuların başında gelmektedir. Bu sebeptendir ki siber güvenlik “varlıkların” korunmasında ilk sıralarda yer almaya başlamıştır. Siber güvenlik için donanım, yazılım ve uzman insan kaynakları alanlarında her türlü önlemlerin birinci dereceden ele alınması ve uygulanması artık zaruri hale gelmiştir. Güvenlik açıklarının uygun proje ve yatırımlarla giderilmesi her türlü iş akışının kesintiye uğramadan devam etmesi için ön koşullardan biri olmuştur.

Kaspersky Lab tüm dünyada en çok kullanılan 13 paylaşım aracı uygulama güvenliğini incelediğinde hemen hepsinde güvenlik açıklıklarının olduğunu tespit etmiştir. Araştırmada ayrıca, kötü niyetli kişilerin çalıntı hesaplarla bu uygulamalar üzerinden uzun süreler boyunca yasal olmayan gelir elde ettikleri de belirlenmiştir. Tespit edilen bu güvenlik açıklıklarının başında şunlar gelmektedir (Hürriyet Teknoloji, 25 Temmuz 2018):

- Ortadaki Adam Saldırısı'na (*man in the middle*) karşı önlem alınmaması
- Tersine mühendislik (sistemin nasıl çalıştığının kolayca tespit edilip sunucu altyapılarına erişimin kolaylaştırılması) için önlem alınmaması
- Root yetkilendirmelerinin engellenmemesi
- Zayıf parolaların talep edilmesi
- Kullanıcılara ait verilerin çalınabilmesi ve kimlik hırsızlığı

Blokszincir (Blockchain) yapısına dayalı mimariler siber güvenlik için yeni çözüm önerilerine ilham olmaktadır. Blokszincir yapısına dayanan bu mimari ile veri bütünlüğü, mahremiyet, kullanılabilirlik ve güvenlik servislerinin ve hata toleransının sağlandığı etkin çözümler geliştirilebilmektedir. Blokszincir sistemleri ile siber güvenlik çözümlerinin etkinleştirilmesine yönelik çalışmalar gerçekleştirilebilir. Örneğin; IoT, akıllı şehirler ve bilgisayar ağlarının siber güvenliği için ve kişisel verilerin korunmasında kullanımına dair çalışmalar bunların başını çekebilir (Karaarslan ve Akbaş, 2017, s. 20). Yine Blokszincir alt yapısını kullanan Etheurum *akıllı kontratları* (smart contracts) yaşamımıza sokmaya

çalışmaktadır. Blok'ları oluşturan algoritmalar içerisinde çeşitli kodlar yazılabilmesine fırsat veren Ethereum yapısı Blokzincir'in dağıtık (distributed) ve merkezi olmayan (decentralized) yapısını kullanarak siber güvenlik açısından da bazı tehditleri bertaraf etmeyi hedeflemektedir.

Siber saldırılar kişilerin, çeşitli gurupların, illegal örgütlerin ve legal örgütlerin (devlet vb.) genellikle hibrit olarak yaptıkları saldırılara dönüşmüş, sahada yaşanan konvansiyonel saldırılara destek olarak (gelecekte bu sıralama yer değiştirecektir) icra edilmektedir. Öyle ki siber saldırılar yalnızca bilişim teknolojileri üzerinden çeşitli yazılımlarla/uygulamalarla değil aynı zamanda sosyal medya üzerinden çeşitli SM teknikleri kullanılarak da yapılmaktadır: Karşı tarafa ait veri ve bilgileri kullanma, çalma ve yayınlama, tehdit, şantaj, kitleleri yönlendirme, kalpleri kazanma ya da çeşitli nefretler uyandırma, manipülasyon, ilk kıvılcımı başlatma, yanlış ve yalan haberler, kara propaganda ve benzeri şekilde yürütülebilmektedir. Bütün bu "saldırı araçları" siber saldırı teknikleri ile ya da siber saldırı teknikleri aracılığıyla elde edilen verilerle desteklenerek yapılabilmektedir. Saldırı tüm cephede her yönde gerçekleştirilmektedir. Yakın gelecekte E 4.0 uygulamalarının daha fazla yaygınlaşmasından itibaren siber saldırıların (Nesnelerin İnterneti platformu aracılığı ile) neredeyse tüm sistemleri eş zamanlı tehdit etme olasılığı gündeme gelebilecektir.

Siber saldırılara karşı korunabilmek için katı çözüm denilebilecek bir sistem henüz geliştirilememiş olsa da, çeşitli önlemler almak elbette mümkündür. Siber güvenlik adına alınabilecek önlemler için ABD Ulusal ve İç Güvenlik Bakanlığı Idaho National Laboratory'den ulusal şebeke stratejisti Bochman (2018) şu önerilerde bulunmaktadır: Devre dışı kaldığında işleyişe zarar verecek olan fonksiyonları belirlemek, bu sistemleri olabildiğince internetten izole etmek, dijital teknolojileri minimuma indirmek ve bu sistemlerin izlenme ve kontrol süreçlerinde analog araç ve yöntemler ile güvenilir insan kaynağı kullanmak. Kritik sistemlerin dijital unsurlar tarafından saldırıya uğramasını engellemenin tek yolunun bu (s. 41) olduğunu belirten Bochman ayrıca, siber saldırıların finansal etkilerinin de gittikçe arttığını, son birkaç yılda *WannaCry*, *NotPetya* gibi saldırıların sırasıyla 4 milyar dolar ve 850 milyar dolarlık bir zarara neden olduğunu belirtmektedir. Bu saldırıların, 150 ülkede hastanelerde, okullarda şirketlerde ve hanelerde yüz binlerce

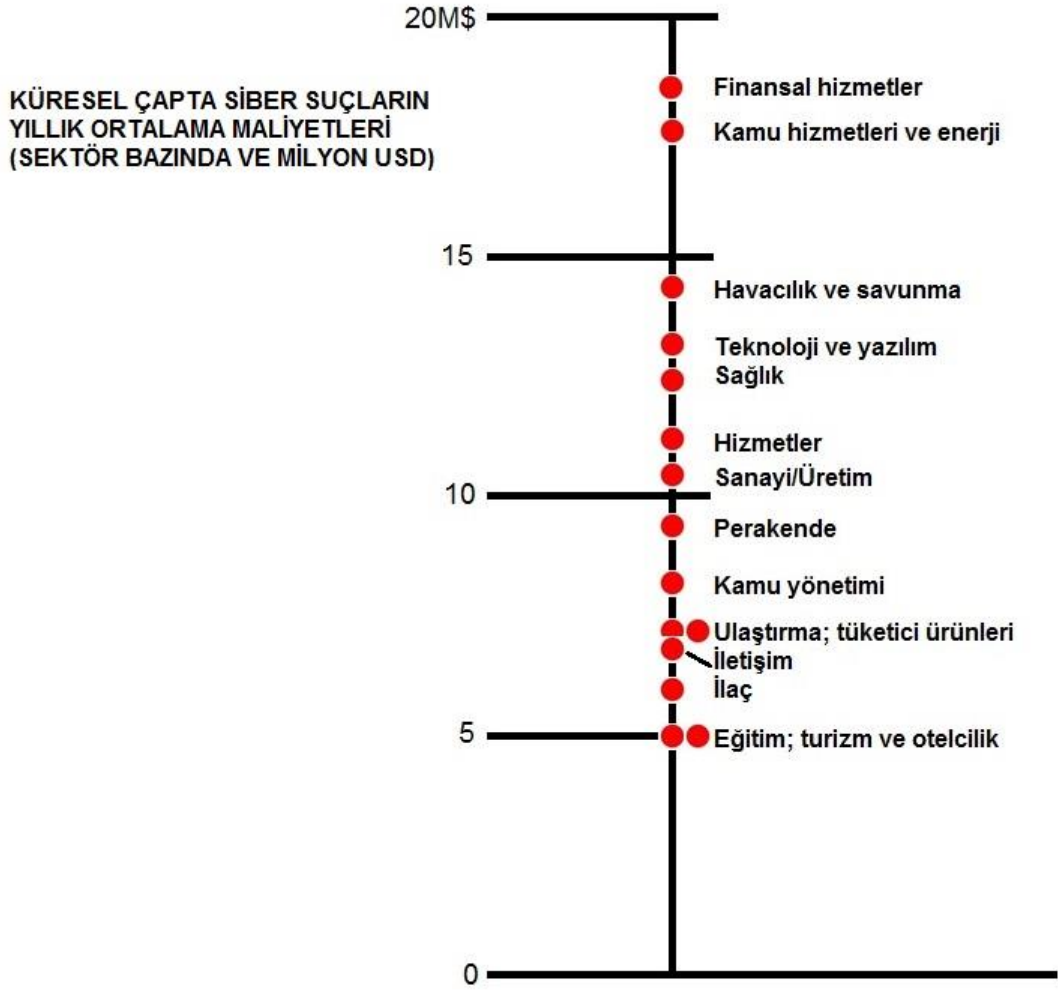
bilgisayarın ele geçirilmesi ve şifresinin açılması karşılığında fidye istenmesi (ransomware) şeklinde kurgulandığını (s. 42), eğer bir hedefe yönelik on yol varsa, ancak bunların hepsi belirli bir düğümden (node) geçiyorsa savunmayı kurmak için ideal noktanın bu düğüm olduğunu, bu düğümün olduğu yere *tripwire*¹² olarak adlandırılan ve olası bir sorundan uzmanları anında haberdar eden yüksek hassasiyete sahip bir algılama sisteminin kurulabileceğini (s. 48) belirtmektedir.

Siber güvenlik için aktif ve pasif savunmaların neler olabileceği konusunda Berinato (2018) şu bilgileri paylaşmaktadır; son dönemlerde pek popüler olmayan bazı fikirler (bazı sistemleri internetten çıkarmak -ağ'dan bağımsız hale getirmek-, bazı mekânlardaki otomasyonu kaldırmak, süreçlere güvenilir insanları yerleştirmek) artık makbul hale gelmiştir (s. 50). Aktif siber savunmaya dair verilebilecek bir örnek şudur: Bir sistem düşünün, bu sistem sızma girişimlerini izliyor, sızma girişimini tespit ettiğinde kaynaktan gelen diğer şebeke iletişimlerini bloke ederek ve sistem yöneticisine alarm vererek yanıt veriyor. Aktif siber savunma için diğer bir örnek ise; DDoS saldırıları yapan bir *botnet*'i tespit edip devre dışı bırakmak olabilir. “yanıt verme” ve “devre dışı bırakma” tabirleri aktif savunmayı işaret etmektedir. Pasif savunma için ise verilebilecek bir örnek; casuslara ve hırsızlara karşı iletişimi ve depolanan verileri şifrelemek olabilir (s. 51). Burada dikkat edilmesi gereken önemli bir unsur ise hem aktif hem pasif savunma için olsun, önerilen önlemlerin ön alıcı (proaktif) girişimler/yaklaşımlar şeklinde olması gerekliliğidir.

Berniato ve Perry (2018), Ağustos 2018 Harvard Business Review Türkiye’de yer alan “*Rakamlarla Güvenlik Trendleri*” başlıklı çalışmalarında Accenture ve Ponemon Institute kaynaklı, küresel çapta gerçekleşen siber suçların yıllık ortalama maliyetlerini ve sektörel dağılımını (s. 59) gösteren bilgilere yer vermektedir. Şekil 38’de detayları görülebilen bu bilgiler arasında dikkat çeken nokta ise finansal hizmet sağlayan kurumlar ile kamu hizmetleri ve enerji sektöründe faaliyet gösteren kuruluşlara yapılan saldırıların diğer sektörlerle göre açık ara önde olmasıdır. Özel ve kamu sektöründe bu alanlarda faaliyet gösteren kurum ve kuruluşların siber güvenlik altyapılarına ve önleyici sistemlere daha fazla zaman ve kaynak ayırmaları gerektiğini hatırlatmanın faydalı olacağını düşünmekteyiz.

¹² **Tripwire:** Bir davetsiz misafir taarfindan tetiklendiğinde sistemi alarma geçiren düzenek.

Şekil 38. Küresel Çapta Siber Suçların Sektör Bazında Yıllık Ortalama Maliyetleri



Kaynak: Berniato ve Perry, 2018, “2017 Cost of Cyber Crime Study: Insight on the Security Investments That Make a Difference” Accenture and Ponemon Institute ©HBR.ORG

3.2.7 Siber Fiziksel Sistemler (*Cyber Physical Systems*)

Siber Fiziksel Sistemler (SFS) hesaplama, ağ ve fiziksel işlemlerin entegrasyonudur. Gömülü bilgisayarlar ve ağlar, fiziksel işlemlerin hesaplamalarını yaparak, bunun tersi yönde geri besleme döngüleri ile fiziksel süreçleri izler ve kontrol eder. Bu tür sistemlerin ekonomik ve toplumsal potansiyeli, gerçekleştirilenden çok daha büyüktür ve teknolojiyi geliştirmek için dünya çapında büyük yatırımlar yapılmaktadır. Bu teknoloji, eski (ama hala çok genç) disiplinler üzerine kuruludur; arabalar, oyuncaklar, tıbbi cihazlar ve bilimsel enstrümanlar gibi prensip görevi hesaplama yapmak olmayan cihazlara gömülü sistemler, bilgisayarlar

ve yazılımlardan oluşur. SFS, fiziksel süreçlerin dinamiklerini, yazılım bütçesi ve ağ oluşturma ile birleştirerek, bütünleşik soyutlama ve modelleme, tasarım ve analiz tekniklerini meydana getirir (Ptolemy Project, 2012).

SFS, kişiselleştirilmiş sağlık bakımı, acil durum müdahalesi, trafik akışı yönetimi ve elektrik enerjisi üretimi ve sunumu ile birlikte şu anda öngörülemeyen diğer birçok alanda gelişmeler getirecektir. SFS, entegre fizik ve mantık yoluyla işlev için tasarlanmış etkileşimli dijital, analog, fiziksel ve insan bileşenlerini içerir. Bu ve ilgili SFS teknolojileri içerisinde; Nesnelerin İnterneti (IoT), endüstriyel internet, akıllı şehirler, akıllı grid'ler ve akıllı olan her şey (örneğin; arabalar, binalar, evler, üretim süreçleri, hastaneler, aletler) yer almaktadır (NIST Engineering Laboratory).

SFS; iletişimi, fiziksel süreçleri ve sistemleri yönetmek ve/ya izlemek için enformasyon teknolojisinden yararlanır. Gömülü (embedded) sistem olarak da adlandırılan siber-fiziksel sistem örnekleri arasında akıllı şebekeler, otonom taşıt sistemleri, medikal izleme, endüstriyel süreç denetim sistemleri, robotik cihazlar ve otomatik kumanda elektroniklerini saymak mümkündür (Banger, 2018b, s. 46).

SFS ifadesi aslında E 4.0 için tanımlanmıştır. SFS sanal ve fiziksel dünyaları bir araya getirerek, akıllı nesnelerin birbirleriyle iletişim kurdukları ve birbirleriyle etkileşime girdiği, gerçekten ağı bağlı bir dünya oluşturan teknolojileri (Nesnelerin İnterneti) etkinleştirmektedir. Gerçek ve sanal dünyalar arasındaki sınırlar ortadan kalktığında çok sayıda yenilikçi uygulama yapan ve bunları hayata geçiren sistemler karşımıza çıkmaktadır. Gelecekte, siber-fiziksel sistemlerin, insan güvenliğine, verimliliğe, konfora ve sağlığa çok önemli bir şekilde katkıda bulunacağı öngörülmektedir. Bunu yaparken, demografik değişim, doğal kaynakların azlığı, sürdürülebilir hareketlilik ve enerji değişimi gibi temel zorlukların üstesinden gelmek için de önemli bir rol oynayacağını (Kulabaş, 2017) söylemek mümkündür.

Bilgi teknolojisi, toplumlar, örgütleri ve sektörleri ile üyelerinin yaşamları üzerinde belirgin bir etkiye sahiptir. Üretim süreçlerinin otomasyonu ve kişisel ve mobil cihazların hem iş hem de özel bağlamlarda kullanımı sadece birkaç örnektir. Günümüzde, ileri düzeyde bir gelişme BT altyapısına dayanarak hesaplanamaz bir potansiyel getirmektedir: Nesnelerin İnterneti sensörlere, aktüatörlere ve veri analiz çözümlerine dayanarak, siber-fiziksel sistemlerin kullanımında olan yeni teknoloji

çağı için altyapıyı oluşturmaktadır. Yapay zekâ artık yalnızca analitik ve verilerin değerlendirilmesinde kullanılmakla kalmayıp, siber alanın fiziksel dünya ile robotik çözümler şeklinde etkileşime girmesine de neden olmaktadır (Oks, 2016).

Siber-fiziksel sistemler bir anlamda Toplum 5.0'ın doğumuna da öncülük etmektedir. Gladden (2019)'e göre, Japonya Hükümeti'nin "Toplum 5.0" girişimi, vatandaşların günlük yaşamlarının suni olarak akıllı sistemler ile giderek daha yakın işbirliği yaparak daha da yoğunlaştırılacağı siber-fiziksel bir toplum yaratmayı amaçlamaktadır. Bununla birlikte, bariz bir paradoks, insanların giderek artan özerk sosyal robotlar ve somutlaşmış yapay zekâların yanında yaşayacağı daha "insan merkezli" bir toplum yaratma çabalarının merkezinde yatıyor. Temel olarak, Toplum 5.0, E 4.0'ın işletmeler içinde üretim için kullandığı hızla gelişen teknolojileri almaya ve onları sıradan insanların günlük yaşamlarına daha derinden entegre etmeye çalışmaktadır.

Siber-fiziksel sistemlerin, bugünün özerklik, işlevsellik, kullanılabilirlik, güvenilirlik ve siber güvenlik seviyelerini aşan yeni özelliklere sahip ve gelecekteki mühendislik sistemlerinin tasarımında ve geliştirilmesinde önemli bir rol oynaması beklenmektedir (Baheti ve Gill, 2011).

3.2.8 Otonom Robotlar (*Autonomous Robots*)

Yapay zekâ yeteneği, makine öğrenmesi ve iletişim becerilerine sahip bir robot karşılaştığı bir problemi benzer yeteneklere sahip diğer robotlarla paylaşarak bir 'bütünleşik ve ortak akıl' yaratılmasını sağlayabilecek ve böylece otonom robotlar problemi birlikte çözebileceklerdir (Banger, 2017a). Akıllı makinenin birinci özelliği kendi durumu hakkındaki farkındalıktır. Kendisine atanmış parametrelerden herhangi bir sapma olması durumunda bunun farkına varır ve ağ üzerinden ilgili kişiyi bilgilendirir. Bu tür bir makine durum tespiti için farklı algılama ve ölçme özelliklerine sahip sensörlerle donatılmış olup, gömülü donanım ve yazılım aracılığı ile yapay zekâ uygulamaları sergileyebilir. Böylece akıllı karar ve seçim için operatöre ihtiyaç duyulmayan durumlarla sınırlı olmak üzere makineye bir özerklik sağlanmış olur (Banger, 2017b). Robotlar, yazılım aracılığı ile yönetilen ve bir amaç için iş ve değer üreten makinelerdir. Robotik ise; makine mühendisliği, uçak mühendisliği, uzay mühendisliği, elektronik mühendisliği, bilgisayar mühendisliği dallarının birlikte çalışmasıyla ortaya çıkan bir bilim dalıdır (Yılmaz, 2017, s. 9).

Robotların tekrarlamalı iş ve işlemlerde standardın, kalitenin ve iş güvenliğinin üst düzeye çıkmasına yardımcı olmaları hız ve maliyet bağlamında önemli avantajlar getirmektedir. E 4.0 teknolojilerinde akıllı, yani öğrenebilen ve iş ortamında insan ile birlikte çalışabilen robotlar mevcut robotları IoT ortamına taşıyarak uzaktan yönetilir olabilme, olası süreçlerde robot yatırımlarına gitme, hem bu teknoloji ile tanışmaya hem de iş ve üretim süreçlerinde standartların artmasına katkı sağlayacaktır (Apilioğulları, 2018, s. 93). E 4.0 çatısı altında robotik'in bu şekilde kullanımı; Apilioğulları (2018)'nin ifadesi ile, tüm üretim süreçlerinde değer oluşturmeyen kayıpların ortadan kaldırılması (JIT-Just in Time), üretim hatlarının mümkün olduğunca çabuk bir şekilde farklı bir model üretebilmeye uygun hale getirilmesi (Heijunka) ve üretim sürecinde belirli bir hata meydana geldiğinde üretim hatlarını hatanın ortadan kaldırılıp yeniden oluşmasını engelleyinceye kadar durdurulması (Jidoka) temeli üzerine kurulu olan Toyata Üretim Sistemi felsefesini (s. 101-102) de doğrudan destekleyecek yapıyı oluşturmada önemli katkılar sunabilecektir. Otonom robotlar ve uygulamaları, atıl (muda) görünen kayıp ve zararları daha kolay bertaraf edilebilmek ve müşterinin istediği zaman diliminde müşterinin isteği şekil ve miktarda ürünün karşılanabilmesi üzerine kurgulanmış olan çekme (pull) sisteminin de daha kolay uygulanmasını sağlayacaktır.

E 4.0'ın vazgeçilmez bir yüzü, “Nesnelerin İnterneti” (IoT) olarak adlandırılan bir konseptle desteklenen otonom üretim yöntemleridir -birbirine bağlı nesneler, cihazlar ve bilgisayar makinelerinin birbirleriyle iletişim kurabileceği fikri-. Otonom robotlar, üretim dâhil sayısız endüstri genelinde en önemli örneklerdir. Merkezi bir sunucuya, veri tabanına veya programlanabilir mantık denetleyicisine bağlanarak, robotların hareketleri daha önce hiç olmadığı kadar büyük ölçüde koordine edilebilir ve otomatikleştirilebilir. İşleri akıllıca, en az insan girdisiyle düzenlenmiş bir şekilde tamamlayabilirler. Malzemeler fabrikalarda otonom mobil robotlar üzerinden taşınabiliyor, bu robotlar engellerden kaçınıyor, filo arkadaşları ile koordine oluyor ve alıcıların ve teslimatların gerçek zamanlı olarak nerede olduğunu tespit ediyor (Melanson, 2018).

Milvus Robotiğin kurucu ortağı Hacıneçipoğlu (2017) endüstriyel robotların gelişimini, Otomatik Kılavuzlu Araçlar (OKA) ile Otonom Mobil Robotların (OMR) karşılaştırmasını da yaparak şu şekilde açıklıyor:

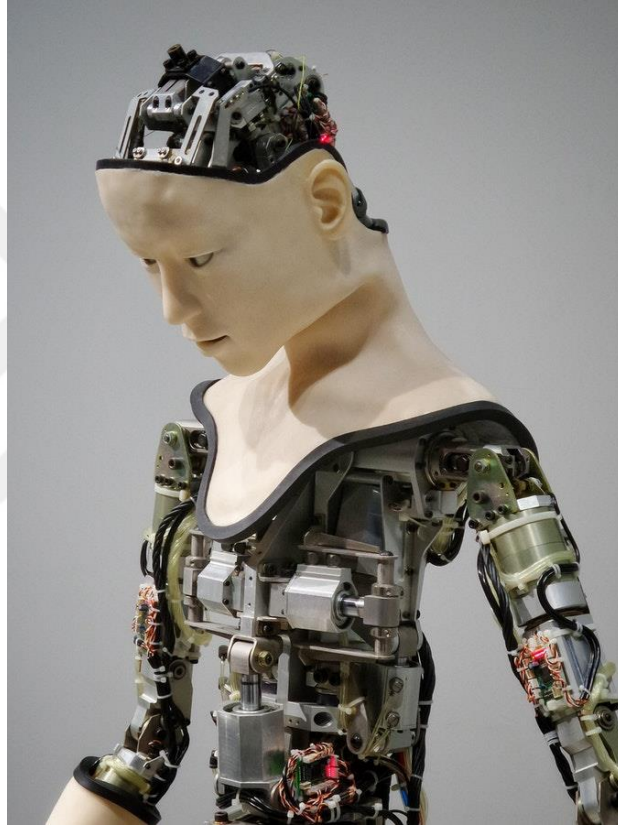
Endüstriyel robotlar veya başka bir deyişle robotik kollar bize üçüncü sanayi devrimi tarafından hediye edildi ve temel olarak kısa hedefler için belirli nesnelerin taşınması veya üretim hattında art arda ve hızlı bir şekilde kaynak yapılması gibi önceden tanımlanmış görevleri üstlenebiliyorlar; bu durum fabrikalar için onları oldukça önemli kılıyor. OKA'lar ise daha uzun mesafeler için doğadaki daha ağır nesneleri hareket ettirme görevini üstlendi. Malzemelerin taşınması konusuna kısmi bir çözüm sunsalar da, OKA'ların doğal dezavantajları, fabrikalar için vazgeçilmez olmalarını engelledi. Önceden belirlenmiş rotaları bırakamama ve fabrikadaki değişikliklerin yanı sıra fiziksel belirteçler nedeniyle sınırlı hareket yapıları ve bunlara bağlı aşınma ve yıpranma hareketleri, insanlarla gerçek zamanlı çalışma yetersizliği ile birlikte OKA'ların ömrünün sona erdiğinin sinyallerini verdi. Dördüncü sanayi devrimi ile halen bazı tesislerde kullanılsalar da, E 4.0'ın bize sunduğu teknolojik avantajlara erişememeleri nedeniyle, yerlerini OMR'lere bırakıyorlar. Dördüncü sanayi devrimi tarafından getirilen duysal ve işleme güçlerinin kullanılması yoluyla OMR'ler, OKA'lara kıyasla çok daha esnek, verimli ve entegre bir üretim yöntemi sunmaktadır. Doğal bir gezinme süreci içinde çalışacakları ortamı haritalandırırken, herhangi bir bant, ray veya başka altyapı yatırımlarına ihtiyaç duymazlar. Dinamik rota planlama yeteneğine sahip oldukları ve herhangi bir fiziksel hatla sınırlı olmadıkları için, OMR'ler belirlenen limitler dâhilinde alınacak en iyi rotayı seçebilir ve karar verebilir. Özerk yapıları nedeniyle, OMR'ler rotalarındaki olası herhangi bir engelde güvenle gezinebilirler. İnsan çalışanlarla bir alanı paylaşabilen bu robotlar, herhangi bir tesisin mevcut yönetim sistemlerine entegre olabilir ve onlardan sipariş alabilir. Ayrıca, bu robotlar yükleme/boşaltma işlemini gerçekleştirmek için bir robotik kol veya bir konveyör ile de iletişim kurabilir. Araç takip ve/ya filo yönetim sistemleri sayesinde birden fazla OMR aynı tesiste uyumlu bir şekilde çalışabilir. Bir bakıma, bu robotlar Google ve Tesla'nın sürekli üzerinde çalıştığı "özerk araç" teknolojisini fabrikalara getiriyor. Bu bakımdan, genellikle Kendi Kendini Süren Araçlar olarak da adlandırılırlar.

Nelmia Robotics Insight'ın "Robots and Industry 4.0" başlıklı çalışmasında otonom robotlarla ilgili şu verilere yer verilmektedir: Robotların kullanım alanları; "üretim, endüstri, altyapı, sağlık hizmetleri, perakende, yiyecek-içecek, eğitim, güvenlik, inşaat, enerji, lojistik, tarım, eğlence ve turizm" olarak belirtilirken, robot pazarının Amerika'da 2025 yılına kadar yaklaşık 70 milyar dolarlık bir hacme ulaşacağı belirtilmektedir. Aynı raporda, Boston Consulting Group'un verilerine göre bu pazarın dağılımının şu şekilde olacağı ifade edilmektedir: Kişisel alanda 9 milyar dolar, ticari alanda 17 milyar dolar, endüstri alanında 24,4 milyar dolar ve askeri alanda 16,5 milyar dolar.

E 4.0'ın önemli bir yüzü güvenlik, esneklik, çok yönlülük ve işbirliğine odaklanarak tanımlanan işleri akıllıca tamamlayabilen robotların desteklediği otonom üretim yöntemleridir. Çalışma alanını tecrit etmeye gerek kalmadan, insan

alışma alanlarına entegrasyonu daha ekonomik ve üretken hale geliyor ve endüstrilerde birçok olası uygulamayı başlatıyor. Endüstriyel devrimi kolaylaştırmak için en son teknolojik yeniliklerle daha fazla endüstriyel robot gelişmektedir. Akıllı robotlar, yalnızca, kapalı alanlarda çalışan insanların yerini almayacak. E 4.0'da robotlar ve insanlar el ele çalışacak, görevlerine uygun olarak birbirine bağlanacak ve akıllı sensör-insan-makine ara yüzleri kullanılacak (Bahrin, Othman, Azli ve Talib, 2016, s. 139).

Şekil 39. Otonom Robotlar



Kaynak: <https://unsplash.com/photos/YKW0Jp7rIU>, Erişim: 28.05.2020

Robotik ile ilgili önemli bir diğer kavram ise sibernetiktir. Gürel (2017), sibernetiği, bilginin rol oynadığı tüm biyolojik ve mekanik sistemler arasındaki etkileşimi inceleyen ve kanunları tespit eden bir bilim dalı olarak ifade ediyor (s. 126). Gürel (2017), Norbert Wiener'in sibernetik ve otomasyon kavramını birleştirerek E 4.0'ın temelini attığını, sibernetiğin en önemli uygulama alanlarından birinin robot teknolojisi olduğunu belirtiyor: "İnsan ve hayvan anatomi ve fizyolojisinden elde edilen verilerin kuantum teknolojisi ile birleşmesi sonucu robot

teknolojisi ivme kazandı. Her canlı organizmada haberleşme (bilgi aktarımı) ve geri besleme mekanizması vardır. Geri besleme; sistemin performansı ile ilgili elde edilen verilerdir. Gözbebeğinizin maruz kaldığı ışığın şiddetine göre büyüyüp küçülmesi geri beslemeye örnek verilebilir. Siberetik sistem bilgi aktarımı ve geri besleme metotları ile kendi kendini gözler ve ayarlar/düzenler”(s. 127).

3.2.9 Artırılmış Gerçeklik (*Augmented Reality - AR*)

Sanal gerçeklik, gerçeği olduğu gibi sanal dünyaya taşımayı hedeflerken, artırılmış gerçeklik, gerçekliği sanal bilgilerle zenginleştirmeye odaklanmaktadır (Somyürek, 2014, s. 67 Akt: Öztuna, 2017, s. 78). Çeşitli simülatörler, pilot başlıkları, askeri haritalar, tıp vb. alanlarda kullanılmakta olan artırılmış gerçekliğin yakın gelecekte günlük yaşamda daha çok yer alacağı düşünülmektedir. Özellikle yapay zekâ uygulamaları ve otonom karar verme destekli robotik sistemlerin daha da yaygınlaşması ile entegrasyonu sağlanacak olan artırılmış gerçeklik makine-insan arayüzünün vazgeçilmez araçlarından biri haline gelebilecektir. Banger (2018b) ise sanal gerçeklik ile artırılmış gerçeklik arasındaki farkı şu şekilde ifade etmektedir: *Sanal gerçeklik* bilgisayarlar tarafından taklit edilmek suretiyle oluşturulan ortamlara denir. Çoğu sanal gerçeklik ortamı bir bilgisayar ekranı yoluyla edinilen görsel deneyimlerden ibarettir. *Artırılmış gerçeklik* ise gerçek dünyadaki çevrenin ve içindekilerin bilgisayar tarafından üretilen ses, görüntü, grafik ve GPS verileriyle zenginleştirilerek meydana getirilen canlı, doğrudan veya dolaylı fiziksel görünümdür (s. 51). Artırılmış gerçeklik için, sanal gerçekliğin çeşitli öğelerle desteklenerek daha işlevsel ve etkileşimli hale getirilmesidir de diyebiliriz.

Artırılmış gerçeklik; bilgisayar tarafından üretilen ses, görüntü ya da GPS’den elde edilen verilerin gerçek dünyadaki objeler üzerine eklenmesidir. Yani fiziksel olmayan (sanal) bir görüntünün genellikle üç boyutlu olarak modellenip gerçek zamanlı reel ortama yansıtılmasıdır. Başka bir deyişle; sanal ve gerçek olan nesnelerin aynı ortamda harmanlanmasıdır (Gürel, 2017, s. 55). Bu şekilde ortaya çıkan yeni “şey”, gerçek olanın teknolojik destekle daha ayrıntılı ve anlaşılır hale getirilmesi, detaylandırılması ve hatta yorumlanması olarak ifade edilebilir.

Artırılmış gerçeklik büyük alışveriş marketlerinde özellikle perakende satışlarda ve anlık stok takiplerinde de kullanılabilmektedir. Teknolojik inovasyon alanında birçok girişimin öncülerinden olan Walmart yine bu alanda da bir ilki

başlatmıştır. Nisan 2019'da Walmart'ın Akıllı Perakende Laboratuvarı Long Island, New York'ta açıldı. Artırılmış Gerçeklik destekli (AI-powered) mağaza, perakende teknolojilerini test etmekte ve envanteri gerçek zamanlı olarak izleyerek her ürünün daima stokta olmasını sağlamaktadır. 1,500 kamera ve sensör ile donatılan şeffaf camın arkasındaki yapı (Büyük Veri merkezi) alışveriş yapanlar tarafından görülebilmektedir. Müşterilerin, kullanılan teknoloji hakkında daha fazla bilgi edinebilecekleri bir *hoş geldiniz merkezi* ve bilgi istasyonu bulunmaktadır. Ayrıca, müşterileri hareket ettirmeye ve AI'nın müşteri hareketlerini nasıl analiz ettiğini görmeye teşvik eden etkileşimli bir ekranı da bulunmaktadır (<https://trendwatching.com/>) .

Yanlış ürünlerin pazarda yer alması sadece ekonomik kayba değil, aynı zamanda itibar kaybına da yol açacağından ilgili işletmenin daha fazla zarar görme riskini doğurmaktadır. Bu risklerin ortadan kaldırılabilmesi için, üretilip piyasalara sürülecek ürünlerin varyasyonları, sanal olarak tasarlanıp fiziksel üretime geçmeden önce artırılmış gerçeklik uygulamalarından faydalanılmaktadır. Yine aynı şekilde, ürün lansmanı ve tanıtımlarında, her yere fiziksel ürün göndermenin oldukça maliyetli olması sebebiyle sanal ürünler müşteriyle buluşturularak, hız ve maliyet avantajı elde edilebilmektedir (Apilioğulları, 2018, s. 24). Bu avantajların yanında ayrıca, iş güvenliği, insan kaynaklarından tasarruf, eş zamanlı sunum ve tanıtım kolaylığı, daha çok kişiye ulaşım ve ayrıca ürünü fiziki olarak satın almadan ürünü (kısmen de olsa) kullanma deneyimi imkânı sunulabilmektedir.

Dijital ortamların sanallaştırma kolaylığı ürünün fiziksel hale getirilmeden geliştirilmesi, yorumlanması, kontrol edilmesi, tanıtılması, kullanıcı deneyimi yaşatması gibi birçok avantajı da beraberinde getirmektedir. Artırılmış gerçeklik uygulamaları sayesinde hizmet ve ürünlerin simüle edilebilmesi sayılamayacak kadar çok avantaj sağlamaktadır. Bu nedenlerle işletmeler özellikle ürün geliştirme ve pazarlama alanlarında artırılmış gerçeklikten yararlanmayı önemsemektedir.

Gerek zaman gerek kaynak eksiklikleri nedeniyle yapılamayan faaliyetler sonucunda üretim süreçlerinde kayıplar ve değişkenliklerle karşılaşmakta ve devamında bu problemleri ortadan kaldırmak için Kaizen ve/ya Altı Sigma projeleri devreye sokulmaya çalışılmaktadır. Oysa bu problemlerin daha tasarım aşamasında öngörülebilir ve elimine edilebilir olmaları gerekmektedir (Apilioğulları, 2018, s.

158). İşi tersinden yapmak zaman ve maliyet kayıplarına yol açmaktadır. Bu kayıpların oluşmaması için proaktif çözümler üzerinde daha çok çalışılması gerekmektedir. Artırılmış gerçeklik ve sanal gerçeklik sayesinde ortaya konulan simülasyon çalışmalarını proaktif çözümler arasında görmek uygun olabilir. Bu bağlamda, kalite uygulamalarının kronolojik yapısına günümüzü temsilen “simülasyonda kalite” adımını yerleştirebiliriz (Şekil 40). Böylece ürün henüz ortada yokken, üretim aşamasından önce kaliteyi yakalama fırsatı doğmuş olacaktır.

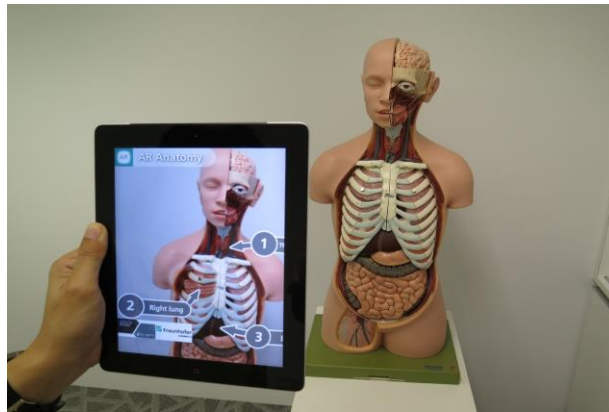
Şekil 40. Yıllara Göre Kalite Yaklaşımları

1920	1960	1985	2000	2020	
Kontrol (inspection)	Örnekleme (AQL)	Organizasyonel Odaklanma	Toplam Kalite Yönetimi (TQM)	Tasarımda Kalite (DFSS)	Simülasyonda Kalite (Artırılmış Gerçeklik)
Eski yöntem. Üretim sonrası kontroller			Kaliteyi Proseste Üret	Kaliteyi Tasarımda Yakala	Kaliteyi, Üretmeden Yakala

Kaynak: Apilioğulları, 2018, s. 158’den uyarlanarak geliştirilmiştir.

Sağlık hizmetlerinden eğitime kadar yaşamın her alanına girmesi beklenen artırılmış gerçeklik uygulamalarının insanoğlunun zamana karşı yarışında önemli bir yardımcı görevi üstleneceği düşünülmektedir. Artırılmış gerçekliğin kaynak kullanımının azaltılmasında ve riskli işlerin deneyimlenmesi ve icrasında büyük önemi bulunmaktadır. Şekil 41’de artırılmış gerçek’e yönelik bir görsel paylaşılmıştır.

Şekil 41. Artırılmış Gerçeklik



Kaynak: <https://pixabay.com/photos/augmented-reality-medical-3d-1957411/>,
Erişim: 31.05.2019

3.2.10 Akıllı Bina ve Şehirler (*Smart Buildings and Cities*)

İnsanların yaşamını daha kaliteli hale getiren, ucuz ve gelişmiş hizmet alabilmesini mümkün kılan, birçok otomatik sistemin mevcut olduğu, iletişim ve bilgi teknolojilerini kullanan şehirlere *akıllı şehir* denmektedir (Gürel, 2017, s. 61).

Küresel nüfusun yaklaşık %68'i, 2050 yılına kadar kentsel alanlarda yaşayabilir. Akıllı şehirler, yaşamımızı daha rahat, daha güvenli ve daha sürdürülebilir hale getirme sözü vererek, bu geleceğin bir parçası olacak (Weber, 2019). Artık rekabet içinde olan ülkeler değil, şehirlerdir. Her şehir kendini diğerlerinden ayırmak için rekabetçi bir avantaj kazanmak zorunda kalacak. Kaynaklarını çeşitlendirebilen ve vatandaşlarına ekonomik, sosyal ve kültürel fırsatlar sunabilen esnek ve çevik şehirler hayatta kalabilecektir (Okuy, 2018).

E 4.0 kavramının ortaya koyduğu bir diğer önemli konu ise akıllı bina ve akıllı şehirler'dir. Şehirleri akıllı yapmak ve insanların (hatta tüm canlıların) daha uygun şartlarda yaşayabilmesi E 4.0 ile mümkün gözüküyor. Özellikle büyük şehirlerde etkisini daha fazla hissedebileceğimiz bu kavram, bir şehrin zaman ve mekândan bağımsız olarak daha verimli yönetilebilmesini hedeflemektedir. Trafik azaltmak, otoyolları takip etmek, zamanında gelen toplu taşıma araçları vb. (Özdoğan, 2018, s. 31) örnek olarak verebiliriz. E 4.0, akıllı binalar (Şekil 42) ve akıllı şehirler (Şekil 43) sayesinde insan yaşamına sadece konforu getirmekle kalmayacak, aynı zamanda zamanın daha iyi kullanılmasından, verimlilik, her türlü güvenliğin sağlanması, sağlık hizmetlerinin iyileştirilmesine kadar bir çok fayda sağlayacaktır. Yalnızca akıllı trafik lambalarının, trafikte harcanan günlük kayıp zamandan bize 15-20 dakika geri vermesi bile başlı başına büyük bir kazanç olacaktır; trafikte daha az geçen zaman, ulaşacağımız yere zamanında erişim, daha az araç trafiği, daha az hava kirliliği ve daha az karbon salınımı, küresel ısınmanın azalması, yakıt tüketiminin azalması, yolların daha az yıpranması gibi ilk bakışta göremediğimiz onlarca katkı sağlayabilecektir.

Akıllı bina otomasyon sistemleri (Şekil 42), bina sistemleri yönetimini otomatikleştirmek ve iyileştirmek için çeşitli sensör bilgileri kullanır. Gün ışığı sensörleri, güneş ışığına bağlı olarak oda aydınlatmasını otomatik ayarlar. HVAC (Heating Ventilating and Air Conditioning) sistemleri ısıtma, soğutma ve havalandırmayı ayarlamak için sıcaklık, hava kalitesi ve kullanım bilgilerini kullanır.

Binalar, geçmiş kayıtlardaki doluluk oranlarına bakılarak doluluk için önceden soğutulur veya önceden ısıtılır. Asansör kontrol sistemleri, daha sonra çağrılacakları katlara en yakın asansörleri konumlandırmak için geçmiş tarihlerdeki asansör trafik kayıtlarını kullanır. Bu uygulama, asansör yanıtını hızlandırır ve asansör lobilerindeki tıkanıklığı azaltır. Akıllı bina sistemleri, ofis otelciliğinin etkin bir şekilde uygulanmasını kolaylaştırır. Akıllı bina akıllı telefon uygulamaları, paket teslimatları, bekleyen teslimat bildirimi ile birlikte işçinin meşgul olduğu alana otomatik olarak yönlendirilebilir (Ptolemy Project, 2012).

İngiltere'nin Milton Keynes kasabasında uydu görüntüleri kullanılarak, "çarpık kentleşme"nin büyümesi denetleniyor ve yapılaşmalardaki gelişmelerin, stratejik planlarla ve mevzuatlarla uyumlu hale getirilmesi için çalışmalar gerçekleştiriliyor. Sensörler, şehir genelinde trafik akışlarını takip ediyor ve bu verilerle sürücüleri trafik sıkışıklığına karşı uyarıyorlar. Bu veriler aynı zamanda gelecekteki şehir trafiği planlamasında da kullanılmak üzere değerlendiriliyor. Akıllı sokak aydınlatması teknolojisi, insanların gece ne zaman ve nerede yürüdükleri hakkında verileri toplayarak güvenlik için gerekli olduğu vakitlerde aydınlatma sağlıyor, gerekli olmadığında ise enerji tasarrufuna gidiyor. Su ve enerji kullanımı hakkındaki veriler, talebi daha iyi anlamak ve tedarik planlamasına yardımcı olmak için toplanıyor. Şehirde yaşayanların sosyal medya kullanımı incelenerek, uygulanan ve geliştirilmekte olan projelerle ilgili düşüncelerinin neler olduğu öğrenilerek değerlendirmeye alınıyor. Ayrıca, kent yetkililerinin ve mercilerinin, İngiltere'deki diğer şehir ve kasabalara kıyasla vatandaşlarıyla ne kadar iyi iletişim kurduğunu karşılaştırmak amacıyla, diğer alanlardaki sosyal medya kullanıcıları da takip ediliyor (Mar, 2017, s. 158-159).

Şekil 42. Akıllı Binalar

Kaynak: <https://pixabay.com/illustrations/home-smart-automation-house-system-4100193/>, Erişim: 11.03.2020

Şekil 43. Akıllı Şehirler

Kaynak: <https://pixabay.com/photos/smart-city-communication-network-4168483/>, Erişim: 11.03.2020

3.2.11 Üç Boyutlu (3B) Yazıcılar (3D Printers)

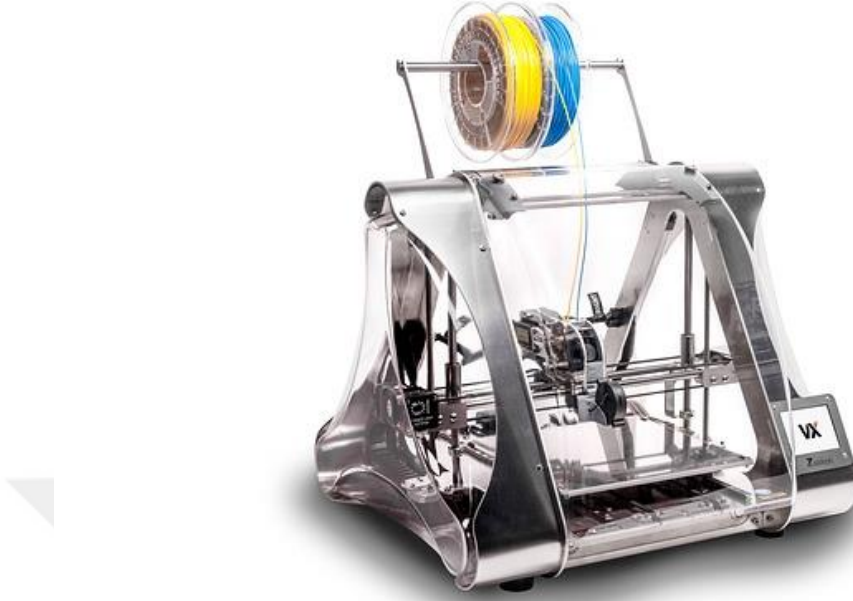
Üç boyutlu yazıcıların (3B) temel amacı üç boyutlu olarak tasarlanmış nesnelerin hayata geçirilmesidir. Bu anlamda 3B yazıcılar Endüstri 3.0 ile yoğun bir şekilde kullanılmakta olan CNC (Computer Numerical Control) tezgahlarının E 4.0'a uyarlanmış halidir denilebilir. 3B yazıcıların üstünlüğü, daha doğrusu en büyük farklılığı ise nesne üretiminde kullanılan materyallerin ihtiyaca uygun olarak canlı dokulardan dahi oluşturulabilecek olması ve en ince ayrıntılarıyla hassas bir şekilde işlenebilmesi ve üretilmesidir.

3B yazıcılar ve Nesnelerin İnterneti ile birlikte herkes üretici olabilme imkânı elde edebilmektedir. 3B yazıcılar ile hızlı bir şekilde birçok tasarım ürün elde etme imkânına ulaşılması, esnek üretime de yeni ilerlemeler getirmektedir. 3B teknolojisi sayesinde maliyetlerin de düştüğü görülmektedir (Öztuna, 2017, s.65).

3B yazıcılar, kendi yedek parçalarını kendileri basabilir. Pahalı bir iş olan takım yenileme çalışmaları için para ve zaman harcatmaz. 3B yazıcılarla, yalnızca tek bir ürün üretilbileceği gibi gelen siparişler doğrultusunda ve en az maliyetle küçük partiler halinde de üretim yapılabilir. Merkezi fabrikaların sermaye-yoğun ölçek ekonomileri ve yüksek maliyetli sabit üretim hatları seri üretim için tasarlanmıştır ve aynı üründen tek bir adedi de yüz bin adetlik partinin tek adedini de aynı fiyata üretebilen 3B üretim süreciyle rekabet etmesi ve baş etmesi imkânsızdır (Rifkin, 2015, s. 99).

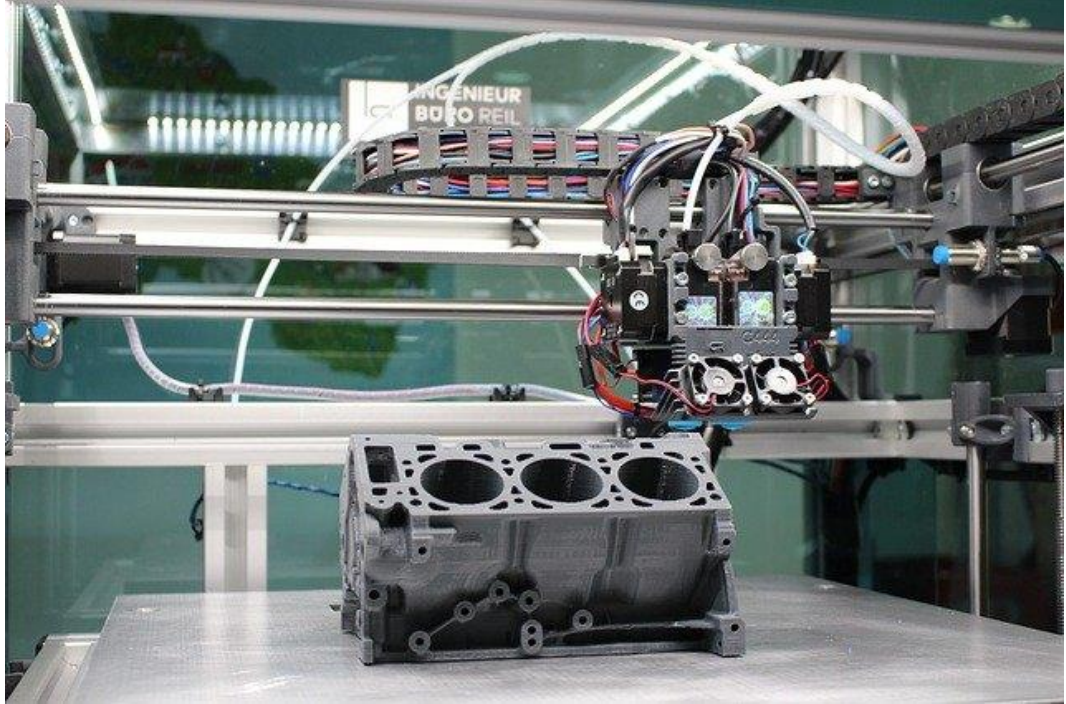
Oyuncak sektöründen tıp dünyasına kadar farklı alanlarda kullanılabilen 3B yazıcılar daha şimdiden endüstrideki yerini almış durumdadır. En ince detayların çizildiği bilgisayar uygulamalarındaki şekilleri üç boyutlu olarak fiziksel ortama transfer etmek artık mümkün gözükmektedir. Yakın gelecekte yapay insan organı üretiminde de kullanılacağı belirtilmekte olan 3B yazıcıların nano teknolojiler sayesinde canlı hücreleri de enjekte etmesi çok uzak bir ihtimal gibi durmuyor. Teknolojinin ilerlemesi buna mukabil maliyetlerin düşmesi sayesinde, yakın gelecek zaman diliminde evlerimizde yerlerini alacak olan 3B yazıcılar ile internet üzerinden satın alacağımız hazır kod grafikler ile kendi elbisemizi kendimiz basabileceğiz. Şekil 44 ve Şekil 45 3B yazıcılara iki farklı görsel örnek olarak verilmiştir.

Şekil 44. Üç Boyutlu (3B) Yazıcılar - Örnek I



Kaynak: <https://pixabay.com/photos/3d-printing-3d-printer-technology-3800204/>,
Erişim: 11.03.2020

Şekil 45. Üç Boyutlu (3B) Yazıcılar - Örnek II



Kaynak: <https://pixabay.com/photos/industry-technology-machine-3d-3225119/>,
Erişim: 11.03.2020

3.2.12 Proaktif Önlemler (*Proactive Prevention*)

E 4.0 çatısı altında çalışan sistemlerde ya da E 4.0 bileşenlerinde uygulanmak istenen önemli yaklaşımlardan birisi, kendi kendini kontrol etme (self-control) ve özerklik (self-determination) olarak adlandırabileceğimiz sürekli ve anlık bilgi akışı sayesinde izlenen sistemlerde meydana gelebilecek bir hata, arıza, duraklama ya da karmaşa için otonom karar verme mekanizması ile iş süreçlerinin kesintiye uğramadan devam edebilmesini sağlamak, yani proaktif önlemlerdir. Bir makinenin ya da malzemenin kullanım ömrü, sıcaklık, ısı, nem vb. özelliklerinden hareket ederek (arşiv kayıtlarının da benzer şekilde gözden geçirilmesi sayesinde) ne zaman bir kesintiye yol açabileceğinin tahmin edilmesi ve bunun önceden yönetim kademesine ve ilgili kişi ve teknisyenlere rapor edilebilmesi proaktif önleme yaklaşımlarının artık büyük oranda başarabildiği bir durumdur. Bu sayede iş kayıplarının en aza indirgenmesi, müşteri memnuniyetinin ise en üst seviyeye çıkartılması hedeflenmektedir.

Üretim hattı simülasyonu ve benzeri bazı kurgusal simülasyonlar sayesinde fiziksel sistem daha kurulmadan bilgisayar üzerinde sanal olarak kurulup çalıştırılabilmektedir. Böylece kurulacak fiziksel sistemin en iyi şartlarda oluşturulması için gerekli ön hazırlık yapılmış olmaktadır. Akıllı makinelerin (ve sistemlerin) kendi durumunu izliyor olması, “önleyici bakım” konusunda ihtiyaç duyulan verileri sağlamaktadır. Makinenin kendisinde veya işlemekte olduğu malzemede herhangi bir arıza oluşmadan operatöre ve bakım-onarım takımına gönderilen durum iletileri ile gerekli önlem alma girişimi otonom olarak gerçekleştirilmektedir. Sonuç olarak henüz sistemde arıza oluşmadan düzenlenebilen bakım ve erken müdahale ile makinenin durma süresi azaltılmış ve üretim kesintiye uğramamış olur (Banger, 2018b, s. 46-47). Bilişim sistemlerine yönelik siber saldırılarda da yine aynı mantıkla sisteme entegre edilen anlık izleme aygıtları ile ağ üzerindeki veri trafiği ve davranışlar izlenerek, saldırı daha gerçekleştirilmeden sistem alarm durumuna geçirilebilmekte ve gerekli manevralar (cihazların ağ bağlantılarını kesmek de dahil) sistem tarafından kendiliğinden uygulanabilmektedir.

E 4.0 çatısı altında yer alan diğer önleyici önlemler için dikey, yatay ve çok yönlü (uçtan uca) entegrasyondan söz etmek mümkündür. Yatay entegrasyon dış, dikey entegrasyon ise iç işbirliğini ifade ederken çok yönlü entegrasyon ise her

ikisinin birlikte uygulanmasıdır. Banger (2018b), işletme içi dikey entegrasyon sayesinde üretim alanı ile yönetim-ofis kademesi arasındaki kopukluk ve ilişkisizliğin ortadan kalkarak verimliliğin artacağını, yatay entegrasyon ile hammadde tedarikçilerinden teçhizat üreticilerine kadar kaliteli bir işbirliği sayesinde işletmenin ekosistemindeki dış paydaşlarla entegrasyonun daha rahat sağlanabileceğini ifade etmektedir (s. 47).

Bilişim teknolojileri yönünden proaktif önlemler için bu çalışmamızda "Bilgi Güvenliği" bölümü altında yer alan şu başlıklara da ayrıca bakılabilir:

2.5.12 Siber Saldırlara Karşı Güvenlik (*security against cyber attacks*)

2.5.12.1 Bilgi Güvenliği Yönetim Sistemleri (*Information Security Management Systems - ISMS*)

2.5.12.2 Saldırı Tespit/Önleme Sistemleri (*Intrusion Dedection System-IDS, Intrusion Prevention System-IPS*)

2.6.5 Siber Olaylara Müdahale Ekipleri (SOME)

3.3 İşletmelerin Endüstri 4.0'a Adaptasyonu

Banger (2017a) işletmelerin daha çok insan kaynakları yetersizliği, ilgili teknolojilerin nasıl uygulanacağını ve adapte edileceğinin tam olarak bilinmediği, yatırım ve risk çekinceleri gibi bir çok nedenden dolayı E 4.0'a entegrasyonda zorlandıklarını ifade etmektedir. Ayrıca konuyla ilgili yapılan birçok çalışmanın akademik boyutta ve buna bağlı olarakda teknik bilgiler içerdiği, işletmelerin önlerine alabilecekleri ve takip edebilecekleri bir yol haritasının ve iş süreçlerinin açıkça ortaya konulmadığını belirtmektedir. Yine bu açıklamalara bağlı olarak dönüşümün nasıl gerçekleştirilebileceğine dair şunları dile getirmektedir:

Yeni pazar ve teknoloji şartlarında pazardaki müşteri taleplerinin karşılanmasına ve pazara yenilikçi ürün-hizmet sunumlarının yapılmasına yönelik konuların başında bilişim-iletişim teknolojileri (BİT) gelmektedir. Bu konu iki farklı işletme fonksiyonu ile ilişkilendirerek ele alınabilir. Birincisi; inovasyona ve ürün geliştirmeye yönelik olarak BİT'ten yararlanma, ikincisi ise imalat sürecinde BİT kullanımıdır. Bu iki konunun yerine getirilmesi, anılan bu fonksiyon ve süreçleri -sonuçta işletmenin tamamını- akıllı hale dönüştürür. Söz konusu dönüşüm, günümüz iş dünyası için vazgeçilmezdir. Rakiplerin rekabetçi üstünlüklerini tekdüze geliştirmeleri ve pazar-müşteri şartlarının ürün-hizmet, hız, çeşitlilik ve yenilik olarak evrimleşmesi işletmeleri yapısal dönüşüme zorunlu kılmaktadır. Bu doğrultuda, E 4.0'ın dayanakları olan teknolojilerin kullanımı ile yaratılan Akıllı Fabrika'da inovasyon, operasyonel mükemmeliyet ve müşteri sadakati hedeflerini gerçekleştirmek üzere çeşitli çözümler uygulanabilir. Tesis zekâsının altyapısını akıllı ve bağlantılı nesneler (sistemler, cihazlar vb.) oluşturmaktadır. Böylece işletmenin her noktasından veri toplamak, bunları işlemek ve depolamak

mümkün olabilmekte, bu verilerin gerçek zamanlı analizi ve işlenmesi geleceğe ilişkin öngörüler geliştirerek olası sorunları tespit etme ve çözümler üretme için senaryolar yaratma ve simülasyonlar oluşturma imkânı sunmaktadır. Sonuçta bu şekilde daha yüksek yönetim performansına ulaşma imkânı sağlanmış olur. İşletmenin dönüşümü sadece teknolojinin değişiminden ibaret değildir. İşletmede teknolojik donanım ile ilgili görev yapan çeşitli kullanıcılar ve yararlanıcılar bulunmaktadır ve bunların ihtiyaçlarını doğru anlamak işletmenin insan kaynağı verimliliğini artırır. Dolayısıyla akıllı fabrikaya dönüşürken uygulanacak çözümlerin insan kaynağı ihtiyaçları dikkate alınarak yapılması gerekmektedir.

Davenport (2014) Büyük Verinin birçok yeni enformasyon teknolojisi gibi maliyetlerde çarpıcı düşüşler, hesaplama işlemlerinde önemli zaman tasarrufları getirebileceğini (s. 68), bir kuruluşun Büyük Veri kullanımı ile ilgili yapabileceği en iddialı şeyin onu veriye dayalı yeni ürün ve hizmet teklifleri geliştirmekte kullanması gerektiğini (s. 73), iş kararlarını destekleme açısından ise; bir müşteriye hangi tekliflerin sunulması gerektiği konusunda, yakında müşteri olmayı bırakma ihtimali en yüksek olan müşterilerin tespit edilmesinde, depolarda ne kadar stok tutulacağını hesaplanması ve ürünlerin nasıl fiyatlandırılacağı (s. 75) konusunda Büyük Verinin kullanımının önemine dikkat çekmektedir. Bu açıklamalar doğrultusunda, E 4.0'ın en önemli bileşenlerinden biri olan Büyük Verinin işletmelerin E 4.0'a dönüşümü konusundaki önemi bir kez daha ortaya çıkmış oluyor.

Üst düzey yönetim ya da strateji üreten kişilere giden bilgiler ile daha farklı bir strateji, daha farklı bir organizasyon hedeflenebilir çünkü daha önce hiç fark etmedikleri bir bilgiye E 4.0 bileşenlerinden olan Büyük Veri ve veri analitiği sayesinde kavuşmuş olabilirler. Bu durumdan pazarlama ve satış bölümleri de aynı şekilde etkilenecektir. Müşterilerle ilgili çarpıcı ve yeni verilerin elde edilmesi yeni taktikler geliştirmede kullanılabilir. Eğer ilgili veri, kurumsal kaynak planlaması (ERP) sistemini de etkileyebilecek şekilde bir sunum içeriyorsa o zaman organizasyon içindeki her bölümün etkilenebileceğini de söylemek mümkün olabilecektir (Özdoğan, 2016, s. 47).

İşletmelerin E 4.0'a dönüşümü ve özellikle yapay zekâ alanındaki çalışmalar için; yazılımcıların, istatistikçilerin ve matematikçilerin yanı sıra sağlık hizmetlerinde çalışanların ve nörologların birlikte çalışmalarına ihtiyaç duyulmaktadır. Gürel (2017)'in kuantum bilgisayarların üretimi için vermiş olduğu şu örnekte de benzer bir yaklaşımı görmek söz konusudur: E 4.0, disiplinlerarası çalışmalara ihtiyaç hissettiğinden, bilim insanlarının bakış açıları da değişecektir.

Farklı disiplinlere ait bilgiler belirli yöntem ve çalışmalarla bir araya getirilerek mevcut soruna yeni bakış açıları kazandırılıp, var olan soruna birçok yönden ışık tutabilecektir. Örneğin; kuantum bilgisayarlar üretebilmek için matematikçi, fizikçi, bilgisayar mühendisi, elektrik mühendisi, metalürji ve malzeme mühendisi gibi uzmanları buluşturmaya ihtiyaç duyulmaktadır (s. 58).

Mevcut teknolojilerin ötesine geçen donanım ve yazılım bileşenleri, ara katman yazılımı ve işletim sistemleri geliştirilmelidir. Donanım ve yazılım, bileşenlerden tutun da tamamen tümleşik sistemlere kadar oldukça güvenilir, yeniden yapılandırılabilir ve gerektiğinde sertifikalandırılabilir olmalıdır. Bu tür karmaşık sistemler, günümüz siber altyapılarının çoğunda bulunmayan bir güvenilirliğe sahip hale getirilmelidir. Örneğin, sertifikasyonun havacılık sektöründe yeni, kritik güvenlik sistemleri geliştirmek için gereken kaynakların %50'sinden fazlasını tükettiği tahmin edilmektedir. Tıp, otomotiv, enerji sistemleri ve diğer uygulama alanlarında da benzer çabalara ihtiyaç vardır. Aşırı tasarım şu anda güvenli ve başarılı bir sistem sertifikası ve dağıtımına giden tek yoldur. Yine de bu yaklaşım, karmaşık tasarımlar ve birlikte çalışabilirliğin gerekli olduğu sistemler için hızla anlaşılabilir hale gelmektedir. “Para tükenene kadar” testi uygulanabilir bir strateji değildir ve sistem güvenilirliği hakkında akıl yürütmek için bilime ve kanıta dayalı yöntemlere ihtiyaç vardır. Kontrol tasarım aşamasında yazılım ve sistemlerin doğrulanması ve onaylanmasını içerecek yeni modeller, algoritmalar, yöntemler ve araçlar gereklidir (Baheti ve Gill, 2011).

Yalınlık; sürekli iyileştirme ve insanlara saygı şeklinde, müşteriye değer akışını teşvik eden bir iş metodolojisidir. Bir işletme, E 4.0 dönüşümünü uygulamadan önce yalın felsefenin ortaya koymuş olduğu gereklilikleri büyük oranda yerine getirmiş olmalıdır (Banger, 2018b, s. 147). İşletmelerin E 4.0'a geçişi için yalın yönetim ve toplam kalite yönetimi uygulamaları ön şart olmamakla birlikte kurum kültürünün önemli bir eksikliği olacağından dijital ve endüstriyel dönüşüm sürecine geçilmesi oldukça zor olacaktır. E 4.0 BİT üzerine kurulu olsa da, işletmelerin temel felsefelerinden olan kurum kültürünün olmayışı ayakta durmayı güçleştirecektir. E 4.0, kendi döneminden önce işletmelerde süregelen bazı değerleri de bünyesinde taşımakla mükelleftir. Bu değerlere örnek olarak; toplam

kalite yönetimi, Kaizen, JIT, esnek yönetim, yatay hiyerarşi, kurum kültürü geliştirme, insana saygı ve müşteri öncelikli yaklaşımlar vb. sayılabilir.

İşletmelerin E 4.0'a dönüşüm süreçlerinde E 4.0 öncesi dönemden bağımsız hareket etmelerinin zor olacağı daha önce ifade edilmişti. Kurum kültürü oluşturamamış işletmelerin dijitalleşme süreçlerini tamamlamalarını ve E 4.0 dönüşümünü gerçekleştirmelerini beklemek pek de mümkün gözüküyor. Banger (2018b, s. 205-206)'e göre, bir işletmenin kültürel anlamda dijital olarak nitelendirilebilmesi için şu temel ilkeleri sağlaması gerekiyor:

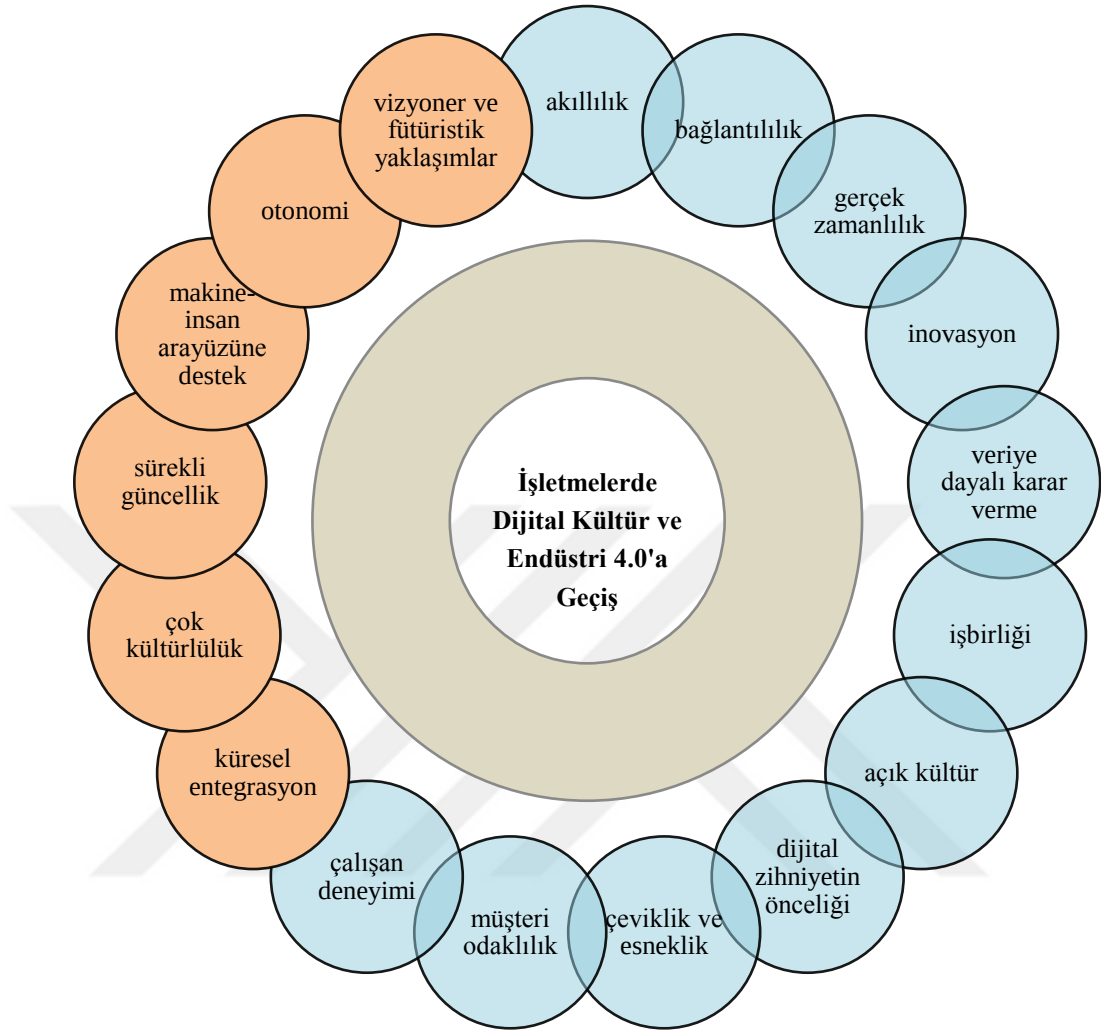
- Akıllılık (yapay zekâ vb.)
- Bağlantılılık (yerel ağ ve internet bağlantıları vb.)
- Gerçek zamanlılık
- İnovasyon
- Veriye dayalı karar verme
- İşbirliği
- Açık kültür (dış ağlarda -tedarikçi-müşteri-girişimci- ortaklıklar)
- Dijital zihniyetin önceliği
- Çeviklik ve esneklik
- Müşteri odaklılık
- Çalışan deneyimi

Bu temel özelliklere şu alanların da ilave edilmesi mümkündür:

- Küresel entegrasyon
- Çok kültürlülük (farklı kültürlerden insan kaynakları ve ürün ve hizmetlerin farklı kültürlerde de kabul görmesi)
- Sürekli güncellik
- Makine-insan ara yüzüne destek
- Otonomi
- Vizyoner ve fütüristik yaklaşımlar

E 4.0'a dönüşümde işletmelerin bağlantı halinde olması gereken bu öncelikli alanlar, işletmelerde dijital kültür özelliğini meydana getirmiş olacak ve geçişi büyük oranda kolaylaştıracaktır. İşletmelerde dijital kültür özellikleri Şekil 46'da görsel olarak ifade edilmeye çalışılmıştır.

Şekil 46. İşletmelerde Dijital Kültür Özellikleri



Kaynak: Banger, 2018b, s. 205-206'den uyarlanarak geliştirilmiştir.

E 4.0'a yön veren Silikon Vadisi'ndeki teknoloji devleri Google, Apple, Microsoft, IBM, Amazon ve Facebook *mümkün gelecekler üzerinden tasarımlar* yapıyor ve bu tasarımları hayata geçiriyorlar. 2016 yılında yapay zekâ alanında güçlerini birleştirme kararı alan bu ortaklığın adı "İnsan ve Toplum Yararına Yapay Zekâ Üzerinde İşbirliği". Bahsi geçen bu ortaklığın ana gayesi; insanlığın ve gezegenimizin faydasına olacak şekilde yapay zekâ araştırmalarına dair etik, şeffaflık, güvenilirlik ve gizlilik gibi alanlarda en iyi uygulamaları üretmek üzere teknoloji standartlarını belirlemek olduğu ifade edilmektedir (Gürel, 2017, s. 56). Bu alanda en iyi olan firmaların (iyi niyetli olmak kaydıyla) birlikte çalışma kararı almaları, kimin ne yaptığının bilinmesi ve faaliyet çerçevesinin ortaklaşa çizilerek

kontrol altına alınması, güvenli süreçlerin devamı açısından önemli sayılabilecek bir girişim olarak yorumlanabilir.

E 4.0 kavramını daha dar anlamı ile, yani günümüzde kullanıldığı şekliyle (üretimde dijital teknolojilerin kullanımı olarak) düşünecek olursak; artan rekabet ürün çeşitliliğini, farklı tasarımları, hızlı ve hatasız üretimi, gecikmelerin yaşanmadığı bir tedarik zincirini zorunlu kılmaktadır. Bu noktaya ancak E 4.0 teknolojileri sayesinde ulaşmak mümkün gözükmektedir. Verimlilik ve karlılığa ise veriye dayalı olarak hızlı karar alıp üretimdeki dinamığa anında müdahale ile yaklaşılabilecektir (Meydanlı, 2018, s. 346).

3.4 Endüstri 4.0'ın Önündeki Engeller

E 4.0 sunduğu sayısız avantajlarla birlikte bir takım zorlukları da beraberinde getirmektedir. E 4.0 kapsamındaki teknolojilere uyum sağlayabilmek ve kurumların bunları bir şirket kültürü haline getirebilmesi bu zorlukların başında yer almaktadır. Ayrıca, kurum için ihtiyaç duyulan insan kaynağının kurum içinde yer alabilmesi ihtiyacı da diğer bir zorluğu oluşturmaktadır. E 4.0'ın henüz bu başlangıç aşamalarında, sanal ve fiziksel dünyaların bir araya getirilerek entegrasyonları, uygulama zorlukları, yönergeler ve stratejik kapasiteler, beceri, kültür, standartlar ve bu alanlardaki hazır olma seviyeleri gibi birçok alanda çeşitli zorluklar bulunmaktadır (Kulabaş, 2017).

E 4.0'ın en önemli bileşenlerinden biri olan Nesnelerin İnterneti'nde her akıllı ürün bağımsız olarak tanımlanabilir ve ağdaki diğer nesneler ile iletişime geçebilir olmalıdır. Bu iletişim ve akıcılığın sağlanabilmesi için standart iletişim protokollerinin kullanılması gerekmektedir. Ancak, farklı teknoloji üreticilerinin (farklı model ve markalarla) üretmiş olduğu sensör, aktüatörler ve iletişim modüllerinin hepsinin tanımlanmış standart iletişim protokolleri üzerinden haberleşmesi her zaman mümkün olmamaktadır. Nesnelerin birbirleri ile uyumlu çalışabilmesi IoT ağlarının en öncelikli sorunlarının başında yer almaktadır. Bu sorundan kurtulabilmek için nesnelerin standart web iletişim protokolleri üzerinden iletişime geçebilmeleri konsepti WoT (Web of Things) ortaya çıkartılmıştır (Apilioğulları, 2018, s. 20-21).

E 4.0'ın önündeki engelleri uzun listeler hazırlayarak anlatmak elbette mümkün olmakla birlikte kavramsal yaklaşım ile engellerin kümeler şeklinde

sunulmasının daha faydalı olacağını düşünmekteyiz. Bu nedenle E 4.0 için engel oluşturan (şimdilik bilinen ya da görünen engeller) konuları şu başlıklar altında vurgulamak uygun olacaktır:

- Yatırım Maliyetlerinin Yüksek Olması
- Yetişmiş (Donanımlı) İş Gücü Eksikliği
- Standartların Geliştirilmesi Gerekliliği
- Veri Güvenliği Riskleri
- Değişime Direnç

Yatırım Maliyetlerinin Yüksek Olması: Ülkelerin neredeyse tamamına yakın bir kısmında işletmelerin %90'ın üzerinde küçük ve orta büyüklükteki işletmeler'den (KOBİ) oluştuğunu düşünecek olursak, maddi kaynak açısından yetersiz olan (özellikle mikro ve küçük ölçekteki işletmeler) bu işletmelerde E 4.0 için teknolojik altyapıyı oluşturmak çok kolay bir girişim olarak gözükmüyor. Bu yatırımı yapabilecek maddi kaynak yeterliliğine sahip olan işletmelerin ise Endüstri 3.0'a yapılan yatırımlardan kolay kolay vazgeçmek istememeleri ve E 4.0'ın neler getirebileceğini tam olarak kavrayamamış olmalarını göstermek mümkündür. Az gelişmiş ve gelişmekte olan ülkelerin önemli bir bölümünün henüz Endüstri 2.0'ın sonları ile Endüstri 3.0'ın başlarını yaşadıkları göz önüne alınacak olursa, onlar için E 4.0'a maddi kaynak ayırıp yatırım yapmak şimdilik imkânsız gözükmemektedir.

Yetişmiş (Donanımlı) İş Gücü Eksikliği: Yatırım maliyetlerinin yüksek olması için açıklanan sebeplerin neredeyse tamamı yetişmiş iş gücü eksikliği için de geçerlidir. Bilişim teknolojileri uzmanları, entegrasyon yapılar için deneyimli personel, veri analitiği uzmanları, yazılımcı, teknik eleman ve mühendis açığı bulunan işletmeler için insan kaynakları havuzundaki tecrübeli ve donanımlı personel sayısındaki eksiklik temel engellerden birini oluşturmaktadır. İş yaşamında olan ve tecrübe sahibi kişilerin kuşak olarak teknolojiden kısmen de olsa uzak olması (ya da uzak durması) bu alandaki eksikliği biraz daha sorunlu hale getirmektedir. E 4.0'a doğru dönüşüm sağlamak isteyen işletmelerin şimdiden kendi personel havuzundan uygun olan kişileri gerek hizmet içi eğitim, gerekse hizmet satın alma yöntemleri ile hazırlaması gerekmektedir. Şimdilik dış kaynak kullanımı (outsourcing) ile giderilmeye çalışan bu açık sürdürülebilir bir yöntem olarak

gözükmemektedir. Arz talep dengesinin yakın gelecekte iyice bozulacağı düşünülecek olursa bu alanda dış kaynak kullanımının işletmelere çok yüksek bir maliyete mal olacağını söyleyebiliriz ki, bu durum geçiş sürecini (E 4.0'a geçiş için yeterli maddi imkânların olmayışı, yetersiz insan kaynağı ve insan kaynağı maliyetlerinin yeniden yükselmesi) kısır döngüye sokacaktır.

Standartların Geliştirilmesi Gerekliği: Standartları teknolojik uyumluluk ve süreçlerin yönetimi olarak iki farklı şekilde değerlendirmek gerekir. Farklı marka ve üreticilerin üretmiş oldukları cihaz ve ürünlerin özellikle Nesnelerin İnterneti aracılığı ile iletişim kurmada kullanmış oldukları protokollerin standart hale getirilememiş olması bu alan için temel sorunu teşkil etmektedir. Verilerin toplanabilmesi ve gerekli yerlere iletebilmesi açısından ortak bir iletişim protokolünün geliştirilmiş olması gerekmektedir. Her ne kadar bu sorun üzerinde ciddi çalışmalar yapılıyor olsa da, teknolojik üstünlük ve rekabet avantajını kaybetmek istemeyen ve bu alanda önde gelen gelişmiş ülkelerin tutumları bu sorunun kolay ve hızlı bir şekilde çözümlenebilmesini zorlaştırmaktadır.

Veri Güvenliği Riskleri: E 4.0'ın ana bileşenlerinden olan Büyük Veri, bulut bilişim ve siber güvenlik çerçevesinde devam eden ve büyük riskler içeren veri güvenliği, karşıt teknoloji kullananların (hacker vb.) da aynı hızda, hatta bazen daha ileri teknikler kullanarak ilerlemesi, bu alandaki sorunların daha uzunca bir süre devam edeceğini göstermektedir. Kriptoloji alanındaki önemli gelişmeler; uçtan uca uygulamalar (P2P), iki faktörlü kimlik doğrulama (2FA), 256 bitlik şifrelemeler, SHA şifreleme algoritmaları, blockchain teknolojisi (dağıtık ve merkezi olmayan yapılar) bu alana önemli güvenlik artırıcı katkılar sunuyor olsa da yakın zamanda kullanıma daha çok girecek olan süper bilgisayarlar ve kuantum bilgisayarlar sayesinde yapılacak tersine mühendislik saldırıları sebebiyle veri güvenliği riskleri daha da artabilecektir. E 4.0'ı dünyaya hediye eden ülkenin (Almanya) parlamentosunda bu risklerden korunabilmek için (kullanımını ve varlığını neredeyse unutmuş olduğumuz) daktiloların yeniden kullanılmaya başladığını şimdiden görmekteyiz. E 4.0'ın ruhuna aykırı olan bu tutumun üstelik Almanya'dan gelmesi, üzerinde düşünülmesi gereken bir konu!

Değişime Direnç: E 4.0'dan bağımsız olarak bildiğimiz ve üzerinde onlarca çalışma yapılan değişime direnç konusu E 4.0 ile yeniden karşımıza çıkmaktadır.

Yukarıda açıklanan başlıklar aslında değişime direnç için önemli ölçüde sebep oluşturmakta ve çalışanların ya da yönetimlerin E 4.0'a karşı bir direnç geliştirmesine sebebiyet vermektedir. Değişime direncin kırılabilmesi için yeterli insan kaynağı, değişimin neden gerekli olduğunun iyi anlatılması, değişim sonucu elde edilecek kazançlar ve değişim gerçekleşmediğinde ortaya çıkabilecek kayıp ve riskler açık bir şekilde ilgili kişilere ve paydaşlara anlatılmalıdır. Direncin önüne geçmek için; Toplam Kalite Yönetimi'ne benzer yaklaşımlar uygulanmalı ve üst yönetimin sürece sahip çıkması gerekmektedir.

Özdoğan (2018) E 4.0'a taşınmak isteyen işletmelerin her şeyden önce, birinci sırada iş süreçlerini düzgün tasarlamalarını, daha sonra E 4.0'a geçerek bu yeni teknoloji uygulamalarının eklenerek fabrikaların akıllı fabrikalara dönüştürülmesini (s. 32), bu sayede, makinelerin ürettiği veri ve Kurumsal Kaynak Planlama (Enterprise Resource Planning [ERP]) sistemlerinin birleştirilerek ve gerçek zamanlı stok ve tedarik takibini daha önce hiç olmadığı gibi yönetebileceklerini (s. 53) ifade etmektedir.

Şu anda bilgisayar teknolojisi diğer tüm alanlara yayılmakta ve yenilenebilir enerji, 3B üretim, çalışma dünyası, pazarlama, lojistik, ulaştırma, sağlık ve çevrimiçi yükseköğrenim alanlarının iletişim mecrası haline gelmektedir. Toplumu yeni baştan düzenleyen yeni bilişim dili çok farklı "çıkar gruplarını" bir araya getirmektedir. Bu grupları birleştiren, bir araya getiren bağ ise, işbirliğine dayalı *açık kaynak ekonomisi* ve *yönetimde ortak kaynaklar modeli*'ne duydukları inançtır. Bununla birlikte piyasalar her ne kadar tamamen ortadan kalkmamış ve devlet tamamen denklemin dışına çıkmamış olsa da bu yeni hareketler eş düzey bireyler arası *ortak kaynak yönetimi*'nin üstünlüğüne sadakatle bağlıdır. Sıfıra yakın marjinal maliyetli toplum idealini engellemek yerine bu ideali gerçekleştirmekte kullanılabilecek en iyi yönetim modelinin bu olduğu düşünülmektedir (Rifkin, 2015, s. 186). E 4.0 ise bu çitayı bir adım daha ileriye taşıyarak sıfıra yakın marjinal maliyetli toplum idealine önemli katkılar sunarak sürece öncülük etmektedir. Ortak kaynak yönetimi konusunda, sanılanın aksine, insanlar ortak kaynakları yönetmede daha bilinçli, adil ve kurallı yönetimdeki optimum kararlara çok yakın kararlar verebildiği/alabildiği kuramına dayanmaktadır. İnsanların kendi başlarına bunu (devlet ve özel sektöre oranla) daha iyi yapacağını öne süren bu kurama en önemli yeni bir destek ise

makine-insan ara yüzü sayesinde yakın gelecekte hayata geçirilebilecektir. E 4.0 kavramı içerisinde yer alan bulanık mantık, yapay zekâ, yapay sinir ağları, makine öğrenmesi ve otonom karar mekanizmaları işbirliğinde bu arayüz yakın gelecekte tahmin edilenlerin çok daha ötesinde, iş süreçlerini en ileri seviyede optimize edebilecektir.

Siber güvenlik açısından E 4.0'ın önündeki engellere örnek olarak Bochman (2018) şunları paylaşmaktadır; bir şirket, güvenlik açısından genel çerçevenin ilk aşaması olan kurumun donanım ve yazılım varlıklarına dair envanteri bile yeterince oluşturamamışsa bu çok ciddi bir eksikliktir, zira sahip olduğunuzu bilmediğiniz bir şeyin güvenliğini sağlayamazsınız (s. 45). Bochman'ın bu ifadelerinden öyle anlaşılıyor ki, bazı kurumlar daha nelere sahip olduklarını detaylı ve doğru bir şekilde tespit edemiyor. Bu durum belki E 4.0'a geçebilmenin değil ama onun güvenli bir şekilde uygulanmasının önünde engel gibi duruyor.

Karar otomasyonları da bazen mantıksız ve kontrolsüz çalışabilmektedir. 06 Mayıs 2010 tarihinde New York borsasında “flash crash” esnasında bu durum yaşanmıştır. Algoritmik alış-veriş yapan algoritmalar kısır döngülere girerek yoğun satışlara neden olmuştur. Yirmi dakika içerisinde borsanın kendisini toparlamış olmasına rağmen geçen süre içerisinde tarihinin en büyük geçici puan düşüşünü yaşamıştır (Aksu, 2013, s. 91).

Dünya Ekonomik Forumu'nun yayınlandığı “Mesleklerin Geleceği” başlıklı rapora göre; 2020 yılına kadar 7,1 milyon çalışan işsiz kalacak, bununla beraber yeni mesleklerin yaratacağı taleple de teknoloji, medya, hizmet gibi sektörlerde 2 milyon kişi iş sahibi olacak (Gürel, 2017, s. 54). Bu verilere bakacak olursak, robotik, yapay zekâ ve otonom sistemlerin günlük ve endüstriyel yaşama daha fazla girmesi belirli bir düzeyde de olsa işsizliğe yol açacak gibi gözükmektedir. Diğer taraftan yeni teknolojiler yeni meslekleri doğurmakta ve süreç bu şekilde devam etmektedir.

DÖRDÜNCÜ BÖLÜM

4. SOSYAL MÜHENDİSLİK, BİLGİ GÜVENLİĞİ VE ENDÜSTRİ 4.0 KAVRAMLARINA İLİŞKİSEL VE BÜTÜNCÜ BİR YAKLAŞIM

Bu çalışmada yer alan Sosyal Mühendislik (SM), Bilgi Güvenliği (BG) ve Endüstri 4.0 (E 4.0) kavramlarının birlikte ele alınarak bütüncü (holistik) bir yaklaşım içerisinde açıklanmaya çalışılmasının önemli olduğu düşünülmektedir. İç içe geçmiş olduğu görülen bu kavramların tekil olarak ele alınarak incelenmesinin konunun gerçek önemi ve bütünlüğünü yitirmesine sebebiyet vereceği kaygısı ile hareket edilmiş, sorunların ve alınabilecek önlemlerin daha açık bir şekilde ifade edilebilmesi için bütüncü bir yaklaşım tercih edilmiştir.

Bütüncü yaklaşım, birbiri ile ilintili alanların bir arada değerlendirildiğinde olgunun kavranabileceğini kabul eden yaklaşım biçimidir ve aynı zamanda sistem kuramı ile de tamamlanmaktadır. Bütüncü yaklaşımda öne çıkan bir başka özellik ise disiplinlerarası düşünme ve yatay bağlantılar kurabilmeye fırsat tanımasıdır. Antropoloji, ekoloji, ekonomi, felsefe, sosyoloji, psikoloji, nöroloji gibi disiplinlerde kullanılmaktadır (www.turkcebilgi.com). Karmaşık sistemleri değerlendirirken daha geniş bir açıyla ve disiplinlerarası bir anlayışla bakılmasını öngören bilim paradigması ya da bilim felsefesi bakış açısı (www.egitimler.info) olarak da tanımlanan bütüncü yaklaşım aynı zamanda Gestaltçı yaklaşım ile de örtüşmektedir. Gestaltçı yaklaşımın temel ilkesi ise genel olarak şu şekilde ifade edilmektedir: Bütün, kendisini oluşturan parçaların toplamından farklı ve büyüktür ve hiçbir parça bütünün sahip olduğu (tüm) özelliklere aynı anda sahip değildir (www.wikisitesi, 2016). 1930-2002 yılları arasında yaşamış Fransız sosyolog Pierre Bourdieu, kuramın yanında metodolojinin önemi üzerinde durarak, kuramın/teorinin pratiği açıklama konusundaki eksiklerini vurgulamaktadır. Özellikle kuram ve metodolojinin bir birinden bağımsız değil iç içe geçmiş bir süreç olduğu vurgusunda bulunmaktadır. Bu yönüyle Bourdieu, olgulara bütüncü bir perspektifle bakmanın önemi üzerinde durmaktadır (Zencirkıran, 2018, s. 48). Albert (2018, s. 32)'in, sistem yaklaşımı ve kaos teorisine eş zamanlı bir gönderme olarak kabul edebileceğimiz şu sözleri de çalışmamızı destekleyici niteliktedir; parçalar bütünü, karmaşık gibi görünen bütün ise çalışan bir sistemi ifade etmektedir; “Hükümet,

ekonomi, akrabalık ve kültür hep birlikte karmaşık bir toplumun özellikleridir. Bir anlamda her biri bir insanın biyolojik organları gibidir. Hiçbir kalp, akciğer, böbrek, kol veya göz bir kişinin geri kalan organlarıyla karmaşık beraberliği olmaksızın işlevsel olarak varlık gösteremez, ancak bu organların her biri kendi içinde bir sistem olarak görülebilir.” ve genel anlamda bütünlük ile güvenlik ancak bu şekilde sağlanabilir.

Birçok güvenlik önlemi kademeli bir şekilde uygulanacak olsa bile, yalnızca SM saldırıları hakkında bilgi sahibi olmak ve onları önlemeye çalışmak, ya da aynı şekilde yalnızca teknolojik güvenlik önlemleri alınarak istenilen güvenlik seviyesine ulaşmak ne de bunların etkilerine E 4.0 tabanlı sistemlerin maruz kalmasını ortadan kaldırmak tek başına yeterli olmaktadır. Tüm alt parçaların bir bütünlük içerisinde sistemin bütününe koruyacak şekilde ilişkilendirilmesi, kontrol edilmesi, sürekli güncellenmesi ve takip edilmesi gerekmektedir. Ayrıca, ne SM’nin ne BG’nin ne de E 4.0’ın yapısının münferit olarak korunmaları mümkün gözükmemektedir. Bütünlüğün korunması açısından yukarıda açıklanan gerekçelere ek olarak ayrıca; finansal, teknolojik ve küresel siber saldırılar gibi kavramların da göz önünde bulundurulması gerekmektedir. Ancak bu sayede işletmeler ve kurumlar için “bilgi varlıklarının” korunması mümkün olabilecektir.

Bilgi varlıklarının korunmasını istemek ve yönetmek, örgütsel bağlamda büyük önem taşıyan bir amaç haline gelmiştir. Bilgi Güvenliği Yönetim Sistemi, bilgi varlıklarını korumak için uygun güvenlik araçlarının kullanılmasını sağlama konusunda eşsiz bir role sahiptir. Güvenlik her zaman *teknoloji*, *organizasyon* ve *insan* üç boyutunda görülmüştür (Alavi, Islam, Mouratidis ve Lee, 2015, s. 161). Burada bahsi geçen insanı SM, teknolojiyi BG, organizasyonu ise E 4.0 platformu olarak ele almak ve ilişkilendirmek oldukça mümkündür.

BG, çoğu şirket içinde en önemli ve en popüler bölümlerden biridir. Bir barikat, uygunluk teyitçisi, günah keçisi ve trafik polisi olarak görülür. BG ekibi bir projeye en son katılan ve kuruluşun BT altyapısında bir şeyler ters gittiğinde ise suçlanan ilk gruptur. Bir endüstri olarak bu noktaya nasıl geldik? Daha da önemlisi, bunu nasıl düzeltebiliriz? SM bu sorunları çözme ve BG ile kurumun geri kalanı arasındaki ilişkiyi geliştirme yönünde uzunca bir yol kat edebilir (Philput, 2019).

Dijital mühendislik ve iletişimin artmasıyla birlikte, SM saldırılarının

kuruluşlara karşı geliştirdiği genel riskler artmakta, saldırgan için ise riskler azalmaktadır. Artan riskle mücadele etmek için kuruluşlar, insan kaynakları (İK) (profesyonel) çalışanlarının, bu riski önlemede bilgi teknolojisi (BT) uzmanları kadar sorumluluk ve kabiliyete sahip olduğunu kabul etmelidir (Seidenberger, 2016). Bilgi teknolojisinin SM saldırılarının tehdidi veya sıklığını artırmasının en az iki yolu bulunmaktadır. Bunlardan birincisi, saldırganlar artık kurban arayışları için (nokta) hedef avcılığı gibi birçok saldırı vektörünü otomatikleştirerek daha geniş bir ağ oluşturabilmekteler. Tek bir hedefe veya organizasyona odaklanmak zorunda kalmak yerine, artık saldırganlar tek bir program kullanarak binlerce mağdur olmasa da yüzlerce kişiyi sömürmeye çalışabilmekteler. İkincisi, sosyal ilişkiler ve sosyal ağlar internet üzerinden giderek daha fazla aracılık edebilmektedir. Bu nedenle, artık insanlar hiç tanışmadığı, tanışmak ya da yüz yüze görüşmek zorunda kalmadığı insanlarla iletişim kurmada eskisine oranla çok daha fazla imkâna sahipler. Bu, Facebook ve LinkedIn gibi sitelerin hem bilgi toplama aracı olarak hizmet edebileceği hem de bir derece anonimlikle insanlarla iletişim kurmak için saldırı vektörlerine dönüşerek çevrimiçi aldatma yolunda yeni olanaklar yaratabileceği anlamına gelmektedir. Bu şekilde internette daha fazla anonimlik oluşturma yeteneği, tespit edilmekten (yakalanmaktan) kaçınmayı ve tespit edilse bile sonuçlarını hafifletmeyi kolaylaştırdığından saldırganlar için genel risk de azalmaktadır (Seidenberger, 2016).

2018 RSA Konferansında yapılan bir röportajda, San Francisco merkezli Social Proof Security CEO'su ve kar amacı gütmeyen Kadın Güvenliği ve Gizliliği Yönetim Kurulu Başkanı Rachel Tobac, ZeroFOX'un baş veri bilimcisi olan Philip Tully'nin makine öğrenmesi yapay zekâ yazılımı ile geliştirmiş olduğu küçük bir uygulama ile kullanıcıların Twitter verilerinden hareketle kişiselleştirilmiş bir bağlantı linki oluşturarak ve hedef gözeterek yapmış olduğu SM ataklarında (spear phishing) %35 başarı sağladığını (linklerin tıklanıldığını) ve bu konu hakkında ne düşündüğü sorulduğunda şu cevabı vermektedir (Heller, 2018); RSAC'de farklı röportajlar veriyorum ve SM nereye gidiyor? SM'nin geleceği nedir? gibi sorulara cevap arıyorum ve şunu diyorum; yapay zekâ kullanılarak yapılan SM'lere dikkat edin. Çünkü şu basit örneği düşünün, OSINT (açık kaynaklı bilgi toplama yazılımı) kullanarak bilgi toparlamaya çalışmam bana 100 saate mal olurken, yapay zekâ

kullanarak bir bilgisayarı eğitmem yalnızca 30 saniye. Kesinlikle inanıyorum ki, artık yapay zekâ kullanılan SM çağına giriyoruz. Yapay zekâ, hedef hakkında her türlü bilgiyi toparlayıp, filtreleyip, en iyi kişiselleştirilmiş bahaneyi üreterek saldıracaktır, bunu göreceksiniz. Tobac, kendisine yöneltilen diğer önemli bir soruya: “SM saldırıları artık çok daha fazla hedefe yönelik düzenlenmiş ve teorik olarak da bunda inandırıcı ise, insanları bu durumdan kaçınmaları için nasıl eğitirsiniz?” şu cevabı veriyor; bunun için yapabileceğiniz birkaç şey var. Makine öğrenmesi sizin hakkınızda bulabileceği tüm bilgilere ulaşmaya devam ediyor, bu nedenle çevrimiçi aracılığıyla gönderdiğiniz şeyleri düşünün. Örneğin, iş bilgisayarınız başında çekilmiş çeşitli resimlerinizi yolladığınızı düşünün, benim o resme ulaştığımda sizin hangi yazılımları (programları, uygulamaları) kullandığınızı görebildiğim gibi yapay zekâ da bunu çok rahatlıkla yapabilecektir, bu değişmez. İş bilgisayarınız karşısında resim çekmeyin. Daha az bilgi sızması için yapabileceğiniz şeyler var. Kendi çıkarlarınızı korumak için bir miktar paranoyak olun ve size gönderilen “şuraya tıkla”, “buraya tıkla”, “bu ilginizi çekebilir” gibi linklere kolayca inanmayın. Çift faktörlü doğrulamalardan da yardım alabilirsiniz, birisi yazışmada size bir arkadaşınızmış gibi davranıp (bu yapay zekâ da olabilir) “Telefon numaranı kaybettim bana yazar mısın?” vb. bir talepte bulunduğunda hemen uyanık olmalısınız, eğer tanıdığınız birisi ise zaten telefon vb. numaranızı biliyor olmalıydı değil mi? Yapay zekâ, ancak sizin sızdırdıklarınızdan hareketle bir şeyler bulabilir...

Bütünlük ve güvenlik açısından önemsenmesi gereken bir diğer konu biyoteknoloji ve yapay zekâ yönlendirmesidir. Biyoteknoloji ve bilgi teknolojilerinin kaynaşması kısa süre sonra milyonlarca insanı iş dünyasının dışına itebilir. Büyük Veri algoritmaları yüzünden iktidar tümüyle bir avuç seçkinin eline geçerek çoğunluğun sadece istismar edilebilir değil (çok daha kötüsü) ayrıca gereksiz konumuna düşmesine sebep olacak dijital diktatörlükler ortaya çıkarabilir (Harari, 2018, s. 15). İnsanlar Google’dan rotalarını çizmesini istiyor. Bir yol ayrımına geldiklerinde iç sesleri onlara “sola dön” dese de Google Maps onlara “sağa dön”melerini söylüyor. Kendi hislerine güvenip sola dönüp trafiğe yakalanıyor ve önemli bir toplantıyı geçiriyorlar. Daha sonraki seferde, bu kez Google’ı dinleyip zamanında varıyorlar. Bu şekilde çeşitli tecrübeler edinerek artık Google’a

güvenmeyi, birkaç sene içinde de her durumda (körü körüne) Google’a uymayı kabul ediyor, telefon çalışmadığında ise öylece ortada kala kalıyorlar (Harari, 2018, s. 65).

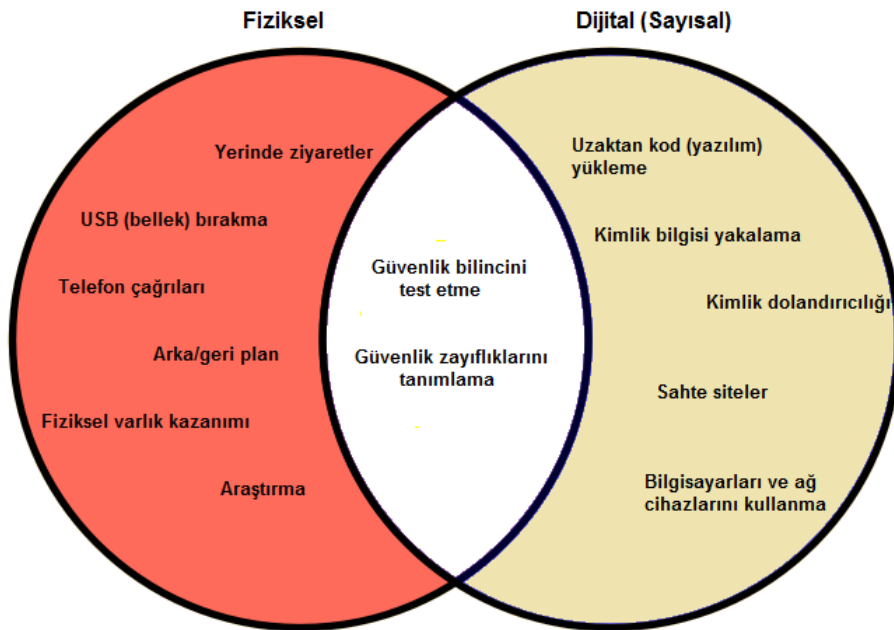
Dijital çağın petrolü bilgidir ve E 4.0’ın temelinde bilgi yönetimi bulunmaktadır. Teknoloji tabanlı süreç, sistem ve akıllı ürün tasarımları, yeni dönemin uzmanlık gerektiren konularının başında yer almaktadır. İletişim protokolleri, sensör teknolojileri, E 4.0 teknolojileri, uygulamalı matematik, istatistik, olasılık gibi konulara hâkim olmadan, süreç ve ürün tasarımı yeni dönemde pek mümkün gözükmemektedir. Bu nedenlerle, hangi teknolojinin, nasıl ve nerede kullanılacağını iyi bilen insan kaynaklarına ihtiyaç vardır. (...) Yeni dönemde süreçleri çevrimiçi izleme (surveillance) algoritma ve korelasyon analizleriyle, yapılandırılmamış verilerden anlamlı bilgi üretme konusu da oldukça önemli hale gelecektir. Ağa bağlı binlerce nesneden toplanan verilerin gerçek zamanlı izlenmesi ve yorumlanması (enformasyon’un bilgiye dönüşümü) için veri analistlerine ihtiyaç olacaktır (Apilioğulları, 2018, s. 67-70).

Nesnelerin İnterneti (IoT), bir birlerine bağlı (ve ağ’a da çıkış yapabilen) “akıllı” makinelerin, yalnızca kahve makinesi, buzdolabı, televizyon vb. değil, bunun yanı sıra, su depoları, elektrik santralleri, barajlar, otonom araçlar ve akıllı binalar, hastaneler ve ameliyathaneler gibi birçok alanı da kapsayacağından, bu platform (Nesnelerin İnterneti) üzerinden gerçekleştirilecek SM, siber güvenlik, BG, fideye yazılımı saldırıları vb. ataklar şimdiki tahminler ve öngörülerin ötesinde zarar verebilecek bir potansiyel taşımaktadır. Bu zararlar kişilerin ya da daha kalabalık grupların mağdur olması, günlük yaşam akışının durması, sel baskınları, ülke çapında elektrik kesintileri ve belki de savaşların başlatılması için kullanılabilecektir.

Yeni yüzyıl(lar) adaletin, iyi ve kötünün, haklı ve haksızın, doğru ile yanlışın yeniden tanımlanacağı ya da bu tür kavramların artık var olmayacağı, daha doğrusu, yapay zekâ beslemeli süper bir algoritmaya mı dönüşeceği sorusunu akıllara getiriyor. “İnsanlık, etik ve algoritma üçgeni” üzerinde çalışılması gereken yeni bir araştırma sorusu olabilir mi? Daha da önemlisi bu araştırmayı insanlar mı, yapay zekâ mı ya da ikisinin iş birliği mi gerçekleştirecek? Cevap “evet” ise bu nasıl gerçekleştirilmeli? vb. sorular bir an önce cevaplandırılması gereken sorular olarak karşımızda durmaya devam etmektedir.

SM, BG ve E 4.0 için en temel girişim ve koruyucu ortak önlemlerden bir diğeri de penetrasyon uygulamalarıdır. Bir penetrasyon (sızma) testi girişiminin veya güvenlik bilinci programının bir parçası olarak, kuruluşun fiziksel ve BT güvenlik altyapısını denetlemek için SM testleri yapmak gerekebilir. Herhangi bir SM testini gerçekleştirmeden önce, kuruluşun hedeflerini açıkça tanımlamak ve ulaşmak istedikleri hedefleri açıkça ortaya koymak için kuruluşla karşılıklı konuşmak gerekmektedir. Çoğu kuruluş, güvenlik eğitim programlarının etkinliğini ölçmek veya mevcut güvenlik politikalarındaki ve Bilgi Teknolojileri (BT) savunma mekanizmalarındaki zayıflıkları belirlemek istemektedir. Değerlendirmenin amacı net bir şekilde anlaşıldığında, ilgili tüm alanları ele alan bir saldırı planı oluşturulabilir. Genel olarak, iki farklı SM penetrasyon (sızma) testi türü bulunmaktadır: Dijital (sayısal) ve fiziksel testler. Dijital bir SM testi BT güvenliği ve politikaya uyumluluk üzerine yoğunlaşırken, fiziksel bir SM testi ofis alanları ve şirket ekipmanları gibi insan davranışları ve maddi varlıklar ile daha fazla ilgilenmektedir (Metasploit, 2019). SM ve bilgi teknolojileri güvenliğine dayalı olan her iki testin de ortak amacı güvenlik bilincini test etmek ve güvenlik zayıflıklarını ortaya çıkarmaktır. Şekil 47’de SM ve BT güvenlik testleri ve ortak alanları yer almaktadır.

Şekil 47. Sosyal Mühendislik ve Bilgi Teknolojileri Güvenlik Testleri



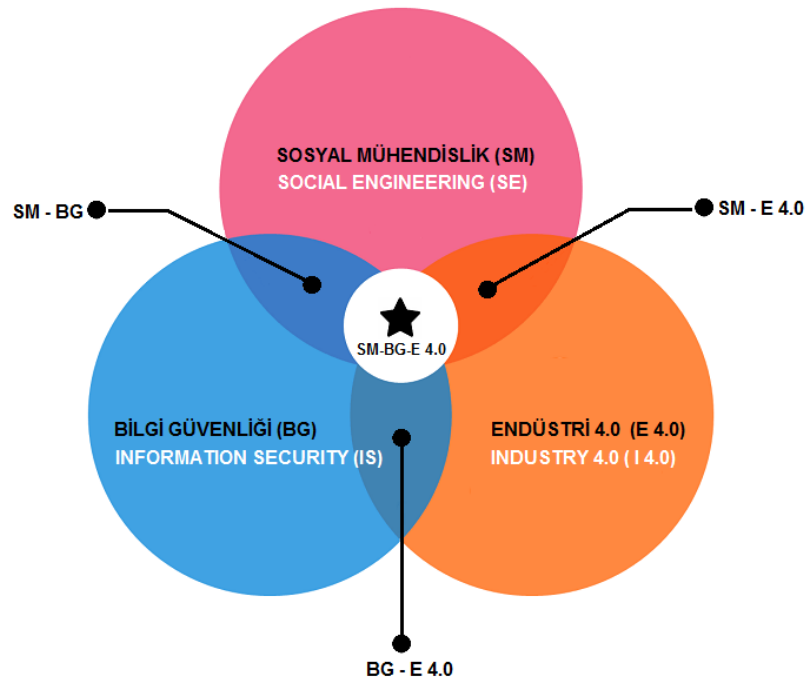
Kaynak: Metasploit, 2019

SM saldırıları, bilgi sistemlerinin güvenliği için önemli bir tehdit oluşturmaktadır. Güvenlik uzmanları bugüne kadar sadece SM saldırılarının potansiyel etkilerini yönetiyorlardı. Güvenlik uzmanları bu tür saldırıları genel bilgi sistemine dış tehdit olarak görmekte ve şu ana kadar önleyici tedbirler, insanlara uyarlanmış siber farkındalık kampanyaları yoluyla mağdur olmalarına karşı hazır olmalarını ve kendilerini korumalarını isteme konusuna odaklanmaktaydı. SM saldırı çerçevesi proaktif olmanın yolunu sunarken, sistem mühendisliği ise karmaşıklıkla baş etmekle ilgilenmektedir (Merwe ve Mouton, 2017). Bu bize göstermektedir ki SM ve BG her zaman iç içe geçmiş durumdadır ve birlikte ele alınmalıdır.

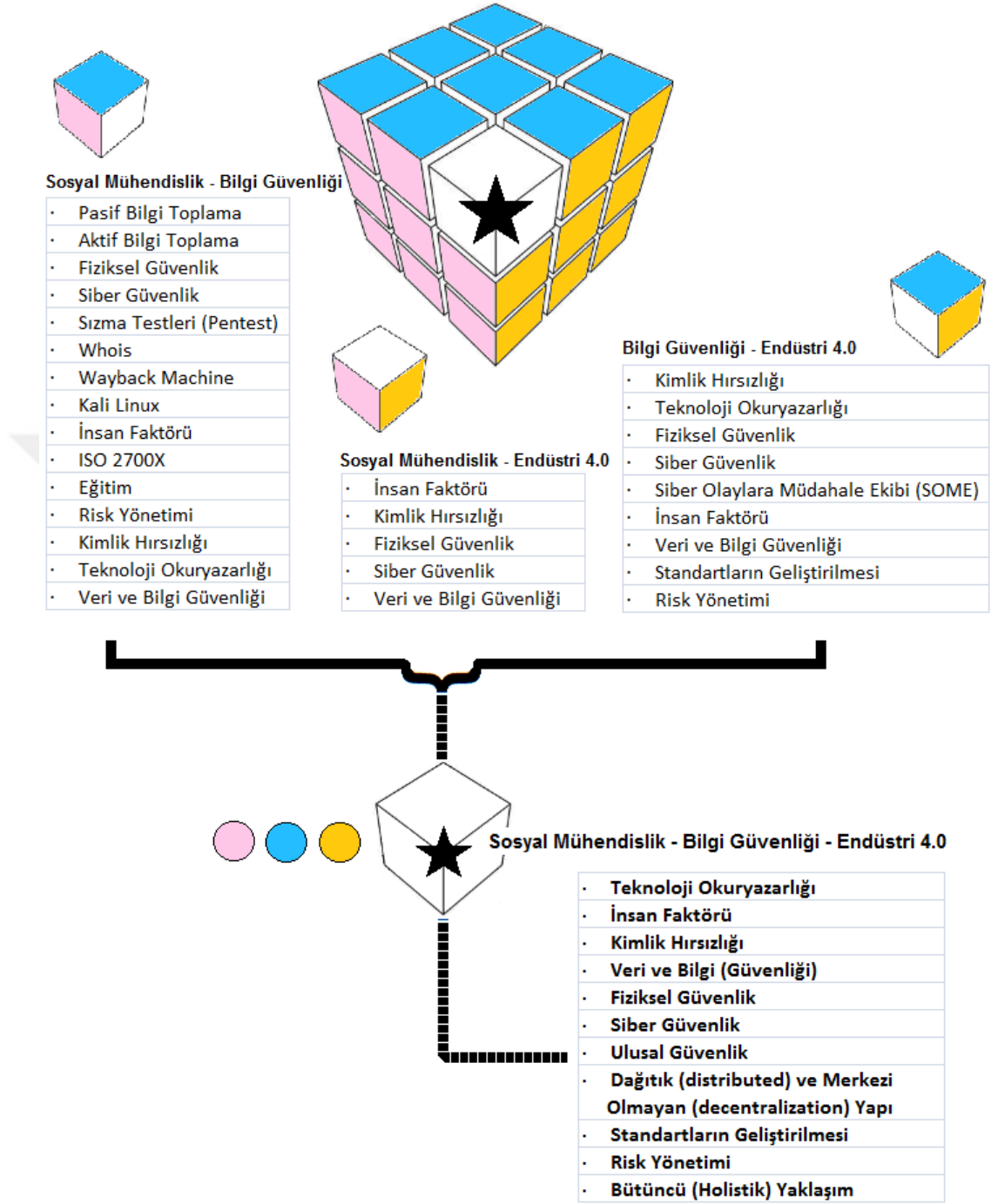
Literatür incelemesinde BG konusunda yapılan çalışmaların BG ile Bilgi Güvenliği Yönetim Sistemlerine yönelik olduğu ve bu bağlamda “en zayıf halka” olan insan unsurunu BG konusunda bilinçlendirme üzerinde durulduğu tespit edilmiştir (Keser ve Güldüren, 2015). En zayıf halka olarak insan, bu çalışmada üç temel kavram olarak ele aldığımız SM, BG ve E 4.0’da da karşımıza çıkmaktadır.

SM, BG ve E 4.0’ın kesişme alanları, önce ikili gruplamalar, daha sonrasında her üçünün ortak alanları şeklinde tespit edilmeye çalışılmış olup, görsel olarak da Şekil 48 ve Şekil 49’da verilmiştir. Bu kesişim noktalarının ele alınması ve açıklanmasında daha çok bütüncü yaklaşım ve sistem yaklaşımı dikkate alınmıştır.

Şekil 48. Sosyal Mühendislik, Bilgi Güvenliği ve Endüstri 4.0’ın Kesişme Alanları



Şekil 49. Sosyal Mühendislik, Bilgi Güvenliği ve Endüstri 4.0'ın Kesişme Alanlarına Ait Bileşenler



Şekil 49 araştırmacı tarafından literatür araştırması sonucunda oluşturulmuş olup, öneriler ile yeniden düzenlemeye açıktır.

Şekil 49'da gösterilen kesişme alanlarında yer alan kavramlar aşağıda kısaca açıklanmıştır:

Pasif Bilgi Toplama: Hedef ile doğrudan temasa/iletişime geçmeden bilgi toplama.

Aktif Bilgi Toplama: Hedef ile doğrudan temasa/iletişime geçerek bilgi toplama.

Fiziksel Güvenlik: Kritik alanların, odaların, ekipmanların, giriş ve çıkışların çeşitli teknik ve fiziksel yöntem ve araçlarla güvenlik altına alınması.

Siber Güvenlik: Teknoloji ve bilişim cihazlarının donanımsal, yazılımsal ve veri güvenliğinin sağlanması.

Sızma Testleri (Pentest): Her türlü güvenlik açıklarını tespit etmek ve önlem alabilmek için yapılan testler/girişimlerdir. Test sonucunda sistemle ilgili çeşitli bilgiler edinilir ve sınıflara ayrılarak (önerilerle) kullanıma hazır hale getirilir.

Whois: Bir alan adı ya da IP adresinden yola çıkılarak sahibine ait çeşitli bilgiler (yer, şehir, ülke, adres, e-posta, telefon numarası vb.) elde edilir.

Wayback Machine: www.archive.org adresi üzerinden 1996 yılından bu yana internet (web siteleri) kayıtlarını barındıran platform.

Kali Linux: Bu yazılım üzerinden hem BG atakları hem de SM araçları ile SM atakları gerçekleştirilmektedir.

İnsan Faktörü: İş süreçleri ve teknolojik işleyişler açısından en zayıf halkanın insan unsuru olduğu ortak görüştür.

ISO 2700X: Bilgi Güvenliği Standartları.

Eğitim: Farkındalık yaratmak açısından eğitimin önemi üzerinde önemle durulmaktadır.

Risk Yönetimi: Doğabilecek riskler için risk yönetiminin uygulanması ve çeşitli teknikler yardımıyla hazırlanacak olan öngörüler ile doğacak zararı en aza indirmek için proaktif ve reaktif tutumların önceden belirlenmesi.

Kimlik Hırsızlığı: Kişi ya da kuruma ait bilgilerin çalınması. Özellikle çok katmanlı güvenlik önlemleri (Ör: 2FA) almak önemli.

Teknoloji Okuryazarlığı: Teknolojiyi kullanabilme, yönetebilme, değerlendirebilme ve anlamayabilme yeteneği.

Siber Olaylara Müdahale Ekibi (SOME): Siber olaylara mümkün olduğunca anlık ve erken müdahale edebilmek için kurulmuş olan teknoloji bilgisi üst düzeyde olan ve donanımlı ekipler.

Standartların Geliştirilmesi: İlgili alanda/sektörde ortak dilin geliştirilmesi, ulusal ve uluslararası normların oluşturulması, kavram ve anlam bütünlüğünün

sağlanabilmesi, teknolojik iletişimin aynı teknik standartlar kullanılarak yapılabilmesi vb. çalışmaları içeren yapı.

Dağıtık (Distributed) ve Merkezi Olmayan (Decentralization) Yapı: Dağıtık Yapı; işlemlerin tek bir merkezden ziyade birden çok noktada gerçekleştirilmesidir. Merkezi Olmayan Yapı ise; kayıtların işlenmesinde tek bir yapının/kurumun kontrolünün olmamasıdır.

Veri ve Bilgi Güvenliği: Her türlü veri ve bilgi güvenliğinin sağlanması, korunması, izinler ölçüsünde iletilmesi, belirli bir zaman sonra (gerekliyse) imhası ve imhasının uygun şartlarda gerçekleştirilmesi.

Ulusal Güvenlik: İster kişisel ister kurumsal düzeyde olsun, her türlü güvenlik ihlali sonuç olarak ulusal güvenliğe bir tehdit unsurudur. Alt birimlerde gerçekleşen tehditler üst yapıyı tehdit edebilmektedir. Ülkenin kurum ve vatandaşlarını, yaşamın akışını sekteye uğratabilecek şekilde tehdit eden her türlü güvenlik unsuru ulusal güvenlikle ilintilidir.

Bütüncü (Holistik) Yaklaşım: Bu çalışma açısından bütüncü yaklaşım, çalışmada yer alan üç ana kavramın (SM, BG ve E 4.0) birlikte ele alınarak değerlendirilmesini ifade etmektedir. Disiplinler/alanlar arası bir yaklaşım olarak bütüncü yaklaşım parçaların ayrı ayrı ele alınmasının yanı sıra bütünün önemine vurgu yapar.

İşletmeler açısından bakıldığında bilgi en temel “varlık” haline dönüşmüş durumdadır. Öyle ki, bazı çok tanınmış markalar için marka değeri (elinde tutmuş olduğu veri ve bilgi varlığı sayesinde) işletmenin maddi mal varlıklarından (kaynaklarından) onlarca kat daha değerli kabul edilebilmektedir. Bu varlığı başka bir şekilde ifade edebilmek için “piyasa değeri” vurgusu kullanılmaktadır. Örneğin; beş milyar dolar mal varlığı bulunan bir işletmenin piyasa değeri elli milyar dolar olabilmektedir. Şirketin piyasa değeri, bilançosunda maddi varlık olarak yer almasa da, bu değer; şirket birleşmelerinde, şirketin el değiştirmesinde, şirket satın almalarda, borsada, hisse senetlerinde belirgin bir şekilde (maddi ve manevi) değer olarak ifade edilebilmektedir. Örneğin; UBER’in tek bir adet taksisi olmadan 2018 itibariyle piyasa değerinin 120 milyar dolar (www.HaberTurk.com, 19 Ekim 2018), AirBNB’nin tek bir otel odası olmadan piyasa değerinin 31 milyar dolar (Özoğul, 2017) olması gibi. Artık işletmelerin marka değeri ve tanınırlık parametreleri önemli,

maddi duran varlıkları değil. Veri ve bilginin, araştırmamızda yer verilen her üç ana kavram olan SM, BG ve E 4.0 için ortak değer olduğu görülmektedir. İşletmelerin fiziksel, maddi ve manevi varlıklarının sürdürülebilmesinde veri, bilgi ve BG'nin çok kıymetli temel değerler olduğunu bu araştırma ortaya koymaktadır. Bu varlığın korunmasında teknoloji okuryazarlığı en başta edinilmesi gereken bir diğer öge olarak karşımıza çıkmaktadır, tıpkı insan kaynaklarının önemi gibi. Keza çalışanlar yani insanlar en zayıf halkayı temsil etmektedir. Kişisel ve/ya şirket bilgilerinin dışarıya izinsiz/illegal bir şekilde çıkartılmasında ya da çalınmasında, kimlik hırsızlığında en büyük rolü oynayan bu halkadır. İşletmeler için fiziksel ve siber güvenlik, devletler için ulusal güvenliğin ayrılmaz bir parçasını oluşturmaktadır. İşletmelerin her türlü varlığının korunabilmesi için bu doğrultuda çeşitli standartların geliştirilerek, risk yönetimine doğrudan hazır olması gerekmektedir. Bu hazırlığın şirketin maddi ve maddi olmayan tüm varlıkları gözetilerek dağıtık ve merkezi olmayan bir yapıyla hayata geçirilmesi, kayıpların en aza indirgenmesi açısından kaçınılmazdır. İşletmeler, ancak böyle bütüncü bir yaklaşımla kârlılık, verimlilik ve sürdürülebilirliğini devam ettirerek E 4.0 olarak adlandırılan yeni çağa ayak uydurabileceklerdir. İşletme yönetimlerinin ancak proaktif önlemler ve ilişkilendirme sanatı sayesinde büyük resmi görmeye yaklaşabileceklerini, bu tutumlarını güçlendirmek için ise Şekil 49'da yıldız (★) ile ifade edilen alanda yer alan ve yukarıda kısmen açıklaması yapılan kavramları dikkatle ele alması gerekmektedir. Bu yaklaşımın, işletmelerin yakın gelecekteki dünyaya hazır olmaları yönünde önemli katkılar sunacağı düşünülmektedir.

Buraya kadar yer alan veri ve değerlendirmeler ışığında, kurumsal başarının: Dinamik, güvenli ve verimli işletmelerin varlığının özellikle İK aracılığıyla, çalışanların SM konusunda eğitilerek duyarlı ve dikkatli hale getirilmesi; BT departmanları tarafından sağlanabilecek destek, güncelleme ve önlemler sayesinde BG yapılanmasının tam ve eksiksiz uygulanması; verimlilik, küresel rekabet ve müşteri memnuniyetinin ise E 4.0 ve bileşenlerinin (Nesnelerin İnterneti, yapay zeka, robotik, siber fiziksel sistemler vd.) adaptasyonu sayesinde yakalanabileceği, bunun da ancak SM, BG ve E.40'ın birlikte ele alınarak eş güdüm ve sinerji yaratılmasından mütevellit olduğu düşünülmektedir.

Nöron Model (Analoji)

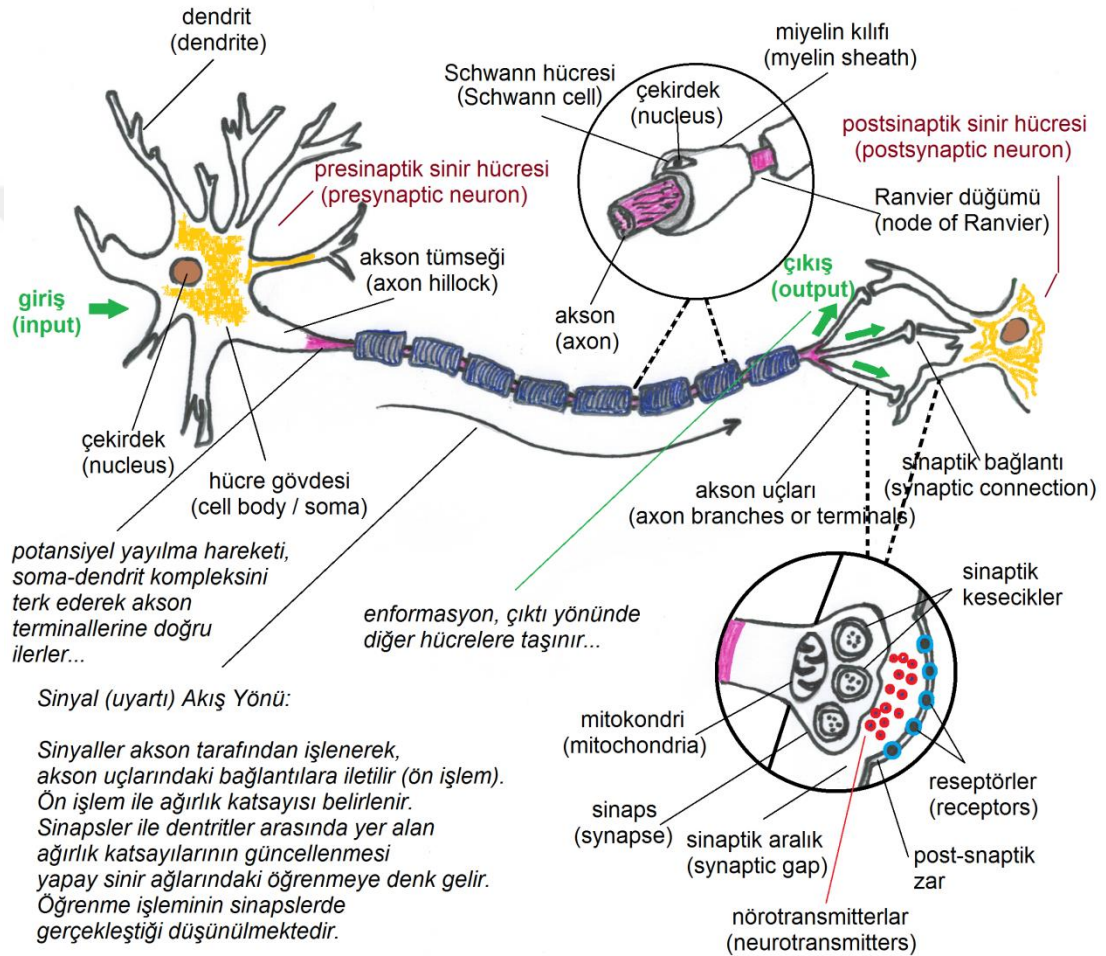
Bu çalışmada SM, BG ve E 4.0 arasındaki bağ, insan biyolojisi sinir sistemindeki nöron yapısı, nöronlar arası iletişim ve nöronların çalışma düzeni benzetişimi (analoji) üzerinden açıklanmaya çalışılmıştır. Sinir hücrelerini genel işlevi açısından tarif etmek gerekirse; iç ve dış uyartıları olarak değerlendirir ve ilgili yerlere (kas, bez ve beyin) komut olarak iletir. Sinir hücresine *nöron* denmektedir. Nöron çekirdeğinin etrafına *soma* adı verilir ve bu somalara kısa uzantılar olarak ağaç dalları şeklinde *dentrit*'ler bağlanır (Şekil 50). Dentritler gelen bilgileri alarak hücre gövdesine iletir. Bir nöron diğer bir nörona *akson* denen uzantıyla bağlanır. Bazı aksonların üzerinde *miyelin* kılıfları bulunur, bu kılıflar ileti hızının artmasında rol oynarlar. Miyelinler arasında *Ranvier Boğumları* bulunur. Miyelin ile çevrili aksonlarda ileti, boğumdan boğuma yapılan atlamalarla (*impuls*) gerçekleştiğinden daha hızlı ve daha az enerji kullanılarak yapılmaktadır. Aksonların dentritlerle birleştiği yerlere *sinaps* adı verilmektedir. Uyarıların ön değerlendirme ve kontrol yerleri bu sinapslardır. Bir nöronun aksonu başka bir nöronun dentriti ile sinaps yaparak birleşir. Nöronlarda uyarı dentritlerden aksona doğru iken, sinapslarda uyarı yönü aksondan dentritlere doğrudur. Sinapslarda bulunan sinaptik kesecikler nörotransmitter maddeleri (Asetilkolin, Dopamin, Serotonin, GABA, DOPA, Taurin, Histamin, Noradrenalin) dentritlerdeki reseptörlere ulaştırır. Bu sayede impuls diğer nörona geçmiş olur. Her impuls komşu nörona iletilmez, burada seçici direnç (sigorta, firewall vb.) ile karşılaşır (Ayancikanadolu, 2018). Sinir sistemi üzerinde meydana gelen rahatsızlıklar karar almayı zorlaştıracak gibi gecikmelere, yanlış uyarı ve komutlara, bazı organ ve kasları kullanamamaya, istem dışı kasılmalara ve benzeri birçok kusura sebebiyet verebilmektedir. Multipl Skleroz (MS), alzheimer, parkinson, epilepsi, siyatik ve menenjit bunlardan en çok bilinenlere örnek olarak verilebilir. Örneğin MS, akson etrafındaki miyelin kılıflarının zarar görmeleriyle ilişkili bir hastalık olup beyin ve omuriliğin birçok alanını etkileyebilmektedir (Şekil 51). Araştırmacılar, sanılanın aksine, dendritlerin, elektrik sinyallerinin (atımların/pulse) esas üretildiği yer olarak bilinen ve soma adı verilen beyin hücrelerinden 10 kat daha fazla elektrik sinyali yarattığını keşfettiler (PeerScientist, 2017). Los Angeles Kaliforniya Üniversitesi (UCLA) ekibinden Mayank Mehta, bu durumun insan beynini taklit eden bilgisayarların gelişimini anlamada yeni bir yol

açabileceğini söylemektedir. Beynimiz nöron adı verilen yaklaşık 100 milyar sinir hücresinden oluşmaktadır. Nöronlar elektrokimyasal sinyalleri toplama ve iletme kabiliyetine sahiptirler. Bunu bir bilgisayarın giriş-çıkış (kapı) ve kablolarına benzetmek mümkündür (HowStuffWorks.com). İnsan beyinde yaklaşık 100 milyar nöron olduğu düşünülmektedir (yapılan son çalışmalarda bu rakamın 85 milyar civarında olabileceği öne sürülmekte). Sinir hücrelerinin diğer sinir hücreleriyle olan bağlantılarının ise 60 trilyonu bulduğu belirtilmektedir. Nesnelerin İnterneti (Internet of Things - IoT) dünyasında henüz çok yakın bir gelecek olan 2020-2025 arasında 50 milyar aygıtın (bilgisayar, tablet, modem, televizyon, bulaşık makinesi, akıllı saat, cep telefonu vb. -bunların her birini nöron olarak düşünebiliriz-) birbirine bağlanacağı (birbirleriyle iletişime geçeceği) tahmin edilmektedir. Bir aygıtın birden çok (belki onlarca hatta zaman içerisinde yüzlerce) aygıta bağlanacağı düşünüldüğünde ve bu durum nöron bağlantılarına benzetildiğinde, ilk etapta kabaca 100 trilyonluk bir bağlantı ile karşı karşıya kalacağımız anlamına gelmektedir. Bu henüz önümüzdeki 4-5 yıl için geçerlidir. Yirmi otuz yıl sonrasını düşünecek olursak bu bağlantı sayısı hayal edebileceğimizin de ötesine geçecektir. E 4.0'ın bileşenlerinden olan Nesnelerin İnterneti'nin, dolayısıyla gelecekteki E 4.0'ın ne kadar hassas bir yapıda ve oldukça kompleks olacağı ortadadır, tıpkı nöronların yapısında olduğu gibi.

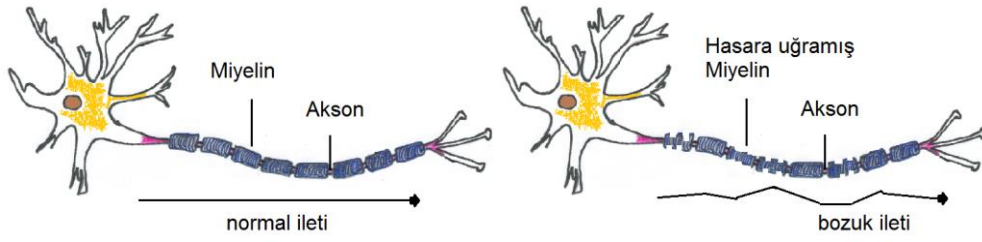
Küçük bir SM (müdahalesi) ile BG tehlikeye girerek, bağlı tüm birimler bu durumdan olumsuz etkilenebilecektir, tıpkı post modern yönetim kuramlarından biri olan *düzensizlik içerisinde düzeni* tarif eden, evrenin doğrusal olmayan (non-lineer) yönlerini açıklamaya çalışan *kaos teorisi* ve onun içerisinde yer alan Edward Lorenz'in *kelebek etkisi* teorisi'nde olduğu gibi. Yine aynı şekilde, Mayo, Barnard ve Bartalanffy'nin (1937), Norbert Wiener'in (1948) olay ve birimlerin birbirleri ile olan ilişkisini dış çevre şartları ile ilişkili olarak incelediği, sistemin birbirlerine bağlı alt sistemlerden oluştuğunu ve aralarında sıkı bir ilişkinin bulunduğunu, entropi, açık-sistem, girdi-çıkı, çevresel etki ve geri beslemenin de söz konusu olduğu modern yönetim kuramlarından biri olan *sistem yaklaşımı*'ndan hareketle, sinir hücrelerinin (nöron) bir birleri arasındaki bağlantıların ve bunun oluşturduğu ağ yapının, Nesnelerin İnterneti ve E 4.0 ağ yapısına benzerliğine baktığımızda her ikisinde de meydana gelecek olumsuz (yapıcı olmayan veya yıkıcı saldırılar) etkiler düşünülürse

ve ayrıca, üretilecek ve/veya dolaşıma sokulacak bilginin manipüle edilebileceği olasılığı bile tüm sistemin defalarca gözden geçirilerek güvenli (sağlıklı) hale getirilmesinin ve bu önleyici (proaktif) girişimlerin sürekli olarak tekrarlanması “normal işleyişin sürekliliği” açısından son derece önemli ve hayati olduğu sonucuna ulaştıracaktır bizi.

Şekil 50. Sinir Hücresi (Nöron) Yapısı ve Bağlantıları



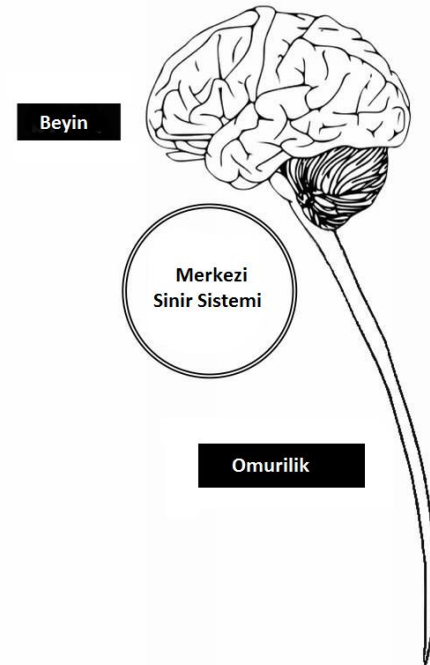
Kaynak: Araştırmacı tarafından HowStuffWorks.com sitesinde yer alan *basic neuron design* görselinden yararlanılarak geliştirilmiş ve çizilmiştir, Erişim:14.06.2019

Şekil 51. Multipl Skleroz (MS) Hastalığı

Kaynak: Araştırmacı tarafından <http://ayancikanadolu.meb.k12.tr>'de yer alan Multiple Skleroz görselinden yararlanılarak çizilmiştir, Erişim: 13.06.2019

Beyin ve Sinir Sistemi

Beyin, insan vücudunun en karmaşık parçasıdır, bilincin merkezidir ve aynı zamanda tüm istemli ve istemsiz hareket ve bedensel fonksiyonları kontrol eder. Elektrokimyasal sinyalleri taşıyan bir kanal ağı olan sinir sistemi vasıtasıyla vücudun her bir kısmı ile iletişim kurar (Biswas-Diener, 2018). Şekil 52'de görüleceği üzere merkezi sinir sistemi beyin ve omurilikten oluşmaktadır.

Şekil 52. Merkezi Sinir Sistemi

Kaynak: Biswas-Diener, 2018

Tanımlar:

Nöron: Beyin'e özgü hücreler.

Soma: Çekirdeği ve genetik bilgiyi içeren bir nöronun hücre gövdesidir. Protein sentezini yönlendirir.

Akson: Soma'dan uzayan ve diğer nöronlarla bağlantı kurmak için birkaç kez ayrılan nöronun bir parçasıdır (uzantısıdır); nöronun ana çıkışıdır.

Sinaps: Bir nöronun presinaptik terminal düğümleri ile başka bir postsinaptik nöronun dendriti, aksonu veya soma arasındaki bağlantısıdır.

Dendrit: Nöronun bir parçası olup, hücre gövdesinden (soma) uzayan ve nöronun ana veri girişinin yapıldığı dallardır.

Miyelin Kılıf: Bazı nöronların aksonlarını yalıtıcı yağ dokusudur; miyelin, nöronlar arasındaki elektriksel uyarının normal iletimi için gereklidir.

Schwann Hücresi: Periferik sinir sisteminde (beyin ve omurilik [spinal kord] dışında kalan sinir sistemi) yer alan Schwann hücreleri, nörona gelişimi ve büyümesi esnasında eşlik etmekten sorumludur.

Ranvier Düğümü: Ranvier düğümü akson uzantılarında bulunan her bir miyelin kılıfının arasındaki aralık ya da boşluktur. Miyelin kılıf arasındaki boşluk titreşim iletiminin en iyi şekilde yapılmasını sağlayarak kaybolmalarını engellemek için gereklidir. Ranvier düğümü'nün asıl fonksiyonu hareketi kolaylaştırmak ve enerji tüketiminde tasarrufa gitmektir (www.cognifit.com)

Sinir Sistemi: Vücudun elektrokimyasal iletişim ağıdır. Bu sistem, vücuttaki tüm sinir hücrelerini içerir.

Merkezi Sinir Sistemi: Beyin ve omuriliği içeren sinir sisteminin kısmıdır.

Periferik Sinir Sistemi: Merkezi sinir sistemini organlara, kaslara ve cilde bağlayan çevresel sinirleri içermektedir. Elektriksel uyarılar aracılığıyla bilgi taşırlar.

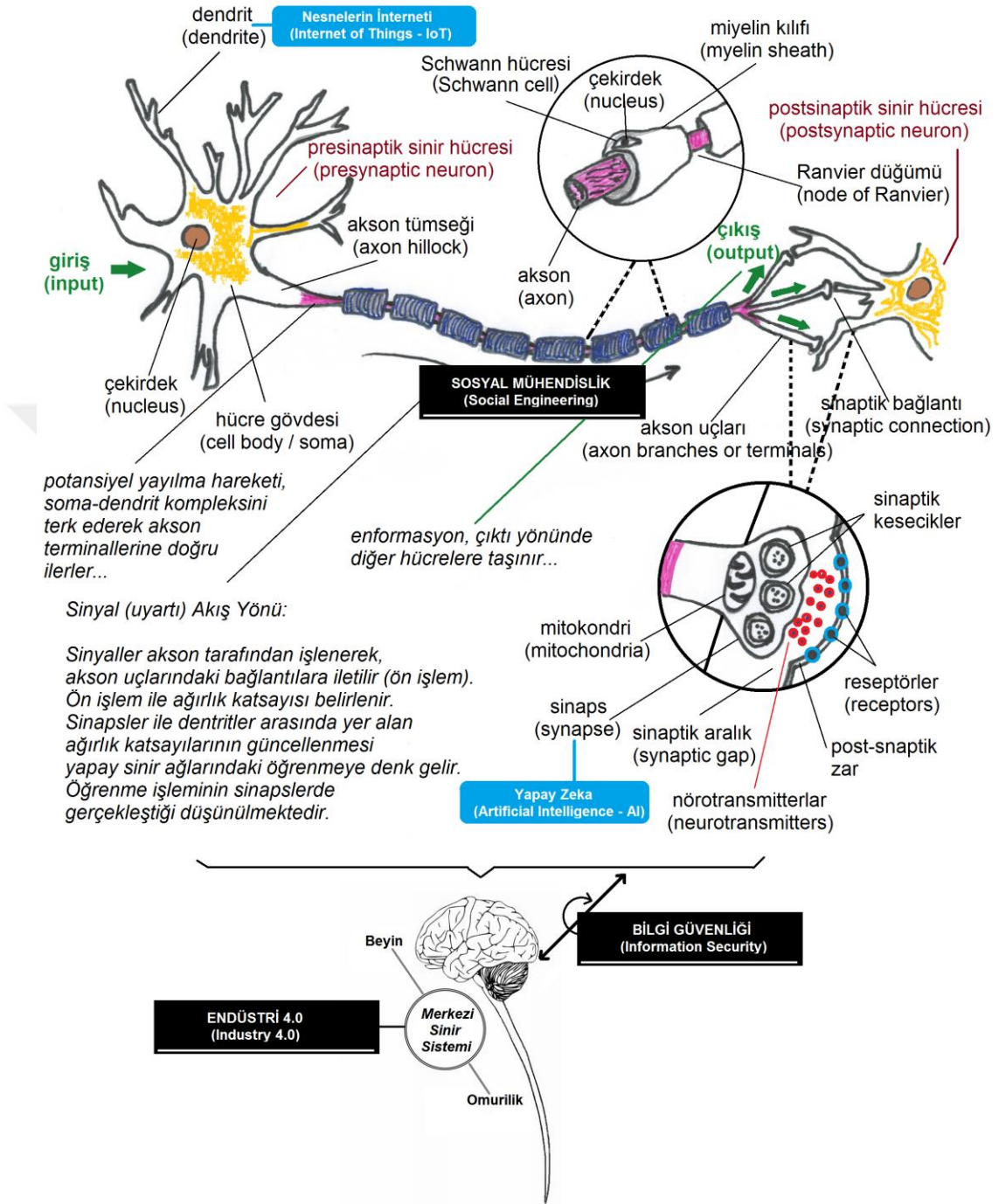
Nörotransmitter: Postsinaptik hücreye etki eden presinaptik terminal uçları tarafından salınan kimyasal madde.

Sinaptik Boşluk: Sinaptik yarık olarak da bilinir; presinaptik terminal uçları ile postsinaptik dendrit yapı, akson veya soma arasındaki küçük boşluk.

Her nöron'un girdileri vardır (giriş katmanı), bir nöron diğer bir nörona bağlanırken işlem görür (ara katman) ve bir çıktısı (çıkış katmanı) vardır. Aksonlar, elektrokimyasal iletileri, akson uçları (akson terminal) ile komşu sinir hücrelerinin reseptörleri aracılığı ile diğer sinir hücrelerine veya son organa iletirler (Berova Klinik, 2014). Bu çıktı diğer nörona geçişte bir ağırlık katsayısı ile işlem görür ve diğer nöronun girdisi olarak döngü devam eder. Dendritler girdileri, akson uçları ise çıktıları temsil eder. Ağırlık katsayıları ise sinapslara karşılık gelir.

SM, BG ve E 4.0'1, Şekil 50'de gösterilen sinir hücresi (nöron) yapısı ve bağlantılarına göre uyarladığımızda ortaya genel hatlarıyla, Şekil 53'de gösterilen tasarım model çıkmaktadır.

Şekil 53. Sosyal Mühendislik, Bilgi Güvenliği ve Endüstri 4.0'ın İlişkisel Tasarım Modellemesi



SM-BG-E 4.0 kavramları; sinir sistemi, nöron yapıları ve nöron bağlantıları ile merkezi sinir sistemi arasındaki ilişkiler üzerinden benzeştirilerek, şu şekilde modellenmiştir;

- Hücre gövdesine bağlı olan dendritlerin Nesnelerin İnternetini (tüm makinelerin -burada nöronlar kastedilmektedir- bir birlerine bağlanması) temsil ettiğini,

- Genel kabul olarak, biyolojide öğrenme işleminin sinapslerde gerçekleştiği düşünülmektedir. Sinapsler ile dendritler arasında bulunan ağırlık katsayılarının güncellenmesi yapay sinir ağlarındaki öğrenmeye denk gelmektedir. Bu nedenle sinapsler ve sinaptik bağlantıların bulunduğu yerin yapay zekâya denk düştüğünü,
- İki nöron arasındaki ana bağlantıyı oluşturan aksonların (burada uyarı -enformasyon- bir yönden diğerine doğru iletilmektedir) SM'ye denk geldiğini,
- Nöronlardan gelen uyarıların -enformasyon- beyin ve omurilikten oluşan merkezi sinir sistemine giriş ve çıkışlarında kat ettiği tüm yolların BG'yi,
- Merkezi sinir sisteminin ise E 4.0'ı temsil ettiğini düşünebiliriz.

Her birimin kendi içerisinde ayrı ayrı yapı ve görevleri bulunmakla birlikte, sistem içerisinde sürekli bağlantı ve anlık iletişim söz konusudur. Parçalardan birine ait olan çıktı diğer parçanın girdisini oluşturmakta ve döngü bu şekilde devam etmektedir. Eğer parçalardan biri devre dışı kalacak olursa, düzgün veri akışı kısmen kesilecek ve sistemde performans ve verim kayıpları oluşacaktır. Merkezi olmayan ve dağıtık yapı sayesinde sistemin işleyişi çöküntüye uğramayacak olsa da, kayıpları gidermek için yeni yapılar oluşacak fakat bu yapı parçanın bozulmadan önceki bütüne olan desteğine yakın bir destek sunmaktan kısmen uzak olacaktır. Bu nedenlerle süreçlere bir bütünlük içerisinde yaklaşmak ve ağ yapının işleyişini her boyutuyla gözeterek değerlendirmek ve kontrol etmek uygun olacaktır.

Sonuç: Biyoloji, ekoloji, sibernetik ve genel sistem teorisindeki gelişmeler organizasyonları anlamak için ortaya çıkan yeni metaforlara yol açmıştır. Bu metaforlar örgütleri insan beyni, organizma ve ekosistem olarak görmektedir. Bu metaforların ortak noktası, parçalardan bütüne bir değişimi gözetmesidir; insan ilişkilerine, insanların ve süreçlerin birbirine bağlılığına odaklanır. Aynı zamanda iç ve dış ortamdaki değişikliklere uyumluluk ve cevap verme ihtiyacına da vurgu yapar. Bu metafor aracılığıyla, organizasyonlar karşılıklı olarak birbirine bağımlı olan karmaşık ağlar olarak görülmektedir. Geri bildirim döngüleri, sistemin ortamdaki değişiklikleri izlemesini ve yanıt vermesini sağlar, tıpkı kendi kendini düzenleyen ve *kararlı denge*'ye (stable equilibrium) doğru hareket eden bir organizma gibi. Ehemmiyeti ise bir organizasyonun çevresiyle olan ilişkisini, bir organizasyonun diğer organizasyonlarla ilişkisini ve bunun yanı sıra parçalarla (bölümlerle) bütün arasındaki ilişkileri içerecek olan anlayışı ele almasındadır. Pratikte, bu

manifestonun ikinci sırasında yer alan ehemmiyet ise, örgütsel etkinliğin, bireysel ve örgütsel amaçların uyumu ile başarıldığı fikrinde ortaya çıkmaktadır (Wiggins ve Hunter, 2016, s. 10-11). Csikszentmihalyi (2017)'ye göre, kompleksliğin yararlı bir kavram olduğunu gören ilk bilim dallarından biri biyolojidir. Evrimsel biyologlar organizmaların zaman içerisinde farklılaştıklarını, giderek daha özel işlevleri olan organlara sahip olduklarını ve aynı zamanda daha da bütünleştiklerini, bütünü oluşturan parçaların birlikte daha iyi çalıştığını gözlemlemişlerdir. Bu nedenle, pek çokları evrimin birincil olarak organizmaların kompleks yapısındaki artışla ilişkili olduğunu iddia etmişlerdir (s. 90). Komplekslik ucuz bir şey değildir; öne çıkan ve kalıcı her şeyin maddi ya da psikolojik bir bedeli vardır (s. 103). Öte yandan, yapay sinir ağları (YSA), insan beyninin işlem yapma ve karar verme özelliklerinden esinlenerek oluşturulmuştur. YSA, açıklanması veya yorumlanması gereken olayın eldeki mevcut örneklerinden ya da olayın geçmiş verilerinden faydalanarak gerekli bilgiyi alır, o bilgileri öğrenerek daha önce karşılaşmamış olduğu olaylar için bu bilgileri kullanarak çözüm önerileri üretir ve çeşitli tahminlerde bulunur (Çakır, 2018, s. 19). Bir YSA hücresinde beş farklı bölüm vardır. Bunlar; girdiler (inputs), ağırlıklar (weights), toplama fonksiyonu, aktivasyon (transfer) ve çıktılarıdır (outputs). Gerçek sinir hücre yapısındaki aksonlar yapay sinir hücresinin çıktıları, dentritler toplama fonksiyonunu, çekirdek aktivasyon fonksiyonunu ve sinapsler ise ağırlıkları temsil eder (Kaftan, 2010 Akt: Çakır, 2018, s. 8)

Bu çalışmada da insan biyolojisi ve karmaşıklığından hareketle özellikle beyin nöron yapısı gözetilerek oluşturulan model ile; SM, BG ve E 4.0 kavramları benzeşim yoluyla ilişkilendirilerek ve bilhassa kesişme noktaları dikkate alınarak açıklanmaya çalışılmıştır.

4.1 Araştırmanın Yöntemi

Araştırmanın yöntemi aşağıda yer alan başlıklar altında detaylı olarak açıklanmıştır.

4.1.1 Araştırma Yaklaşımının Doğası

Bu çalışmada, neden sonuç ilişkisinden önce araştırma yapılan konu ile ilgili olarak nasıl, niçin ve ne sorularına cevap arayan nitel araştırma yöntemi kullanılmıştır. Yıldırım ve Şimşek (1999)'e göre, nitel araştırma yöntemi sosyal bilim alanında, neden-sonuç ilişkisi yerine, sosyal gerçekliği kendi içinde ve

ortamında bütüncü ve derinlemesine inceleyen, yorumlayıcı yaklaşım olarak ortaya çıkmıştır. Bryman (1992)'a göre, nitel araştırma yöntemi; katılımcı gözlemi, yarı yapılandırılmış, yapılandırılmamış görüşme tekniğini, doküman analizini ve konuşma analizlerini içermektedir.

Nitel araştırmaların, literatürde sık sık sözü edilen altı özelliği bulunmaktadır. Bunlar; doğal ortama duyarlılık, araştırmacının katılımcı rolü, bütüncü yaklaşım, algıların ortaya konması, araştırma deseninde esneklik ve tümevarıma dayalı analizdir (Yıldırım, 1999, s. 10).

Bu çalışmada yer alan üç ana kavram olan SM, BG ve E 4.0 konularının bütüncü bir yaklaşımla ortaya konulması hedeflendiği için, nitel araştırma yönteminin bu araştırmada kullanılmasının uygun olacağı düşünülmüştür. Olayların kendi doğal ortamlarında, gerçeğe en yakın şekliyle ve bütüncü bir biçimde ortaya konulabilmesinde nitel bir sürecin izlenmesi gerektiği düşüncesi bu çalışmada nitel araştırma yönteminin kullanılmasını öne çıkaran bir diğer özelliktir.

4.1.2 Araştırma Modeli (Deseni)

Araştırma deseni olarak; belgesel (documentary) araştırma ve tecrübi (empiric) araştırma birlikte tercih edilmiştir. Belgesel (documentary) araştırmalar; araştırma problemi hakkında var olan kütüphane, arşiv veya internet kaynaklarından derlenen verilere, tecrübi (empiric) araştırmalar ise; araştırma problemi hakkında gözlem, mülakat, anket, test ve diğer ölçme araçlarıyla toplanan geçerli ve güvenilir verilere dayanmaktadır (Hazar, 2019).

Bilginin yapısal olarak analiz edilmesi, kök nedenlerden ana soruna giden yolda bileşenlerin sebep-sonuç ilişkisi içerisinde ele alınmasını ve kavramların matris ilişki şeklinde irdelenmesini de içermektedir. Bu yaklaşımdan hareketle, alana yabancı olan kişilerin de kolayca kavrayabileceği, açık ve anlaşılır bir çalışma planının ortaya konulabilmesi açısından faydalı ve uygun bir yöntem olarak bilinen *mantıksal çerçeve yaklaşımı* içinde yer alan *sorun analizi* tekniği kullanılarak kök sorunlar üzerinden neden-sonuç ilişkileri de gösterilmiş, ilgili sonuçlara Bulgular Bölümünde yer verilmiştir. Sorun analizi; ana sorun, alt sorunlar ve kök sorunların tespit edilerek aralarında neden-sonuç ilişkisinin kurulmasıdır.

Alan araştırması 2019 yılı Eylül-Ekim-Kasım aylarında Türkiye ve İrlanda'da yürütülmüştür.

4.1.3 Çalışma Grubu (Örneklem)

Araştırmanın örnekleme belirlenirken *amaçlı örnekleme* (non-probabilistic sampling) yönteminden *tipik durum örnekleme* (typical sampling) yaklaşımı kullanılmıştır. Amaçlı örnekleme nitel araştırma geleneği içinde ortaya çıkmıştır. Bilindiği gibi pozitivist bilim anlayışında genelleme arzusu vardır. Tek tip bir kalıba sokma gayreti vardır. Nitel anlayışa göre farklılıklar, çeşitlilikler zenginlikler aykırılıklar da çalışmaya dâhil edilmelidir. Doğada var olan konuların bir panoraması gün yüzüne çıkartılmalıdır. Nitel araştırmada esas olan konular tüm ayrıntıları ve olası ayırt edici özellikleri ile gözler önüne serilmelidir (Abbak, 2015). Tipik durum örneklemesinde ise esas olan evrende en genel şekliyle olayı tasvir eden örneklemin bulunmasıdır. Diğer bir deyişle durumu/olguyu en iyi temsil edecek örneklemin bulunmasıdır. Nitel araştırmalarda *örneklem büyüklüğünün* (sample size) hesaplanmasında belirlenmiş bir kural bulunmamaktadır. Araştırmanın amacına ve sahip olunan olanaklara göre kararlaştırılır. Bu doğrultudan hareketle, bu araştırma için örneklem büyüklüğü toplam on farklı kurum olarak belirlenmiş, örneklem büyüklüğüne karar verme noktasında *kuramsal örnekleme* (theoretical sampling) yaklaşımı dikkate alınmıştır. Kuramsal örnekleme yaklaşımında esas olan araştırmacının doyum noktasına ulaşana kadar veri toplamaya devam etmesidir (Yıldırım ve Şimşek, 2011, s. 115).

Bilgi İşlem Teknolojileri ve benzeri alanlarda faaliyet gösteren kurum ve kuruluşlarda/şirketlerde Bilgi Teknolojileri (BT) Yöneticisi, İK Yöneticisi, Mühendis, CEO, Başkan ya da benzer pozisyonda görev yapan kişilerden veri toplanması tercih edilmiştir. Bu kurumların ise BT alanında önde gelen, tecrübeli, sektöre yön veren ve tanınmış (kurumlar) olmasına özen gösterilmiştir. Yurt içi ve yurt dışından toplam on farklı kurum seçilmiştir. Yurt dışı ayağında İrlanda tercih edilmiştir. İrlanda'nın tercih edilmesinin ana sebepleri; araştırmanın konusunda faaliyet gösteren dünyaca tanınmış ve bilinen kuruluşların Avrupa genel merkezlerinin ya da fabrikalarının bu ülkede olması ve bu sayede BT tabanlı girişimlerin dikkat çeken bir düzeyde ülke geneline ve kurumlarına yayılmış olmasıdır. İrlanda'nın, Amerika ve Avrupa teknoloji firmalarının merkez üssü niteliği taşıması ve ayrıca İngiltere'nin Avrupa Birliği'nden ayrılma sürecinde (Brexit) Londra merkezli birçok uluslararası markanın Dublin'e taşınmasını saymak mümkündür.

Türkiye’de görüşme yapılan kurum/kuruluş/şirketler:

- Ankara Cumhuriyet Başsavcılığı
- Cumhurbaşkanlığı Dijital Dönüşüm Ofisi
- Milli Savunma Bakanlığı (MSB)
- Türksat (E-Devlet Kapısı)

İrlanda’da görüşme yapılan kurum/kuruluş/şirketler:

- Aer Lingus
- Athon Institute of Technology
- Maxol Group
- Mersus Technologies
- Scott Company
- Sidero Technology Solutions Ltd.

4.1.4 Sahaya Erişim

Yurt içindeki kurumlarda görev yapan yöneticiler ile görüşme planlamasında önemli ölçüde arkadaş çevresinden yardım alınmış ve/veya internet üzerindeki iletişim bilgileri kullanılarak doğrudan görüşme talep edilmiştir. Yurt dışındaki kurum ve kişilere ulaşılmasında ise bilgi teknolojileri alanında yöneticilik yapan tanıdık çevresinden destek alınmıştır. Randevu talebinde bulunulurken görüşmenin konusu ve içeriği hakkında kısa bilgilendirme yapılarak, görüşme verilerinin doktora tezi çalışmasında kullanılacağı ifade edilmiş ve görüşmenin ortalama ne kadar süreceği belirtilmiştir. Görüşme tarihlerinin belirlenmesinde ise belirli bir gün aralığı sunularak, görüşme yapılacak kişilerin bu aralıklardan kendilerine en uygun olanı seçebilecekleri bilgisi verilmiştir.

4.1.5 Veri Toplama Teknikleri

Nitel araştırma yöntemlerinden *mülakat* tekniği ile veriler toplanmıştır. Mülakat; az sayıda ve uzman kişilerden derinlemesine bilgi ve veri alınmasını sağlayan bir yöntemdir (Kalkınma Bakanlığı, 2018, s.18). Araştırmacı, mülakat yönteminde veri toplama açısından daha fazla kontrole sahiptir. Araştırmacının bu süreçte fiili olarak yer alması yanıt oranlarını yükseltmektedir.

Bu çalışmada katılımcıların görüşlerini daha detaylı ve derinlemesine inceleyip ortaya çıkartmak için *yarı yapılandırılmış mülakat* tekniği tercih edilmiştir.

Bu tür mülakatlarda, mülakatı yapan kişi daha önceden hazırlamış olduğu soru listesini kullanmakla birlikte, görüşmenin akışına göre yan ve alt sorularla mülakatın akışını derinleştirebilmekte ve ayrıntılar elde edebilmektedir.

Mülakat soruları araştırma amacına yönelik olarak düzenlenmiş olup, daha detaylı bilgi edinebilmek açısından açık uçlu olarak hazırlanmıştır. Sorulardan herhangi biri için ihtiyaç hâsıl olduğunda (görüşmenin akışına göre) alt ve yan sorular ile daha net bilgilere ulaşılmaya çalışılmıştır.

Veri toplama aracı altı uzman kişinin görüşü alınarak düzenlenmiş olup, şu şekilde belirlenmiştir;

Mülakat Soruları:

1. Endüstri 4.0 konusundaki yaklaşım ve görüşlerinizden bahseder misiniz?
2. Bilgi Güvenliği konusundaki yaklaşım ve görüşlerinizden bahseder misiniz?
3. Sosyal Mühendislik konusundaki yaklaşım ve görüşlerinizden bahseder misiniz?
4. Endüstri 4.0 ile Bilgi Güvenliği ilişkilendirilerek yapılan çalışmalar nelerdir?
5. Endüstri 4.0 ile Sosyal Mühendislik ilişkilendirilerek yapılan çalışmalar nelerdir?
6. Bilgi Güvenliği ile Sosyal Mühendislik ilişkilendirilerek yapılan çalışmalar nelerdir?
7. Endüstri 4.0, Bilgi Güvenliği ve Sosyal Mühendislik ilişkilendirilerek yapılan çalışmalar nelerdir?
8. Endüstri 4.0, Bilgi Güvenliği ve Sosyal Mühendislik'in kesişme alanlarına ait bileşenler için önem sıralaması sizce nasıl olmalıdır?

Birinci aşama sonunda bütün ana kavramlar konuşulduğu için, ikinci aşamaya, kavramların kesişme alanlarına yönelik sorularla devam edilmiştir. Görüşme sonunda katılımcılardan, literatür değerlendirmesi sonucunda araştırmacı tarafından önceden belirlenmiş olan SM, BG ve E 4.0 kesişme alanlarına ait bileşenleri (Şekil 49) kendi görüşlerine göre önem sırasına koymaları, sonrasında ise bu listeye (varsa) eklemek istedikleri bileşenleri yazmaları istenmiştir.

4.1.6 Veri Toplama Süreci (Alan Araştırması)

Mülakat Süreci: Mülakat alt yapısı hazırlanırken, mülakat sürecinde şu süreçler takip edilmiştir:

1. *Mülakatın Planlanması*: İlk olarak, uygulanacak mülakat türü, mülakat soruları, mülakat yapılacak kişi/kurumların belirlenmesi ve mülakatın ne kadar sürede tamamlanacağı planlanmıştır. Mülakat türü ve mülakat soruları tez danışmanı, Tez İzleme Komitesi Üyeleri ve uzman akademisyenlerin görüşleri alınarak hazırlanmıştır.
2. *Pilot Uygulama*: Esas mülakatlara geçilmeden önce, eksikliklerin tespit edilmesi ve giderilmesi için pilot çalışma yapılarak mülakatın türü, mülakat soruları, ilgili formlar ve ne kadar süre içerisinde tamamlanacağına ilişkin gözlemler yapılarak mülakat planına son şekli verilmiştir.
3. *Mülakat Takviminin Hazırlanması*: Görüşme yapılacak kişi ve kurumlar, görüşme yeri, tarihi ve saatine dair detaylar yaklaşık olarak belirlenmiştir.
4. *Mülakatın Uygulanması*: Mülakat içeriği ile ilgili kısa bir bilgi verildikten sonra, ilgili tanım ve kavramlar hakkında ön bilgilendirme yapılmıştır. Gizlilik esaslarının dikkate alınacağı ve mülakata katılımın gönüllülük esasına dayalı olduğu hatırlatılarak, Katılımcı Onay Formu imzalatılmıştır. Güven ortamı oluşturulduktan sonra, katılımcının fikirlerini açık bir şekilde ifade etmesi teşvik edilmiş, görüşmenin ses kayıt cihazına alınması katılımcının yazılı izni ve onayı alındıktan sonra gerçekleştirilmiştir.

4.1.7 Pilot Uygulama

Pilot uygulama, esas mülakatlar gerçekleştirilmeden önce, eksikliklerin giderilmesi, gerekli önlemlerin alınması, mülakat süresinin yaklaşık olarak tespit edilmesi, soruların yeterince açık olup olmadığının ve katılımcı tarafından tam olarak anlaşılıp anlaşılmadığının gözlemlenebilmesi ve gerçekleştirilecek mülakata şekil ve içerik açısından son halinin verilmesi amacıyla yapılmıştır.

Pilot uygulama Eylül 2019 tarihinde Ankara’da bir kamu kurumunda üst düzey çalışanın katılımıyla gerçekleştirilmiştir. Araştırmanın amacı ve içeriği ile ilgili bir ön bilgilendirmeden sonra, araştırmacıya ait yazışma bilgileri, araştırmanın amacı, verilerin kullanımı, katılımın gönüllülük esasına dayalı olduğu, katılımcının istediği zaman mülakattan gerekçe göstermeden geri çekilebileceği ve mülakatın ses

kaydının yapılacağına dair bilgilerinin yer aldığı Katılımcı Onay Formu (Ek-1) katılımcıya okutulurken imzalatılmıştır. Sonrasında, tanım ve kavram birliği sağlanabilmesi ve mülakatın aynı düzlemde yürütüldüğünden emin olunabilmesi amacıyla, araştırma içerisinde yer alan ana kavramların (Sosyal Mühendislik, Bilgi Güvenliği ve Endüstri 4.0) kısa tanımları (Ek-2) araştırmacı tarafından okunmuştur. Ses kaydının yapılacağı bir kez daha hatırlatılarak, mülakata başlanmıştır. Önceden hazırlanan Mülakat Soruları (Ek-3) sıralı olarak katılımcıya yöneltilmiş, bazı aşamalarda, görüşmenin akışına göre tamamlayıcı ve derinleştirici sorular yöneltilmiştir. Soruların açık bir şekilde anlaşıldığı ve kolaylıkla cevap verilebildiği tespit edilmiştir. Mülakat sorularının son kısmında yer alan ilgili alanlar (SM, BG ve E 4.0'ın kesişme alanlarına ait bileşenlerin önem sırasına göre numaralandırılması, varsa yeni bileşenlerin önerilmesi, katılımcıya ait bazı bilgiler) katılımcıya doldurtularak teşekkür edilip görüşme sonlandırılmıştır. Mülakat süresi yaklaşık olarak 40 dakika sürmüştür.

4.1.8 Mülakat Görüşmeleri

Pilot görüşmede gerçekleştirilen yöntem aynı şekilde mülakat görüşmelerinde de kullanılmıştır. Verilerin toplanması için on farklı oturum gerçekleştirilmiştir. Ses kayıt cihazı kullanılarak toplam iki yüz elli beş dakikalık sekiz ayrı ses kaydı (oturum başına ortalama otuz iki dakika) yapılmıştır. Not alınarak yapılan iki görüşmenin toplam süresi ise yüz on dakika (oturum başına ortalama elli beş dakika) sürmüştür. Oturumların toplam süresi üç yüz altmış beş dakikadan (oturum başına ortalama otuz altı nokta beş dakika) oluşmuştur.

4.1.9 Verilerin Analizi

Creswell (2015)'e göre, nitel veri analizinin temel unsurları; veri kodlamanın ana basamakları (verileri anlamlı bölümlere indirgeme ve bölümlere isim verme) kodları geniş kategoriler veya temalar altında birleştirme ve veri grafiklerinde, tablolarda ve çizelgelerde karşılaştırmalar yapma ve sunma üzerine yorum yapmaktır (s. 180). Veritabanı büyüklüğü ne olursa olsun, genel olarak, 25-30 bilgi kategorisinden daha fazlası geliştirilmemekte, en sonunda da anlatıyı yazmak için kullanılacak beş ya da altı temaya indirgemeye ve birleştirilmeye çalışılmaktadır (s. 184). Nitel araştırmalarda *temalar* (kategoriler olarak da adlandırılmaktadır) ortak bir fikir oluşturmak için bir araya getirilmiş birkaç koddan oluşan geniş bilgi birimleridir

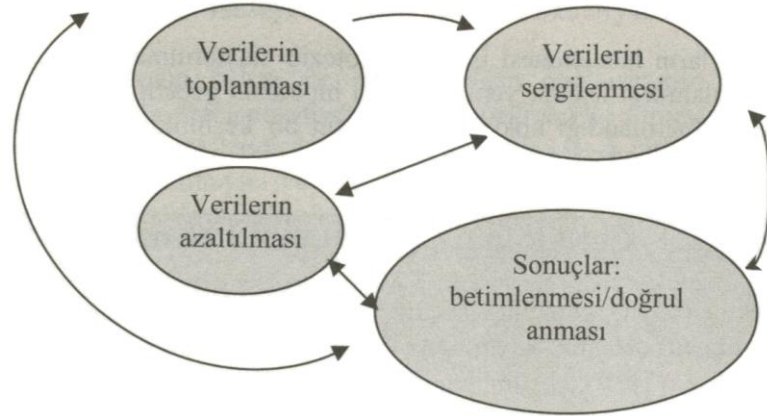
(s. 186). Nitel arařtırmalarda veri *yorumlama*, kodların ve temaların ötesinde verilerin daha geniş anlamlarına yönelik soyutlama içermektedir. Veri *sunma* ise, son aşamada, arařtırmacıların ne bulduklarının, metin, tablo veya şekilden oluşan bir paket halinde sunulmasıdır (s. 187). Güvenirlik; eğer arařtırmacı görüşmeyi/ notlarını yüksek kalitede bir ses kayıt cihazıyla kaydetmiş ve bunları yazıya aktarmışsa, güvenirlik artırılabilir. Verilerin analiz edilmesi ve kodlanması için bilgisayar programlarının kullanılması da güvenirliliği artırır. Kodlayıcılar arası görüş birliği de güvenirliliği destekler (Silverman, 2005 Akt: Creswell, 2015, s. 253). Kodları mı, temaları mı, yoksa hem kodlar hem temalar üzerinde bir anlařmaya varılacağı kodlayıcılar arasında belirlenebilir (Amstrong vd., 1997 Akt: Creswell, 2015, s. 253).

Creswell'in önermiş olduđu nitel veri analizinde kullanılan temel unsurları Miles ve Huberman'ın nitel veri çözümlemesinde önerdikleri ve Miles ve Huberman Modeli olarak bilinen model de desteklemektedir. Punch (2014, s. 191-193), bu modelde yer alan ve verilerin toplanmasından sonra yer alan bileřenleri; “verilerin azaltılması”, “verilerin sergilenmesi”, “sonuçların betimlenmesi ve dođrulanması” olarak bilinen ve birbirlerini eř zamanlı etkileyen üç aşamadan oluştuđunu ifade etmektedir. Punch (2014, s. 192-193) bu aşamaları kısaca řu şekilde açıklamaktadır:

- *Verilerin Azaltılması*: Veri azatılımı, çözümleme boyunca devam eder. Bu, çözümlemeden ayrı bir řey deđil, çözümlemenin bir parçasıdır. Bu işlem, çözümlemenin erken aşamalarında verilerin düzenlenmesi, bölümlenmesi ve özetlenmesi sırasında olur.
- *Verilerin Sunulması*: Verilerin sunumu; bilgileri düzenler, sıkıřtırır ve birleřtirir.
- *Sonuçların Biçimlendirilmesi ve Dođrulanması*: Verilerin azaltılması ve sunulmasının amacı, sonuçlara ulařmaya yardım etmektir. Mantıksal olarak sonuçlara ulařma, veri azatılımı ve sunumunu takiben gerçekleře de aslında, onlarla hemen hemen eř zamanlı olarak geliřir.

Bu üç adım, çözümleme boyunca iç içe geçmiş ve eşzamanlı olarak gerçekleřir. Şekil 54'de veri çözümlemesinin bileřenleri ve etkileřim yönleri görsel olarak verilmiřtir.

Şekil 54. Veri Çözümlemesinin Bileşenleri: Etkileşimli Model

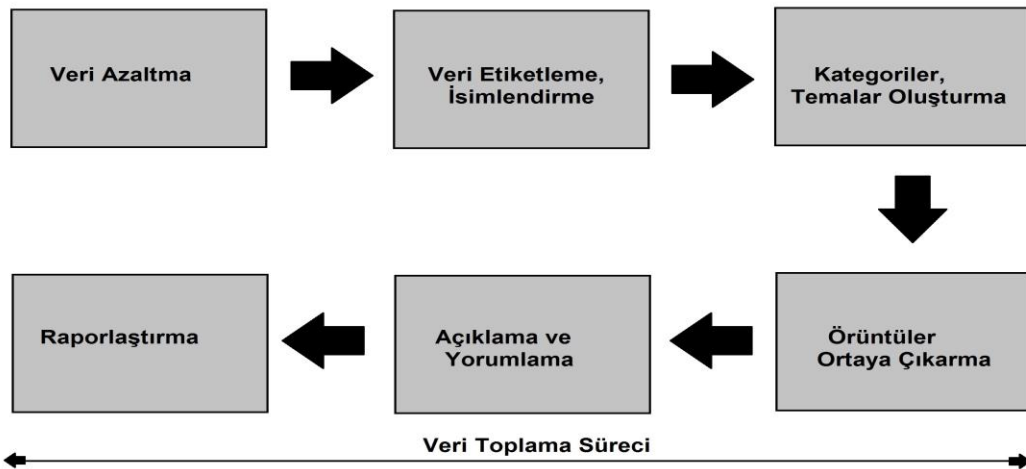


Kaynak: Miles ve Huberman, 1994, s. 12 Akt: Punch, 2014, s. 192

Nitel veri analizi, keşifsel bir süreç olarak değerlendirilmelidir. Bu süreçte, araştırmacı verileri düzenler, tasnif eder, sentezler, örüntüler çıkarır ve kavramlara ulaşarak bulguları raporlaştırır. (...) Nitel veri analizi konusunda ortak bir yöntem ve izlenmesi gereken kesin adımlar yoktur. Şekil 55’de gösterilen ve farklı araştırmacılar tarafından ileri sürülen yöntemlerin ortak özellikleri olarak şunlar sıralanabilir (Gürbüz ve Şahin, 2016, s. 427):

- Veri toplama süreci ve veri kayıt işlemi
- Verinin çeşitli kavramlara tasnifi veya kategorilere ayrılması
- Kavramlar veya kategoriler arasında bağlantılar kurulması
- Araştırmanın raporlaştırılması

Şekil 55. Nitel Veri Analizi Süreci



Kaynak: Gürbüz ve Şahin, 2016, s. 427.

Gürbüz ve Şahin (2016)'e göre, nitel veri analizi, tümevarımcı bir yaklaşım sergileyerek gerçekliği ortaya çıkarmaya ve anlamaya çalışmaktır. Başlangıç aşamasında çeşitli yöntem ve teknikler kullanmak suretiyle elde edilen verilerin detaylı bir incelemesi yapılır. Bu incelemede, araştırma konusuyla ilgili veriler alınır, diğerleri ayıklanır. Bu şekilde veri azaltılması işlemi yapılarak, analiz işlemine tabi tutulanlar isimlendirilir veya kodlanır. Bu şekilde etiketlenen verilerden benzer olanları aynı kategori veya temalar içerisinde toplanır. Bu kategoriler veya temalar da isimlendirilmelidir. Sonrasında, tema veya kategoriler birbirleriyle karşılaştırılarak aralarında ne tür bağlantıların olduğu ortaya çıkarılmaya çalışılır ve bu doğrultuda açıklamalar ve yorumlar yapılır. (...) Son aşamada ise araştırmanın raporlaştırılması yer alır (s. 428).

Yukarıda yer alan açıklamalar doğrultusunda, gerçekleştirilen mülakatlar sonucunda elde edilen veriler yazılı metin haline getirilebilmeleri için bilgisayar ortamına aktarılmıştır. Görüşme sonucu elde edilen verilerin (ses kayıtlarının) metne çevrilmesindeki bir diğer amaç ise gözlemciler arası güvenliğin teyidini sağlamaya alt yapı oluşturmak ve ilgili yazılım programı ile kodlama yapılabilmesine ön hazırlık yapmaktır. Türkçe ses kayıtlarının metinlere doğru çevrildiğinin (çözümlemenin) teyidini yapmak için bir kişiden yardım alınmıştır. İngilizce ses kayıtlarının yazılı metin haline getirilmesi için ana dili İngilizce olan bir kişiden yardım alınmıştır. İngilizce metinlerin Türkçe'ye doğru çevrildiğinin (tercümesinin) teyidi için ise YÖKDİL sınavından yüz tam puan üzerinden doksan üzeri puan almış bir kişinin yardımı alınmıştır.

Verilerin analizinde betimsel analiz ve içerik analizi kullanılmıştır.

Betimsel analiz yaklaşımına göre; elde edilen veriler, daha önceden belirlenen temalara göre özetlenir ve yorumlanır. Veriler araştırma sorularının ortaya koyduğu temalara göre düzenlenebileceği gibi, görüşme ve gözlem süreçlerinde kullanılan sorular ya da boyutlar dikkate alınarak da sunulabilir. Katılımcının görüşlerinden doğrudan alıntılara sık sık yer verilebilir (Yıldırım ve Şimşek, 2013, s. 256). Betimsel analizde veriler, farklı kişilerin aynı soru hakkında farklı düşüncelerinin görüşmede elde edildiği şekliyle değiştirilmeden alıntılar şeklinde aktarılır. Betimsel analiz dört aşamadan oluşur (Altunışık, Coşkun, Yıldırım ve Bayraktaroğlu, 2010, s. 322):

- Betimsel analiz için bir çerçeve oluşturma
- Tematik çerçeveye göre verilerin işlenmesi
- Bulguların tanımlanması
- Bulguların yorumlanması

İçerik analizinde temel amaç ise; görüşmelerden toplanan verileri açıklayabilecek kavramlara ve ilişkilere ulaşmaktır. Betimsel analizde özetlenen ve yorumlanan veriler, içerik analizinde daha derin bir işleme tabi tutulur. Betimsel bir yaklaşımla keşfedilemeyen kavram ve temalar bu analiz sonucu keşfedilebilir. İçerik analiziyle, verilerin içerisinde saklı olabilecek gerçeklerin ortaya çıkartılmasına çalışılır. Temelde yapılan işlem, birbirine benzeyen verileri belirli kavramlar ve temalar çerçevesinde bir araya getirmek ve bunları okuyucunun anlayabileceği bir biçimde düzenleyerek yorumlamaktır (Yıldırım ve Şimşek, 2013, s. 259).

Nitel araştırmada araştırmacı, incelenen olguya yakın olduğu, sürecin doğal bir parçası olduğu ve gerekirse o olguya ilişkin ilk elden deneyimler edindiği için yorumları değerlidir (Yıldırım ve Şimşek, 2013, s. 270).

Yukarıda yer verilen açıklamalar doğrultusunda; görüşme verilerinden kodlama tekniğiyle temalara ulaşılmış, kodların doğru temalara çevrilip çevrilmediği için uzman görüşü alınmış (Nitel Araştırma Yöntemleri dersi veren iki ayrı Dr. Öğr. Üyesinden), temalar arası örüntü ortaya çıkartılmaya çalışılmış ve sonrasında betimsel analizin yanı sıra içerik analizi ile yorumlanması ve sunumu yapılmıştır. Araştırmada elde edilen verilerin kodlanmasında NVivo Programı Ver. 10'dan yararlanılmıştır.

İç geçerlilik için; katılımcılardan doğrudan alıntılara yer verilmiş, görüşme içerikleri (not alınarak yapılanlar) katılımcılara teyit ettirilmiştir. Dış geçerlilik için; araştırmanın aktarılabilirliği, transfer edilebilirliği (benzer bir araştırmanın bu araştırmanın basamaklarının izlenerek yapılabilmesi) için tüm aşamalar ayrıntılı olarak açıklanmıştır. İç güvenirlik (tutarlılık) için; bulgular yorum yapılmadan verilmiş, kodlama tutarlılığı için ise uzmanlara gösterilmiş, fikir birliği sağlanmıştır. Dış güvenirlik (teyit edilebilirlik) için ise; uzmanlara kontrol ettirilerek araştırmanın verilerinin sonuçlarla tutarlı olduğu teyit ettirilmiştir.

4.1.10 Etik

Bu arařtırmada etik kural ve deęerler ok dikkatli bir řekilde ele alınarak, verilerin en uygun řekilde toplanması ve alıřmaya aktarılması iin gerekli hassasiyet gsterilmiřtir. Aynı zamanda, eřitli uzman grř ve yardımlarına da bařvurularak subjektif tutum ve yorumlardan kaınılmaya alıřılmıřtır. Bu doęrultuda, ayrıca;

- Grřme sorularının izni ilgili enstitden alınmıřtır.
- Grřme yapılan kiřilerin isimleri gizli tutulmuřtur.
- Soru sorulurken ynlendirmelerden uzak durulmuřtur.
- Grřmelerden elde edilen verilerin deęiřtirilmeden kullanıldıęı uzman kiřilere teyit ettirilmiřtir.
- Veri analizi yapılırken arařtırmacının yorum ve grřlerine yer verilmeden, objektif kalınmıřtır.
- Onay İzin Formu: “Katılımcıların kimliklerinin saklı tutulması kaydı ile yapılan bu grřmeye ait metin ierikleri ve verilerin doktora tezinde kullanılmasını onaylıyorum” ibaresinin yer aldıęı *onay izin formu* imzalatılmıřtır.

4.2 Bulgular

Bu blmde arařtırmanın bulgularına yer verilmiřtir. Bulgular sekiz ayrı bařlık altında řu řekilde sınıflandırılmıřtır:

- Demografik Verilere Ait Bulgular
- Literatr Arařtırması Sonucunda Elde Edilen SM, BG ve E 4.0’ın Kesiřme Alanlarına Ait Bileřenlerin Katılımcılara Gre nem Sıralaması
- Katılımcılar Tarafından nerilen Bileřenler
- Sorun Analizine Ynelik Bulgular
- Katılımcıların SM, BG ve E 4.0’ın İliřkilendirilmesine Ynelik Dřncelerine Ait Bulgular
- Katılımcıların Endstri 4.0 Baęlamında Yeniliki Teknolojilere Ynelik Olumlu ve Olumsuz Grřlerine Ait Bulgular
- Kodlama, Kategori ve Temalar
- Kodlama Kelime Frekans Daęılımları

“Demografik Verilere Ait Bulgular” başlığı altında; Tablo 9’da çalışma grubuna ait demografik veriler, Tablo 10’da yaş grubuna ait tanımlayıcı istatistikler, Tablo 11’de meslek/eğitim çapraz tablolama yer almaktadır.

“Literatür Araştırması Sonucunda Elde Edilen SM, BG ve E 4.0’ın Kesişme Alanlarına Ait Bileşenlerin Katılımcılara Göre Önem Sıralaması” başlığı altında; Tablo 12’de SM, BG ve E 4.0’ın kesişme alanlarına ait bileşenlerin katılımcılara göre önem sıralaması, Şekil 56’da en önemli (ilk) üç bileşen, Şekil 57’de en az önemli (son) üç bileşen, Şekil 58’de SM, BG ve E 4.0’ın kesişme alanlarına ait bileşenlerin katılımcılara göre önem sıralaması-I, Şekil 59’da SM, BG ve E 4.0’ın kesişme alanlarına ait bileşenlerin katılımcılara göre önem sıralaması-II yer almaktadır.

“Katılımcılar Tarafından Önerilen Bileşenler” başlığı altında; Tablo 13’de katılımcılar tarafından önerilen diğer bileşenler, Şekil 60’da SM, BG ve E 4.0’ın kesişme alanlarına ait tüm bileşenler ve önem sıralaması yer almaktadır.

“Sorun Analizine Yönelik Bulgular” başlığı altında; Şekil 61’de sorun analizi-I (literatür araştırması sonucuna göre), Tablo 14’de literatür araştırması sonucunda oluşturulan sorun analizi’nde (Şekil 61) yer alan tespitlere yönelik olarak katılımcıların söylemlerinden elde edilen destekleyici bulgular, Tablo 15’de literatür araştırması sonucunda oluşturulan sorun analizi’nde (Şekil 61) yer almayan fakat alan araştırması sonucunda sorun analizine eklenen tespitlere (Şekil 62) yönelik olarak katılımcıların söylemlerinden elde edilen bulgular yer almaktadır.

“Katılımcıların SM, BG ve E 4.0’ın İlişkilendirilmesine Yönelik Düşüncelerine Ait Bulgular” başlığı altında; Tablo 16’da katılımcıların SM, BG ve E 4.0’ın ilişkilendirilmesine yönelik düşünceleri-I, Tablo 17’de katılımcıların SM, BG ve E 4.0’ın ilişkilendirilmesine yönelik düşünceleri-II yer almaktadır.

“Katılımcıların Endüstri 4.0 Bağlamında Yenilikçi Teknolojilere Yönelik Olumlu ve Olumsuz Görüşlerine Ait Bulgular” başlığı altında; Tablo 18’de katılımcıların endüstri 4.0 bağlamında yenilikçi teknolojilere yönelik olumlu ve olumsuz görüşleri yer almaktadır.

“Kodlama, Kategori ve Temalar” başlığı altında; Şekil 63’de SM, BG ve E 4.0 temalarına ait kategoriler, Tablo 19’da kodlama ve kategorilerin oluşturulması, Tablo 20’de düğüm özeti raporu (*node summary report*) (NVivo 10 uygulaması),

Şekil 64’de kodlama sonucu elde edilen kavramların kaynaklarla olan ilişkisi yer almaktadır.

“Kodlama Kelime Frekans Dağılımları” başlığı altında; Şekil 65’de kodlama yapılarak kategorilerin oluşturulmasında en sık kullanılan 100 kelime (frekans yüksekliğine göre) (NVivo 10 uygulaması), Şekil 66’da frekansı en yüksek 100 kelime için ekran sorgulama görüntüsü (NVivo 10 uygulaması) yer almaktadır.

4.2.1 Demografik Verilere Ait Bulgular

Tablo 9 incelendiğinde çalışma grubuna ait demografik veriler, Tablo 10 incelendiğinde yaş grubu için elde edilen tanımlayıcı istatistikler, Tablo 11 incelendiğinde ise çalışma grubunda yer alan kişilerin meslek ve eğitimlerine yönelik bulgular (çapraz tablolama) yer almaktadır.

Tablo 9. Çalışma Grubuna Ait Demografik Veriler

Yaş	Meslek	Kaç yıldır bu kurumda çalışıyor	Pozisyonu / Görevi	Sektörde kaç yıldır çalışıyor	Eğitimi
39	Akademisyen	9	Öğretim Görevlisi / Bilgisayar Bilimleri	9	Doktora
49	Dijital Medya Yapımcısı	7	Kurucu CEO	31	Lisans
52	Hukukçu	16	Başsavcı Vekili	28	Y Lisans
40	Mühendis	5	Başkan	18	Doktora
37	Mühendis	14	Direktör	14	Y Lisans
33	Subay	3	Yüzbaşı	13	Y Lisans
57	Yönetici	7	Genel Müdür	20	Lise
56	Yönetici	37	Yönetici / Uçuş, Perakende, Muhasebe ve Raporlama	15	Lise
44	Yönetici	5	Yönetici / Operasyon Planlama ve Finans	20	Lisans
50	Yönetici	4	Yönetici / Teknik Lider	20	Y Lisans
56	Yönetici	12	Bilgi İşlem Teknolojileri Başkanı	30	Y Lisans

Tablo 9’da yer alan katılımcı profili incelendiğinde genel olarak farklı meslek gruplarının bir araya geldiği, büyük çoğunluğunun lisans üstü eğitimi aldığı, çoğunluğunun yönetici pozisyonunda görev yaptığı, şu an çalıştıkları kurumlarındaki çalışma süreleri dikkate alındığında ortalama 11 yıl, sektörde çalışma süreleri dikkate alındığında ise ortalama 20 yıllık bir tecrübeye sahip oldukları görülmektedir.

Tablo 10. Yaş Grubuna Ait Tanımlayıcı İstatistikler

Yaş		
N	Geçerli	11
	Kayıp	0
Ortalama		46,6364
Ortalama Std. Hata		2,55226
Medyan		49,0000
Mod		56,00
Std. Sapma		8,46490
Varyans		71,655
Açıklık		24,00
Minimum		33,00
Maksimum		57,00
Toplam		513,00

Tablo 10 incelendiğinde katılımcıların yaş ortalamasının 46,6364, medyan değer 49,0000, minimum değer 33,00, maksimum değer 57,00 olduğu görülmektedir.

Tablo 11. Meslek/Eğitim Çapraz Tablolama

Sayı		Eğitim				Toplam
		Lise	Lisans	Yüksek Lisans	Doktora	
Meslek	Akademisyen	0	0	0	1	1
	Digital Medya Yapımcısı	0	1	0	0	1
	Hukukçu	0	0	1	0	1
	Mühendis	0	0	1	1	2
	Subay	0	0	1	0	1
	Yönetici	2	1	2	0	5
	Toplam	2	2	5	2	11

Tablo 11 incelendiğinde meslek grubunda 1 akademisyen, 1 dijital medya yapımcısı, 1 hukukçu, 2 mühendis, 1 subay ve 5 yöneticinin bulunduğu görülmektedir. Mezuniyet durumlarına bakıldığında ise; 2 lise, 2 lisans, 5 yüksek lisans ve 2 doktora'dan oluştuğu görülmektedir.

4.2.2 Literatür Araştırması Sonucunda Elde Edilen Sosyal Mühendislik, Bilgi Güvenliği ve Endüstri 4.0'ın Kesişme Alanlarına Ait Bileşenlerin Katılımcılara Göre Önem Sıralaması

Araştırmaya ait literatür araştırması sonucu SM, BG ve E 4.0 kesişme alanına ait tespit edilen en önemli on bir bileşenin (*Teknoloji Okuryazarlığı, İnsan Faktörü, Kimlik Hırsızlığı, Veri ve Bilgi Güvenliği, Fiziksel Güvenlik, Siber Güvenlik, Ulusal Güvenlik, Dağıtık ve Merkezi Olmayan Yapı, Standartların Geliştirilmesi, Risk Yönetimi, Bütüncü Yaklaşım*) önem sırası nasıl olmalıdır? sorusuna A, B, C, D, E, F, G, H, I, J, K katılımcılarının verdikleri cevaplar dikkate alındığında önem sıralamasının ne şekilde oluştuğu ve kümелendiği Tablo 12'de verilmiştir:

Tablo 12. Sosyal Mühendislik, Bilgi Güvenliği ve Endüstri 4.0'ın Kesişme Alanlarına Ait Bileşenlerin Katılımcılara Göre Önem Sıralaması

Bileşenler	Katılımcılara Göre Bileşenlerin Önem Sıralaması (1-11)										
	I.	II.	III.	IV.	V.	VI.	VII.	VIII.	IX.	X.	XI.
Teknoloji Okur-Yazarlığı	D,J	I	B	C,K	A,H	E					F,G
İnsan Faktörü	A,B,C .E,I	D		H	J,K		F,G				
Kimlik Hırsızlığı		K	G	F		B		J		A,C	D,E,H .I
Veri ve Bilgi Güvenliği	F,G	H	C,K	A,D	B	I	E,J				
Fiziksel Güvenlik	K	E		G	D	F,H			C	I	A,B,J
Siber Güvenlik		C	A,F,H	B	G,I	D,K		E	J		
Ulusal Güvenlik		A,B,F, G	E			C	H	D,I		J	K
Dağıtık ve Merkezi Olmayan Yapı	H			E,J				G	A,B,I	D,F,K	C
Standartların Geliştirilmesi			D,J	I			C	A,B	F,G,H .K	E	
Risk Yönetimi					F	A,G,J	D,I,K	C,H	E	B	
Bütüncü (Holistik) Yaklaşım		J	I		C,E		A,B	F,K	D	G,H	

Tablo 12 incelendiğinde, SM, BG ve E 4.0'ın kesişme alanlarına yönelik olarak belirlenen bileşenlerin katılımcılara göre önem sıralaması sorulduğunda en önemli ilk üç bileşenin sıralaması “İnsan Faktörü”, “Ulusal Güvenlik” ve “Siber Güvenlik” olarak belirlenirken (Şekil 56), son üç sırada yer alan bileşenlerin sıralaması “Kimlik Hırsızlığı”, “Dağıtık ve Merkezi Olmayan Yapı” ve “Standartların Geliştirilmesi” şeklindedir (Şekil 57).

Şekil 56. En Önemli (İlk) Üç Bileşen

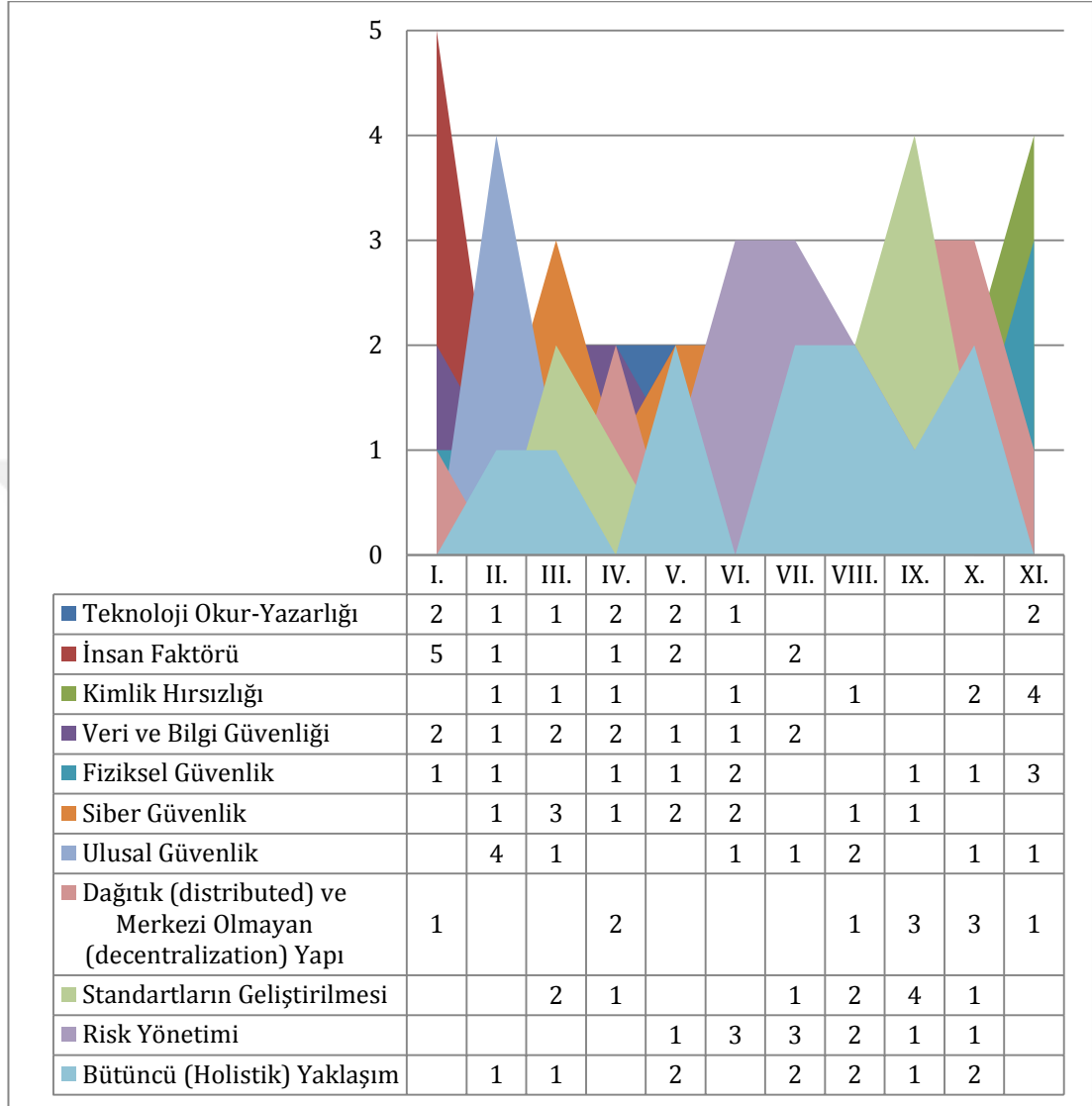


Şekil 57. En Az Önemli (Son) Üç Bileşen

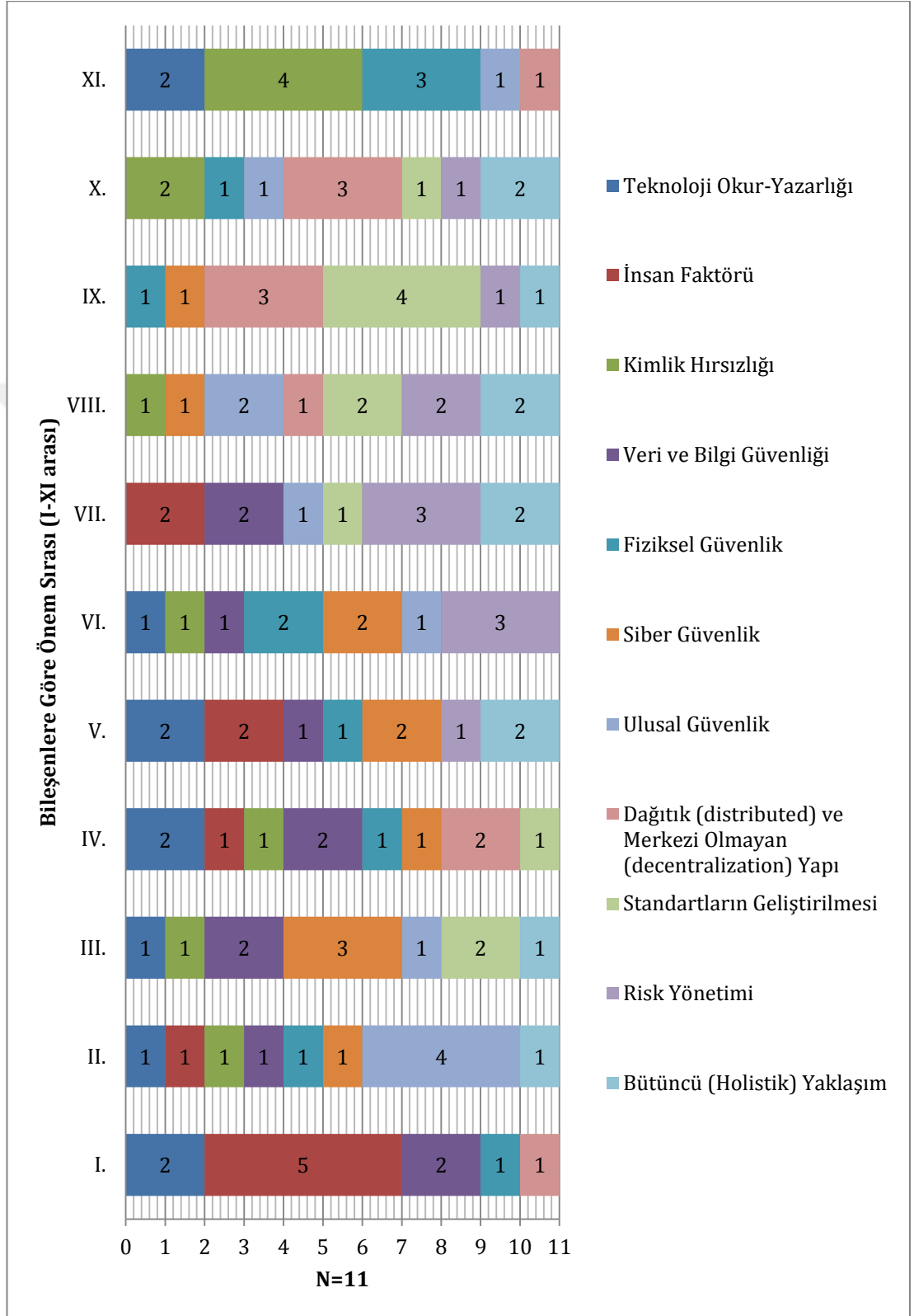


Tablo 12’de yer alan ve SM, BG ve E 4.0’ın kesişme alanına ait bileşenlerin katılımcılara göre önem sıralamasına ait farklı bakış açıları geliştirilebilmesi için aynı Tablo, Şekil 58 ve Şekil 59’da değişik grafiklerle de ifade edilmeye çalışılmıştır. Şekil 58 ve Şekil 59’da yer alan Roma rakamları bileşenlerin önem sırasını gösterirken, her bileşenin karşısında yer alan sütunda bulunan rakamlar ise katılımcılardan kaç kişinin ilgili bileşeni seçmiş olduğunu ifade etmektedir.

Şekil 58. Sosyal Mühendislik, Bilgi Güvenliği ve Endüstri 4.0'ın Kesişme Alanlarına Ait Bileşenlerin Katılımcılara Göre Önem Sıralaması-I



Şekil 59. Sosyal Mühendislik, Bilgi Güvenliği ve Endüstri 4.0'ın Kesişme Alanlarına Ait Bileşenlerin Katılımcılara Göre Önem Sıralaması-II



4.2.3 Katılımcılar Tarafından Önerilen Bileşenler

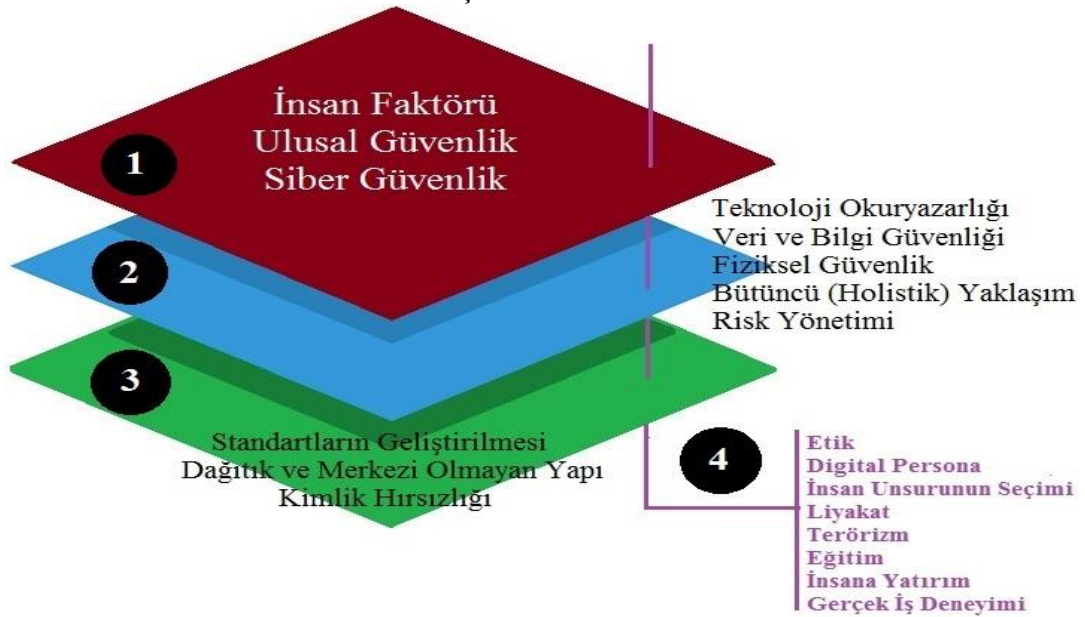
Tablo 13’de, literatür araştırması sonucu SM, BG ve E 4.0’ın kesişme alanlarına ait tespit edilen en önemli on bir bileşenin (Tablo 12) haricinde, alan araştırmasında yapılan görüşmeler neticesinde katılımcılar tarafından önemli olduğu düşünülen ve listeye eklenmesi için önerilen diğer bileşenler yer almaktadır.

Tablo 13. Katılımcılar Tarafından Önerilen Diğer Bileşenler

• Etik • Digital Persona (Kimlik Doğrulama Platformu) • İnsan Unsurunun Seçimi • Liyakat • Terörizm • Eğitim • İnsana Yatırım • Gerçek İş Deneyimi

Katılımcılar tarafından önerilen ve Tablo 13’de ifade edilen bu bileşenler Şekil 60’da “4” numara ile, literatür araştırması sonucunda elde edilen bileşenler ise “1”, “2” ve “3” numaraları ile gösterilmiştir.

Şekil 60. Sosyal Mühendislik, Bilgi Güvenliği ve Endüstri 4.0’ın Kesişme Alanlarına Ait Tüm Bileşenler ve Önem Sıralaması



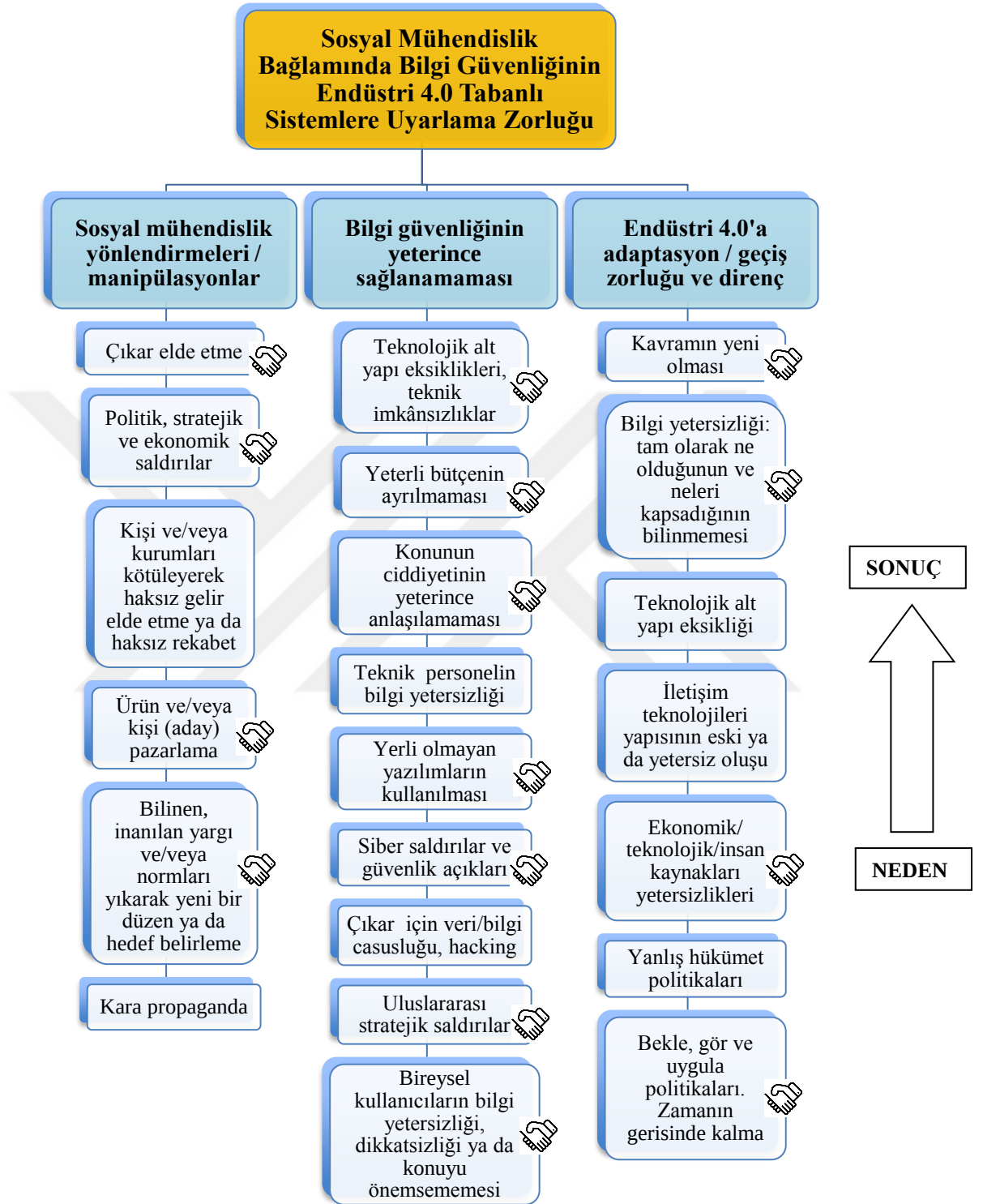
Katılımcıların önermiş oldukları bileşenler (4 numaralı) için ayrıca bir önem sıralaması yapmaları istenemediğinden bu bileşenlerin üç ana katmandan (1-2-3 numaralı) hangisine ait olabileceğine dair bir fikir yürütülmemiştir. 1 numaralı katman en önemli/kritik katmanı ifade etmektedir.

4.2.4 Sorun Analizine Yönelik Bulgular

Mantıksal Çerçeve Yaklaşımı aşamalarından biri olan sorun analizinde; ana sorun, alt sorunlar ve kök sorunların belirlenmesine çalışılır. Aralarında aşağıdan yukarıya doğru neden-sonuç ilişkisi kurulur. Ana sorunun analizi için; bu sorundan en çok etkilenenlerin kimler olduğu, kök nedenlerin neler olduğu, sorunun ilk ortaya çıkış zamanı ve sorunun çözümü için şu ana dek nelerin yapıldığı vb. bulgular ortaya konulmaya çalışılmaktadır.

SM, BG ve E 4.0 için ortaya konulan kavramsal çerçeve ve paralelinde yapılan literatür araştırması sonucunda elde edilen veriler (Şekil 61) “SM Bağlamında BG’nin E 4.0 Tabanlı Sistemlere Uyarılma Zorluğu Sorun Analizini” hazırlamada belirleyici olmuştur ve sorun analizi neden-sonuç ilişkisi içerisinde ortaya konulmuştur. Alan araştırması sonucunda elde edilen veriler ışığında katılımcılar tarafından da teyit edildiği tespit edilen bulgular Şekil 61’de el sıkışma görseli “” ile işaretlenmiştir. Bu (el sıkışma görseli ile işaretlenmiş olan) bulguları teyit olarak, katılımcılar tarafından görüşme esnasında zikredilen cümlelerden alıntılara (bulgulara) Tablo 14’de tırnak içerisinde yer verilmiştir. Literatür araştırması sonucu hazırlanan “sorun analizi”nde (Şekil 61) yer almayıp, görüşmelerde katılımcılar tarafından ifade edilen ve sorun analizine ilave edilebilecek bulgulara Şekil 62’de, bu bulguları teyit edici alıntılara ise Tablo 15’de yer verilmiştir.

Şekil 61. Sorun Analizi-I (Literatür Araştırması Sonucuna Göre)



Kök Sorunlar: Eğitim politikaları, az gelişmişlik, daha öncelikli problemler, yüksek maliyet, yetersiz entelektüel sermaye (İK) vb.

Tablo 14. Literatür Araştırması Sonucunda Oluşturulan Sorun Analizi'nde (Şekil 61) Yer Alan Tespitlere Yönelik Olarak Katılımcıların Söylemlerinden Elde Edilen Destekleyici Bulgular



Sosyal mühendislik yönlendirmeleri / manipülasyonlar	
Çıkar elde etme	[Katılımcı B»] “Maddi kazanç sağlama imkânı varmış gibi çeşitli öneriler sunularak da insanlar kandırılmaya çalışılıyor.” [Katılımcı D»] “Son zamanlarda bunların sayısı artmaya başlayınca emniyetle görüşmeye başladık.”, “Vatandaşın güvenliğini sarsıcı olarak bu kişiler vatandaşın bilgisini bizim adımızı kullanarak ele geçirmeye çalışıyorlar...”, “Vatandaşın kredi kartını ele geçirmeye, neyden mağdur olduklarını bildikleri için buna yönelik ilişkilendirmeler yapıyorlar, bunu kullanmaya çalışıyorlar.” [Katılımcı F»] “Bu tür saldırıları duyduk; BT güvenliği, bu tür e-postalar aldığımızda ya da şu adreslerden bir e-posta geldiğinde ekleri açmamamız gerektiğini belirten uyarılar yapar.”, “Çok şey söyleyebilirim ama oldukça fazla ‘oltalama’ faaliyeti var.”, “Ayrıca giderek artan kredi kartı güvenliği meseleleri. Kredi kartı bilgilerinin ele geçirilmesini hepimiz duyduk. Amazon’dan bile kredi kartı dökümleri ele geçirildi.” [Katılımcı F»] “Evet, karşı karşıya olduğumuz en önemli şey kimlik avı/oltalama (phishing) saldırılarıdır.” [Katılımcı H»] “Evet, demek istediğim hedef gözetilerek yapılan kimlik avı/oltalama saldırısı bir çeşit sosyal mühendisliktir.”
Politik, stratejik ve ekonomik saldırılar	[Katılımcı A»] “ABD sırf bu yüzden Huawei firmasının faaliyetlerini kendi ülkesinde yasakladı.”, “En son ve güncellik açısından herkesin bildiği gibi ABD seçimlerinde sosyal mühendislik yapılarak yönlendirme yapıldığını biliyoruz.” [Katılımcı C»] “Son dönem İngiltere’de seçimlere müdahale olayı ortaya çıktı, Facebook’daki bilgiler kullanılarak...”, “...sosyal mühendislikle hangi partiye oy vereceğinden, inancın, düşüncenin, her şeyi etkileyebiliyorlar.”, “ABD’deki seçimlere Rusya’nın müdahale ettiği söyleniyor.” [Katılımcı H»] “Hiç kimse Facebook’un bir silah olarak kullanılıp seçimleri sallayacağını ve politik amaçlar için Brexit ve Trump konusunda olduğu gibi o ya da bu şekilde kullanılabileceğini düşünmezdi.”
Ürün ve/veya kişi (aday) pazarlama	[Katılımcı C»] “A şahsı şundan hoşlanıyor, bundan hoşlanmıyor, buna ilgisi var vs. Sizin özel yaşama dair bilgilerinizi kullanarak neyi tercih ediyorsunuz, o önünüze geliyor. İlgilendiğiniz bir şeye yönelik ilgili tüm şeyler size sunularak yönlendirilebiliyorsunuz.”
Bilinen, inanılan yargı ve/veya normları yıkarak yeni bir düzen ya da hedef belirleme	[Katılımcı C»] “İnsan unsuruna dikkat edilmesi gerekiyor. Yargı güvenliği açısından, yargıdaki bilginin dışarıya sızması çok önemli konular. İnsan unsurun iyi olması gerekiyor.”, “Bu alanda çok üst seviyede olanlar, bilişime, internete yön verenler, sonuçta gençlere de yön veriyor, onların zihin dünyasını nasıl isterlerse öyle yönlendiriyorlar, şekillendiriyorlar.”, “din kavramı çok ön plana çıkarılarak ‘cemaat çalışmaları’ yapılarak...”, “Cemaat girişimi de bir tür sosyal mühendislik.” [Katılımcı E»] “Facebook ve Google, gerçekte olup biten hikâyeleri anlatan bağımsız haber ve medyayı tedavülden kaldırmaya başlıyor.”, “Geçmişe bakarsanız Facebook’un Filistin’de yapmaya çalıştıklarının ne olduğunu

	<i>görebilirsiniz. Bu yüzden orada neler olup bittiğini ve kukla ustasının ne yaptığını çok iyi anlıyorum.”, “...%1’lik kısım olup bitenleri sosyal mühendislik ile kontrol ediyor.”</i>
Bilgi güvenliğinin yeterince sağlanamaması	
Teknolojik alt yapı eksiklikleri, teknik imkânsızlıklar	<i>[Katılımcı A»] “Altyapı platformlarını gerektiği gibi geliştirebilmek bu açıdan oldukça önemli” [Katılımcı C»] “Olumsuzlukları minimize etmek için çalışmamız lazım, olumlu yönlerinden faydalanabilmek için de altyapıyı geliştirmemiz lazım.” [Katılımcı D»] “Burada da biz hani yeterince Ar-Ge de yapıyor muyuz, belirli bir zaman ayırıyoruz ama Ar-Ge yapmak ayrı bir birim ve birikim gerektiriyor.” [Katılımcı F»] “Benim anladığım kadarıyla dört veya beş servis sağlayıcısı ile veri bütünlüğünü garanti edemediğinden...”</i>
Yeterli bütçenin ayrılması	<i>[Katılımcı C»] “Teknoloji farkı açıldıkça, onu yakalamak için ekonomik olarak onu takip için de bir para ödüyorsun.”, “Teknik mühendis 7-8 bin lira ile çalışmaz. Bu adamlar dışarıda 30 bin lira ile çalışıyor. Neden gelip burada çalışsın. Bunun halledilmesi gerekiyor.” [Katılımcı D»] “Maliyet olarak biraz daha düşürülür, kurumlar teşvik edilirse, kurumlar verilerini yurtdışında tutmak yerine Türkiye’de tutmayı tercih edeceklerdir.”, “İnternet bir maliyet, donanım bir maliyet. Donanım yurt dışından geldiğinden, kaynağında kullanılınca daha az bir maliyet oluşuyor.”, “Kamu-sanayi işbirliğini incelemek ve sermaye de ayırmak gerekiyor bu konuda.”, “Güvenlik cihazları genelde en pahalı cihazlar oluyor.” [Katılımcı J»] “Bu bir kaynak sorunudur.”</i>
Konunun ciddiyetinin yeterince anlaşılması	<i>[Katılımcı I»] “Aslında bilmiyorum. İnsanlar yaptığınız her şeyin dijital bir ayak izi olduğunu fark etmiyorlar. Nüfusun geneli bunu anlamıyor.”, “...bu konuda bir ışık yok.”</i>
Yerli olmayan yazılımların kullanılması	<i>[Katılımcı A»] “...millî teknoloji hamlesini çok önemsiyoruz. Kendi teknolojinizi kendiniz geliştirmede, yerli yazılımlar ihya etmediğinizde sürekli pazar olarak kalmaya mahkûmsunuz.”, “Özellikle ana platform/lar bizde olmalı, üzerine kurulacak olanlar değişebilir, dışarıdan olabilir.”, “Maalesef ‘yerliye’ (yerli ürün, üretim) karşı mesafeliyiz. Bu konuda zafiyetimiz var, bunun giderilmesi gerekiyor.” [Katılımcı C»] “Yazılımların yerli olması bence çok önemli ki şu anda hiçbirinin yerli olduğunu düşünmüyorum.”, “Çok önemli davaların ya da kararların başka yerlerden rahatlıkla ulaşılabilir olduğunu görünce, bunun bir anlamı kalmıyor. Yerli yazılım ve insan unsuru çok önemli.” [Katılımcı D»] “Güvenlik noktasında da bu ürünler desteklenerek yurt dışında da yerli ürünlerin kullanılması sağlanabilir.”</i>
Siber saldırılar ve güvenlik açıkları	<i>[Katılımcı C»] “Teknolojik bilgiye sahip olan ülke, alt düzey teknolojiyi takip eden ülkeyi her an sömürebilir, bilgi açıklarından yararlanabilir.”, “...%100 güvenlik diye bir şey yok. Üst teknolojiye sahip olan ülke, sizin sistemlerinizi ele geçirebilir ya da insan unsurunu kötüye kullanarak ele geçirebilir.”, “Dışarıdan Trojan mailer gönderilerek sisteme zarar verebiliyorlar, bilgiyi değiştirebiliyorlar. Bunlara karşı teknik önlemlerin alınması gerekir.” [Katılımcı D»] “Sistemlere erişim konusunda, yetkisiz kişilerin erişim sağlamaması için, sadece yetkili kişilerin sisteme erişmesi için önlemler alıyoruz. IP kısıtlaması yapılıyor, ilgili kurumdan erişim sağlanabilmesi için yapılıyor bu.”, “Tüm</i>

	vatandaşlara hizmet verdiğimiz için, siber saldırılar ve bu saldırılar ile sistemlerin ele geçirilmesini büyük risk olarak görüyoruz.”, “Kişinin sadece erişebileceği kadar yere erişsin, bilmesi gerektiği kadar bilgiye sahip olsun yönünde bir politikamız var.” [Katılımcı E»] “Yani yaptığımız şey sistemi Bulutun üzerine koymak değil, devreye sokmak. Bu nedenlerle tüm güvenlik duvarlarına ve özellikle de her şeye sahip olması gerekiyor. Güvenlik büyük bir mesele, özellikle de internete bağlı cihazlarda.” [Katılımcı F»] “Geçen sene hangarda ikinci katta sisteme bağlanmış olan bir dizüstü bilgisayar bulduk ve ... birisi ... hangarı boşaltmaya başlamış.” [Katılımcı G»] “Şüphesiz ağı daha fazla genişlettiğinizde daha çok riske sokma ihtimaliniz var.” [Katılımcı H»] “Bilgi güvenliğinin bir risk olduğu... Başka bir cihazın sistemdeki cihazın kimlik numarasını (Mac ID) klonlayabileceği ve bu cihaz gibi davranarak sisteme yanlış veri gönderebileceği şeklinde potansiyel bir zayıflık var.” [Katılımcı J»] “Münih'te bir inovasyon geliştirme merkezinin merkezindeydik ve orada bize ihlalin ne kadar kolay yapılabildiğini gösterdiler.” [Katılımcı J»] “...genel işletim sistemleri makul derecede güvenli ama içeri sızmak isteyen sızacaktır.” [Katılımcı K»] “Her zaman kötü şeyler oluyor. Geçen hafta biri gerçekleşti, ofis 365 portalımız saldırıya uğradı...”
Uluslararası stratejik saldırılar	[Katılımcı A»] “Ulusal veri ve bilgi güvenliği hayati bir konudur.” [Katılımcı C»] “Assange örneğinde olduğu gibi, bir kişi bütün bu şeyleri tek başına yapabildi, birçok şeyi ortaya koyabildi. Wikileaks'de de benzer girişimler söz konusudur.” [Katılımcı D»] “...elektronik seçimlerde de, zamanında Rusya Estonya'ya saldırı düzenlemiş.”, “Bizdeki sistem üzerinden sızmaların olması, ... saldırı sistemin ele geçirilmesi, hizmetin kesintiye uğratılmasıdır. Bunlar bizim açımızdan hem ülkenin itibarını düşürecek bir konu, hem de ...”
Bireysel kullanıcıların bilgi yetersizliği, dikkatsizliği ya da konuyu önemsememesi	[Katılımcı A»] “Bilgi güvenliğini sağlayabilmek için öncelikli olarak beyinlerde dijitalleşme başlamalı ve davranışları değiştirmeliyiz.” [Katılımcı B»] “Bilgi Güvenliğine yönelik olarak gösterilen dirençler aynen Endüstri 4.0'a gösterilen dirençler gibi.”, “Sosyal medya üzerinden kurum içerisinde bulunan ekran görüntü paylaşımları yapılmış. Bu bir bilgi güvenliği riskidir. Bu tür risklerin giderilmesi için kurumsal eğitim ihtiyacı bulunmaktadır.”, “Kurum personeli içerisinde belirli bir “teknoloji okuryazarlık” sorunu bulunmaktadır. [Katılımcı G»] “Güvenlik açısından hepimizin yaptıklarımız konusunda çok uyanık olması hayati önem taşımaktadır.”, “Kabin ekibinden bazılarının uçuşlarda ünlü insanların olduğu, rugby yıldızı ya da her ne ise, onlarla fotoğraf çektirmeleri gibi deneyimler yaşadık.” [Katılımcı I»] “Bilgi güvenliği hakkında çok fazla şey bilmiyorum...”
Endüstri 4.0'a adaptasyon / geçiş zorluğu ve direnç	
Kavramın yeni olması	[Katılımcı C»] “Endüstri 4.0'ın adaptasyonu için insanların zihin dünyasının bu alana dönüştürülmesi lazım bana göre.” [Katılımcı D»] “Estonya'da seçimleri Blockchain ile yaptıklarını söylediler. (...) ...%42 dolayında elektronik olarak seçime katılım sağladıklarını belirttiler. Bir belediye seçimi imiş bu yaptıkları. Türkiye'de bunun uygulanması biraz da kültürel açıdan henüz zor olabilir.” [Katılımcı F»] “Endüstri 4.0 kelimesini sözlü olarak duydum. Gayri resmi toplantılarda bulundum ve bunun hakkında

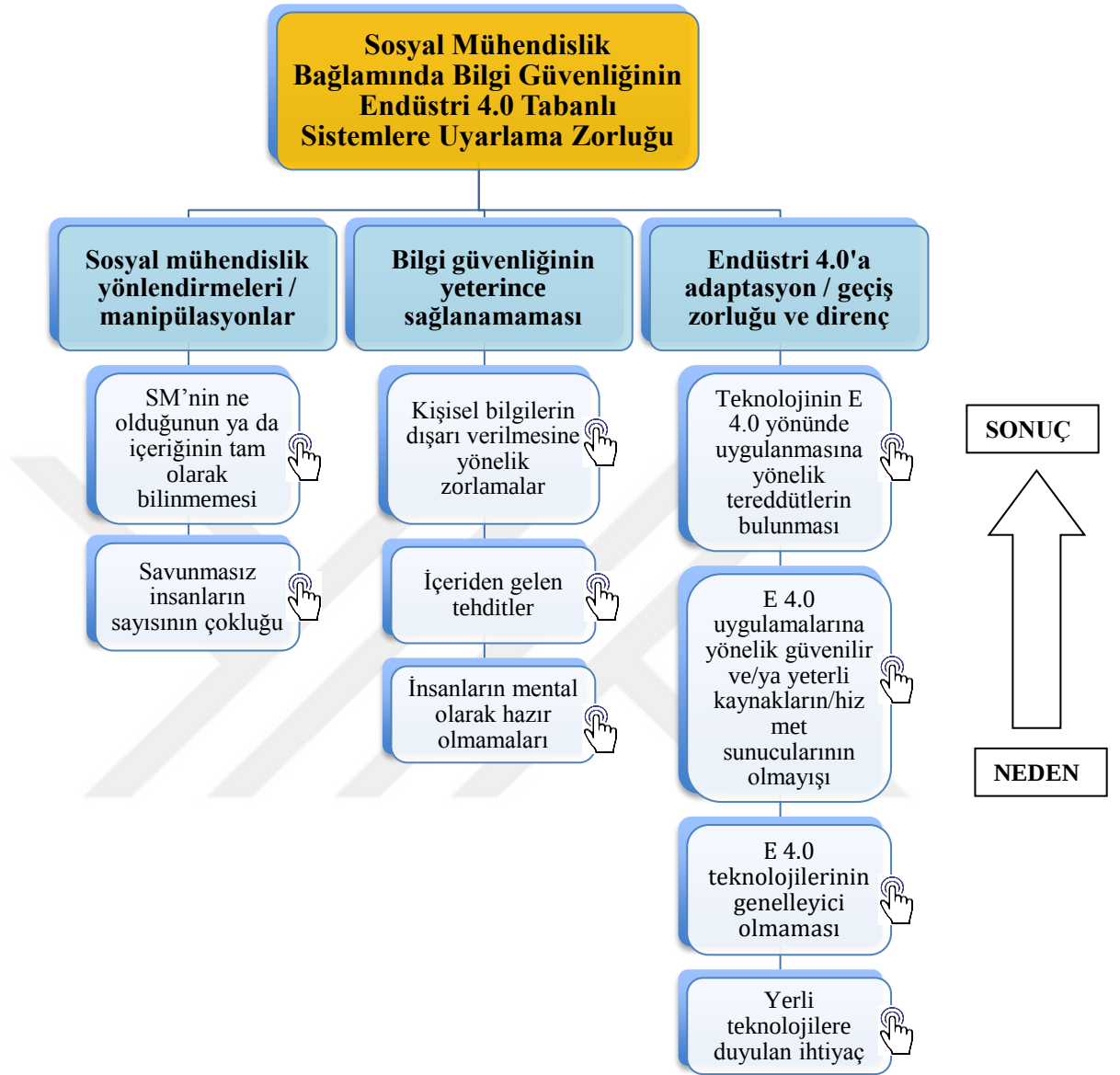
	çok şey duydum. Ama genel olarak bunun PSI uyumluluk ve ödeme kartı endüstrisi ve herkesin bildiği düşünülen PSD2 gibi bir şeyler olduğunu düşünürdük.", "Endüstri 4.0 konusu benim için yeni bir alan..." [Katılımcı I»] "Endüstri 4.0 terimi hakkında çok fazla karışıklık var, bu yüzden birçok farklı şirket bunun ne anlama geldiğini farklı bir şekilde anlıyor." [Katılımcı J»] "Hiç kimse Endüstri 4.0'ı konuşlandıramıyor." [Katılımcı K»] "Yani bunun Endüstri 4.0 diye adlandırıldığını hiç duymamıştım. Bu benim için yeni bir terim..."
Bilgi yetersizliği: tam olarak ne olduğunun ve neleri kapsadığının bilinmemesi	[Katılımcı B»] "Bu direnç göstermenin ana gerekçesi, yeni ve yenilikçi teknolojileri bilmedikleri, kullanamadıkları ve takip edemediklerinden kaynaklanıyor.", "...bilgi eksikliği, bilgi güvenliğinde zafiyet yaratacağı için Endüstri 4.0'ın uygulanması daha zorlaşacaktır. [Katılımcı C»] "Liyakat o kadar önemli ki... IQ'su yeterli olmayan bir insanın çok nitelikli bir yerde görev yapması mümkün mü? Mühendis oluyorsun, ama matematik bilmiyorsun!" [Katılımcı E»] "...insanlara bir çip takılacağından ve herkesin bu şekilde takip edileceğinden konuşuluyordu. Ben, onlara hiç herhangi bir Nesnelerin İnterneti projesinde yer alıp almadıklarını sordum, bu tecrübeli kişilerden oluşan bir oturdumdu güya, söyledikleri şeyin tamamı teorikti ve saçmalıktı." [Katılımcı F»] "Endüstri 4.0'ın tüm iç yüzünü, nasıl uygulandığı ve benzeri konuları çok iyi bildiğimi söyleyemem." [Katılımcı G»] "Endüstri 4.0 konusuna çok aşina değilim..." [Katılımcı I»] "Dürüst olmak gerekirse birçok insanın bunun hakkında çok şey bildiğini düşünmüyorum." [Katılımcı J»] "Yeterli insan kaynakları var ama bu insanların bilgili olmaları gerekiyor."
Ekonomik / teknolojik / insan kaynakları yetersizlikleri	[Katılımcı A»] "Açık kaynak kod platformları için insan kaynağı yetiştirmek lazım", "Commitment (taahhüt) konusunda sorunlar bulunmakta. Yine bu alanda insan kaynağı yeterli değil.", "... Tüm bunların sağlanabilmesi için başta sabır ve insan kaynağı gerekiyor." [Katılımcı C»] "Yetişmiş mühendislerin de yurt dışına gitmesi bizim o alandaki zafiyetimizi arttırıyor.", "İnsan unsuruna, nitelikli insan unsuruna ihtiyaç var." [Katılımcı D»] "...bazı kurumlar var, bunlar vatandaşa çok fazla dokunmuyor. Bazı sistemlerde de vatandaşın direk gitmesi gerekiyor. Bu gibi durumlarda elektronik olarak alt yapılarını yenilemek kurumlar için maliyetli oluyor.", "...Yatırım yapması gerekiyorsa, o yatırım karşılığında çok fazla bir maliyeti gerektiriyor.", "...iş yoğunluğumuz ve farklı şeylerin bir arada işletilmesi biraz zor oluyor, personel olarak.", "Bu alanda kaliteli kişilerin çalışması ve kaliteli ürünler çıkmasında fayda sağlayacaktır." [Katılımcı I»] "...çok büyük bütçelere ihtiyaç var."
Bekle, gör ve uygula politikaları. Zamanın gerisinde kalma	[Katılımcı B»] "Zihniyet değişikliği ve alışılmış davranışlardan vazgeçmek çok zor. Kültürel yapıdan dolayı bu yöndeki değişime direnç var. Yeniliklerden korkuluyor." [Katılımcı C»] "...tutucu davranıyorlar. Zihin dünyası teknolojiyi kaçırmış oluyor. Bunu kaçıranların onu yakalaması çok zor." [Katılımcı E»] "...endüstri onları geçip gidecek ve onlar Kodak gibi olacaklar. Kodak, bu düzeydeki en zengin ve en büyük şirketlerden biriydi. Nokia'nın ve diğer tüm şirketlerin nasıl da akıllı telefon piyasasını ve değişimi göremediklerine bir bakın." [Katılımcı K»] "Teknoloji kararlarımız konusunda ihtiyatlı olmaya çalışırız."

SM, BG ve E 4.0 ana konularından oluşan ve “SM Bağlamında BG’nin E 4.0 Tabanlı Sistemlere Uyarlama Zorluğu Sorun Analizi”nin çözümlemesinde literatür araştırması sonucu elde edilen ve katılımcılar tarafından da desteklendiği tespit edilen bulgulara (Şekil 61) baktığımızda;

- Sosyal mühendislik yönlendirmeleri ve manipölasyonlar için; *bilinen, inanılan yargı ve/ya normları yıkarak yeni bir düzen ya da hedef belirlemenin; ürün ve/ya kişi (aday) pazarlamanın; politik, stratejik ve ekonomik saldırıların; çıkar elde etmenin...*
- Bilgi güvenliğinin yeterince sağlanamaması için; *bireysel kullanıcıların bilgi yetersizliği, dikkatsizliği ya da konuyu önemsememesinin; uluslararası stratejik saldırıların; siber saldırılar ve güvenlik açıklarının; yerli olmayan yazılımların kullanılmasının; konunun ciddiyetinin yeterince anlaşılamamasının; yeterli bütçenin ayrılamamasının; teknolojik alt yapı eksiklikleri ve teknik imkânsızlıkların...*
- Endüstri 4.0’a adaptasyon/geçiş zorluğu ve direnç için; *bekle gör ve uygula politikalarının ve zamanın gerisinde kalmanın; ekonomik/teknolojik/insan kaynakları yetersizliklerinin; bilgi yetersizliğinin (tam olarak ne olduğunun ve neleri kapsadığının bilinmemesi); kavramın yeni olmasının...*

yer aldığı görülmektedir.

Şekil 62. Sorun Analizi-II (Alan Araştırması Sonucunda Eklenenler)



Tablo 15. Literatür Araştırması Sonucunda Oluşturulan Sorun Analizi'nde (Şekil 61) Yer Almayan Fakat Alan Araştırması Sonucunda Sorun Analizine Eklenen Tespitlere (Şekil 62) Yönelik Olarak Katılımcıların Söylemlerinden Elde Edilen Bulgular



Sosyal mühendislik yönlendirmeleri / manipülasyonlar	
SM'nin ne olduğunun ya da içeriğinin tam olarak bilinmemesi	[Katılımcı B»] "Genel olarak, sosyal mühendislik saldırısı gerçekleştirilene değin, insanlar tepkisiz. Ne zaman ki olay olunca, saldırılar gerçekleşince, o vakit insanlar durumu kavrayabiliyorlar.", "Sosyal mühendislik hakkında bilgi eksikliği, bilgi güvenliğinde zafiyet yaratacağı için Endüstri 4.0'ın uygulanması daha zorlaşacaktır." [Katılımcı I»] "...buna Sosyal Mühendislik denildiğini bilmiyordum. Bazı şeylere aşınayım, ... sosyal mühendislik olarak adlandırılmamış olabilirler..."
Savunmasız insanların sayısının çokluğu	[Katılımcı B»] "Yaşlıların sosyal mühendislik saldırılarına daha çok maruz kaldığını biliyoruz." [Katılımcı C»] "Maalesef gençler üzerinde sosyal mühendislikle yapılan yönlendirmeler çok etkili.", "Sosyal medyada uyuşturucu kullanımına yönelik çok girişim var, sosyal mühendislik üzerinden birbirlerini destekliyorlar." [Katılımcı E»] "Özellikle gençleri bu konuda sınırlandırmak gerekiyor. Üç torunum var ve görüyorum ki onlara bitki gibi olacaklarını anlatmakta zorlanıyorum." [Katılımcı J»] "Savunmasız birçok kişi var. İş ortağım ve annesinin banka hesaplarını kolayca boşalttılar, bu çok kolay. Savunmasız bir nüfus var."
Bilgi güvenliğinin yeterince sağlanamaması	
Kişisel bilgilerin dışarı verilmesine yönelik zorlamalar	[Katılımcı I»] "Tipik olarak insanlar öylece bilgi veriyorlar. Bunu kendim de birkaç kez yaptım. Bir oturum açtığınızda bu tür sorulara yönlendirilerek cevaplamaya maruz bırakılabiliyorsunuz."
İçeriden gelen tehditler	[Katılımcı C»] "...insan unsurunu kötüye kullanarak sistemlerinizi ele geçirebilir." [Katılımcı K»] "Bilgi güvenliğinin en büyük alanlarından biri içeriden gelen tehditlerdir. İçeriden gelen tehditler, kritik sistemlere erişimi olan kendi kullanıcılarınızın, istemeden veya bilerek sistemleri kötüye kullanabileceği yerlerdir.", "İnsanlar şirketlerde çok uzun yıllar boyunca çalıştıklarında birçok şeye erişme eğilimindedir. Bu kişiler genellikle en tehlikeli olanlardır çünkü erişime sahiptirler..."
İnsanların mental olarak hazır olmamaları	[Katılımcı A»] "Bilgi güvenliğini sağlayabilmek için öncelikli olarak beyinlerde dijitalleşme başlamalı ve davranışları değiştirmeliyiz.", "Sonuç olarak hiç bir şey bedava değil. Ürünün kendimiz olduğunu bilmeliyiz, verilerimize sahip çıkmalıyız." [Katılımcı B»] "İnsanlar daha çok bilgi edinme ile değil, yaşadıkları ya da çevresinden gördüklerine göre öğrenim gerçekleştiriyor."
Endüstri 4.0'a adaptasyon / geçiş zorluğu ve direnç	
Teknolojinin E 4.0 yönünde uygulanmasına	[Katılımcı B»] "Zihniyet değişikliği ve alışılmış davranışlardan vazgeçmek çok zor. Kültürel yapıdan dolayı bu yöndeki değişime

yönelik tereddütlerin bulunması	<i>direnç var. Yeniliklerden korkuluyor.” [Katılımcı D»] “Yapay zekâ’nın artık insanların yerine geçeceği konuşulmakta, yapay zekâ uygulamalarında artık karar alıcıların makineler olacağı, hani bu noktada yeni çıkan teknolojilere şöyle bakılıyor, acaba bir hata çıkacak mı, çıkarsa herkesi etkileyecek mi, sorumlusu kim olacak gibi düşünceler ortaya çıkıyor.” [Katılımcı E»] “Endüstri 4.0 sanırım bizleri zombi yapacak. Şimdi göreceğiniz tek şey, telefonlarında vakit geçiren insanlar olacak.” [Katılımcı J»] “Endüstri 4.0 teknolojisini uygulamaya isteksiz birçok insan var.”, “Sanırım buna dâhil olmak ve bunu sektör genelinde kullanmak için bir tereddüt var.”</i>
E 4.0 uygulamalarına yönelik güvenilir ve/ya yeterli kaynakların/hizmet sunucularının olmayışı	<i>[Katılımcı J»] “Çok fazlaca alavere dalavere’nin olduğunu söyleyebilirim... dijital dönüşüm ve Endüstri 4.0 üzerinden iş yapmaya çalışan birçok danışman var ve kendileri de uzmanlığa sahip değiller. Yapılması gerekenler etrafında çok fazla bulanıklık var.”</i>
E 4.0 teknolojilerinin genelleyici olmaması	<i>[Katılımcı E»] “Bazen araştırma ve geliştirme için harcanan milyonlarca ve milyarlarca tutardan sonra ortaya çıkan ürünlerin işe yaramadığını görüyoruz, bunlara talep olmayabiliyor.” [Katılımcı H»] “Küçük şirketlerin kaçınılmaz olarak daha büyük şirketlerin geliştirdiği teknolojilere bel bağlaması gerekecek.” [Katılımcı K»] “Teknoloji sağlayıcısı ise teknolojiyi belirli bir durum için tasarlamış olabilir, ancak yine de ne kadar başarılı olacakları kuruluşun bunu konuşturılmasına ve kültürüne bağlıdır. Her teknoloji işe yarayacak diye bir şey yok.”, “...her müşteri kesiminin de farklı bir teknoloji seviyesi ve gereksinimi vardır.”</i>
Yerli teknolojilere duyulan ihtiyaç	<i>[Katılımcı A»] “Milli teknoloji hamlesini çok önemsiyoruz. Kendi teknolojinizi kendiniz geliştirmedeğinizde, yerli yazılımlar ihya etmediğinizde sürekli pazar olarak kalmaya mahkûmsunuz.”, “Özellikle ana platform/lar bizde olmalı, üzerine kurulacak olanlar değişebilir, dışarıdan olabilir.”</i>

4.2.5 Katılımcıların Sosyal Mühendislik, Bilgi Güvenliği ve Endüstri 4.0’ın İlişkilendirilmesine Yönelik Düşüncelerine Ait Bulgular

Tablo 16 ve Tablo 17’de katılımcıların SM, BG ve E 4.0’ın ilişkilendirilmesine yönelik düşüncelerine ait bulgulara yer verilmiştir. 11 Katılımcıdan; SM ile BG’ni ilişkilendirenlerin sayısı 8 (%72.72), SM ile E 4.0’ı ilişkilendirenlerin sayısı 2 (%18.18), BG ile E 4.0’ı ilişkilendirenlerin sayısı 2 (%18.18), SM, BG ve E 4.0’ı ilişkilendirenlerin sayısı ise 4 (%36.36) şeklindedir.

Tablo 16. Katılımcıların Sosyal Mühendislik, Bilgi Güvenliği ve Endüstri 4.0'ın İlişkilendirilmesine Yönelik Düşünceleri – I

	[Katılımcı A»] “Sosyal Mühendislik ile Bilgi Güvenliği arasında sıkı bir ilişki bulunmaktadır.” [Katılımcı B»] “Bilgi güvenliği ve sosyal mühendislik birbirinden ayırt edilemez, çok iç içe girmiş durumdadırlar.” [Katılımcı C»] “Bilgi Güvenliği ve Sosyal Mühendislik de oldukça ilgili alanlar.” [Katılımcı D»] “Bilgi Güvenliği Sosyal Mühendislik ile ilişkili.” [Katılımcı E»] “Özellikle Sosyal Mühendislik ve Bilgi Güvenliği ilişkili.” [Katılımcı G»] “Bilgi Güvenliği ve Sosyal Mühendislik bir bağlantıya sahip.” [Katılımcı H»] “Sosyal Mühendislik, Bilgi Güvenliğiyle alakalı, bilgi güvenliğini geçmek için insanlar sosyal mühendisliği kullanıyorlar.” [Katılımcı I»] “...sosyal mühendislik ve bilgi güvenliği bir ikili oluşturuyor ve insanlar bunun farkında değil.”
	[Katılımcı C»] “Endüstri 4.0 ile Sosyal Mühendislik de bir birlerini tamamlayan kavramlardır. Her teknoloji, her gelişim kendi kültürünü doğuruyor.” [Katılımcı D»] “Yeni teknoloji ile Sosyal Mühendislik bir biriyle ilişkili çalışıyor” [Katılımcı H»] “Endüstri 4.0 ile Sosyal Mühendisliğin ilişkisi olup olmadığından emin değilim.”
	[Katılımcı C»] “Endüstri 4.0 ve Bilgi Güvenliği iç içe girmiş durumdadır.” [Katılımcı H»] “Endüstri 4.0 ve Bilgi Güvenliği arasında kesinlikle güçlü bir ilişkinin var olduğunu düşünüyorum. Sosyal Mühendislikten emin değilim.”
	[Katılımcı D»] “Aslında üç alan da birbiriyle ilişkili. Hepsini birbirini etkiliyor.” [Katılımcı E»] “Sanırım bu üçünün arasında bir geçişkenlik olacak, çünkü önümüzdeki birkaç yıl içinde internet ve sosyal medya ile endüstri arasında robotik ve yapay zekâ da gelecek. Bu oyun değiştirici bir unsur olacak.” [Katılımcı F»] “Endüstri 4.0 konusu benim için yeni bir alan ve son kısımda sormuş olduğunuz bu üç alanın kesişme noktaları ile ilgili ne tür bir çıktı olacağı konusu ilgimi çekiyor.” [Katılımcı G»] “Endüstri 4.0 konusuna çok aşina değilim, bu konu hakkında konuşabilecek kadar anladığımı söyleyemem ama şüphesiz ki onunla da bir bağlantı olduğu kesin.” [Katılımcı I»] “Bu alanlar birbirleriyle bağlantılı... Evet bu üç konu bir biriyle ilişkili” [Katılımcı J»] “Kesinlikle, bu bir trifekta, üç yönlü bir ilişki.”

Tablo 17. Katılımcıların Sosyal Mühendislik, Bilgi Güvenliği ve Endüstri 4.0'ın İlişkilendirilmesine Yönelik Düşünceleri – II

Katılımcı	SM — BG	SM — E 4.0	BG — E 4.0	SM — BG — E 4.0
A	✓			
B	✓			
C	✓	✓	✓	
D	✓	✓		✓
E	✓			✓
F				
G	✓			
H	✓		✓	
I	✓			✓
J				✓
K				
	%72.72	%18.18	%18.18	%36.36

Katılımcılar tarafından aralarında ilişki olduğu düşünülen kavramlar tik (✓) işareti ile gösterilmiştir.

4.2.6 Katılımcıların Endüstri 4.0 Bağlamında Yenilikçi Teknolojilere Yönelik Olumlu ve Olumsuz Görüşlerine Ait Bulgular

Katılımcıların Endüstri 4.0 bağlamında yenilikçi teknolojilere yönelik olumlu ve/ya olumsuz görüşleri incelendiğinde aşağıdaki bulgulara ulaşılmış ve sonuçlar olumlu ve olumsuz sınıflandırmasına tabi tutularak Tablo 18’de sunulmuştur. Olumsuz bölümünde yer alan görüşlerin bir kısmının tamamen olumsuz görüş değil, çekincelerden oluştuğunu, bir kısmının ise katılımcının kendi fikri değil, diğer insanların yaklaşımları ya da davranışları hakkında olduğu gözden kaçırılmamalıdır.

Tablo 18. Katılımcıların Endüstri 4.0 Bağlamında Yenilikçi Teknolojilere Yönelik Olumlu ve Olumsuz Görüşleri

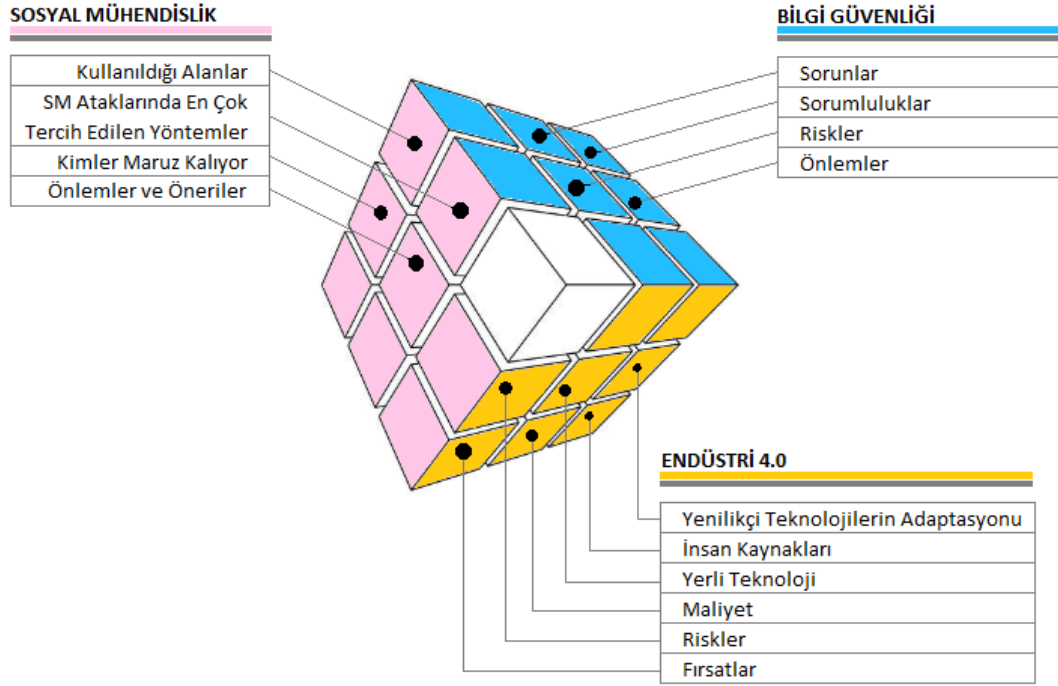
	
[Katılımcı A»] “5G insanlar için olacak, Endüstri 4.0 ise çok önemli bir hale gelecek.” [Katılımcı B»] “Anlık gösterge çok önemli. Endüstri 4.0 bunu yapabilir...”, “Askeri alanda çok belirgin olarak Endüstri 4.0’ın kullanıldığı bir alan yok ama daha çok ‘Dijital Dönüşüm Ofisi’ çalışmaları yapıyor. Bunun gerekliliği iyiden iyiye hissedildi.” [Katılımcı C»] “Bilgisayar olmadan mevcut işlerimizi takip etme imkânımız yok. Bilgisayarı, cep telefonu, iletişimi, interneti hayatımızdan çıkarmamız mümkün değil. Onlar artık olmazsa olmazımız, hayatımızın bir parçası haline gelmişler.” [Katılımcı D»] “Endüstri 4.0 bünyesinde artık insanların müdahil olmadığı, makinelerin kendi kendilerine sistemleri yönetebildiği bir yapı oluşturulmak isteniyor. Bizdeki amaç da buna paralel olarak bilgilerin otomatik olarak sistemlerden çekilip vatandaşın en az müdahaleyle hizmetlere erişebilmesini sağlamak.”, “Bizim platformumuzda şu an 44 milyon vatandaş var bu platformu kullanan ve vatandaşlar bu platforma güveniyorlar. E-devlet kapısından verilen bilgiler bizim için doğrudur, e-devlet kapısından sunulan hizmetler devletin sunduğu hizmetlerdir diye bir güven oluştu.” [Katılımcı F»] “Ne kadar büyük olursa olsun hangi şirket 2 veya 3 gün çevrimdışı kalmayı başarabilir ki!” [Katılımcı H»] “Olumsuz şeyler hakkında epeyce konuştuk ama genel olarak bence Endüstri 4.0 çok olumlu olacak.”, “Tüm bu Nesnelerin İnterneti ve Endüstri 4.0 devrimi ile ilgili ummadığımız bir çok sonuçlar olabilir ama ben hala Facebook örneğinde olduğu gibi avantajların/getirilerin negatifliklere daha ağır bastığını düşünüyorum. Avantaj, milyarlarca kişinin bağlı ve iletişim halinde olmasıdır. Ben işin olumlu tarafındayım.” [Katılımcı I»] “Eğer üreticiysem süreçlerimi optimize eder ve hayatımı kolaylaştırdığından	[Katılımcı A»] “Endüstri 4.0 platformları için insan faktörü ortadan kalkacak olursa sorunların oluşma ihtimali var.”, “Kontrollü dijitalleşmeyi önemsiyoruz ve bunun ne olduğunu ne anlama geldiğini açık olarak bilmek istiyoruz.” [Katılımcı B»] “Zihniyet değişikliği ve alışılmış davranışlardan vazgeçmek çok zor. Kültürel yapıdan dolayı bu yöndeki değişime direnç var. Yeniliklerden korkuluyor.” [Katılımcı C»] “Endüstri 4.0’ın adaptasyonu için insanların zihin dünyasının bu alana dönüştürülmesi lazım bana göre.”, “Özellikle devletin güvenliğini ilgilendiren çok önemli konularda elektronik, yani bilişim alanlarının kullanılmasına şiddetle karşıyım. Çünkü o alana girdiğiniz zaman %100 güvenlik diye bir şey yok. Üst teknolojiye sahip olan ülke, sizin sistemlerinizi ele geçirebilir...”, “Bunları var olma mücadelesi olarak görüyorlar bunları yapanlar. Teknoloji bunun en üst seviyesi. ABD’deki seçimlere Rusya’nın müdahale ettiği söyleniyor.” [Katılımcı E»] “Endüstri 4.0 sanırım bizleri zombi yapacak. Nedenini söyleyeyim: İspanya’da bir kızın geçen gün bir videosunu izledim, telefonuyla konuşurken bir tren sesi duyduğunu sandı. Ancak trenin diğer raylarda olduğunu sandı ve perona doğru yürüdü şanslıydı ki ölmedi.”, “İnsanları yalnızca telefonları başında göreceksiniz, özellikle de çocukları. Tüm bu saçmalıkların etrafında zombiler gibi savrulup duracağız.” [Katılımcı H»] “Sanırım en kötü risk, bir yerlerdeki birinin bu cihazlara yanlış bilgi yüklemenin bir yolunu bulmasıdır, çünkü bu küçük cihazlara koyabileceğiniz sınırlı miktarda koruma imkânı vardır, bu yüzden bu küçük cihazları nasıl güvenilir bir cihaz yapabilirsiniz?” [Katılımcı I»] “Endüstri 4.0 terimi hakkında çok fazla karışıklık var, bu yüzden birçok farklı şirket bunun ne anlama geldiğini farklı bir şekilde anlıyor. Birçoğu şirketin büyüklüğüne

daha fazla para kazanırım...” [Katılımcı J»] “Geçenlerde General Electric’deydik. 755 bileşen 1’e, 200 tedarikçiyi 0’a indirdiler. Etkinlik ve verimlilik harika olacak, iş yükü azalacak ve zamanla gelişecek.”, “Çok fazlaca pozitif tarafındayım. Dediğim gibi 35 yıldır teknolojinin içindeyim. Teknoloji bu günlerde beni kendine hayran bırakıyor ve oldukça şaşırtıyor.” [Katılımcı K»] “... süreçlerimizi her zaman optimize etmenin ve otomatikleştirmenin ve işimizi gerçekten daha verimli hale getirmenin yollarını arıyoruz. Yani bunu yeni teknolojilerle haşır neşir olarak başarabileceksek, her zaman bunun peşindeyizdir.”, “... yapay zekâ sistemine çok fazla veri sağladığımız bir merkez ofis uygulamamız var ve herhangi bir günde belirli bir istasyonda fiyatımızın ne olması gerektiğini tahmin ediyor.”, “... yeni teknolojilerin çoğunu özellikle mağazalarımızda kullanıyoruz ve bundan faydalaniyoruz.”, “Olumlu tarafında olurdum çünkü uzun zamandır teknolojiydim ve birçok çözüm uyguladım. Fayda getirdiğini görebiliyorum.”	göre yönlendiriliyor. KOBİ’lerin kendilerine göre bir perspektifi var, çokuluslu büyük şirketlerinki ise tamamen farklı. Çokuluslu büyük şirketler Endüstri 4.0’a tamamen kendi ortak kelime dağarcıklarından ve tüm farklı sessiz yönlerinden bakıyorlar.”, “Endüstri 4.0 açısından en büyük sorun şirketler için buna yönelik bir yol haritasının nasıl oluşturulacağıdır.”, “Endüstri 4.0 için riskler insanların işini alacak olması” [Katılımcı J»] “Hiç kimse Endüstri 4.0’ı konuşlandıramıyor. Siemens’de müşterilerimiz var. Siemens aslında Endüstri 4.0’ı kullanmaya başladı ve ben de Siemens İrlanda’nın yöneticileriyle çalışıyorum ve onlar da aynı sorunu yaşıyorlar. Endüstri 4.0 teknolojisini uygulamaya isteksiz birçok insan var.”, “... dijital dönüşüm ve Endüstri 4.0 üzerinden iş yapmaya çalışan birçok danışman var ve kendileri de uzmanlığa sahip değiller. Yapılması gerekenler etrafında çok fazla bulanıklık var.” [Katılımcı K»] “Teknoloji sağlayıcısı ise teknolojiyi belirli bir durum için tasarlamış olabilir, ancak yine de ne kadar başarılı olacakları kuruluşun bunu konuşlandırılmasına ve kültürüne bağlıdır. Her teknoloji işe yarayacak diye bir şey yok.”, “Teknolojinin beraberinde sorunlar getirdiğini de biliyorum. En son ve en mükemmeli her zaman en iyisi demek değildir ve şirket kültürünün nerede risk altında olduğuna bağlıdır, çünkü bazı şirketler yeni teknolojileri en önde kullananlardan olmak isterler, bu bağlamda önde olanlardan olma hakkımız yoktur, başka biri bu riski yönetiyor olmalıdır.”

4.2.7 Kodlama, Kategori ve Temalar

Kodlama işlemi için NVivo 10 programı kullanılmıştır. Şekil 63’de kodlama sonucunda oluşturulan kategorilerin ilgili temalar altında dağılımına, Tablo 19’da ise bu kodlamanın referans detaylarına yer verilmiştir. Tablo 20’de kodlamada yer alan kaynak tipleri, kaynak sayıları, referans sayıları, kodlamada kullanılan kelime ve paragraf sayılarına ayrıntılı olarak yer verilmiştir. Kodlamalar; 11 kaynak, 184 referans, 2.440 kelimeden elde edilen bulgulara dayalı olarak yapılmıştır. Şekil 64’de kodlama sonucu elde edilen kategori ve temaların kaynaklarla olan ilişkisi diagram ve sayısal olarak verilmiştir.

Şekil 63. Sosyal Mühendislik, Bilgi Güvenliği ve Endüstri 4.0 Temalarına Ait Kategoriler



Tablo 19. Kodlama ve Kategorilerin Oluşturulması

SOSYAL MÜHENDİSLİK

Toplam: 11 Kaynak, 53 Referans

Kategoriler	Katılımcı
Kullanıldığı Alanlar (5 kaynak, 8 referans)	[A»] “En son ve güncellik açısından herkesin bildiği gibi ABD seçimlerinde sosyal mühendislik yapılarak yönlendirme yapıldığını biliyoruz.” [C»] “Sosyal mühendislikte özellikle insanların yönlendirilmesi o kadar etkili ki... Son dönem İngiltere’de seçimlere müdahale olayı ortaya çıktı, Facebook’daki bilgiler kullanılarak...”, “bilşime, internete yön verenler, sonuçta gençlere de yön veriyor, onların zihin dünyasına da yön veriyorlar.”, “Sosyal medyada uyuşturucu kullanımına yönelik çok girişim var” [E»] “insanların beyinleri yıkıyor.”, “Orta Doğuda da olduğu gibi, %1’lik kısım olup bitenleri sosyal mühendislik ile kontrol ediyor.” [H»] “Sosyal Mühendislik üzerinde pozitif yönde çalışanlar var, örneğin çeşitli mesajlar iletmeye çalışan pazarlamacılar var.” [K»] “Sosyal mühendislik geniş bir alanı kapsar çünkü tüm teknolojiyi içine koyabilirsiniz”
SM Ataklarında En Çok Tercih Edilen Yöntemler (6 kaynak, 11 referans)	[B»] “Başkasının yerine geçerek (kimliğine bürünerek) yapılan sosyal mühendislik saldırıları da oldukça yoğun olarak kullanılmakta.” [D»] “e-devlet kapısına benzer siteler oluşturularak (sahte siteler oluşturularak) vatandaşların kredi kartlarına ulaşma amacıyla çalışmalar yapıyorlar.”, “vatandaşın bilgisini bizim adımızı kullanarak ele geçirmeye çalışıyorlar”, “yurtdışından gelen vatandaşların bilgilerini ele geçirip vatandaşın o telefonlarını kaydetme noktasında çalışıyor bazı kişiler.” [F»] “oldukça fazla ‘ortalama’ faaliyeti var”, “Kredi kartı bilgilerinin ele geçirilmesini hepimiz duyduk.” [H»] “hedef gözetilerek yapılan kimlik avı/ortalama saldırısı bir çeşit sosyal

	mühendisliktir.", "telefonla aranarak şifrelerinin ele geçirilmeye çalışılmasıdır.", "bilgisayarındaki her şey şifrelenmişti, onlara erişemiyordu, fidye yazılımı gibi bir şeydi." [I»] "Her zaman Trojan e-posta alırım." [K»] "İstasyonlarımızdan biri birkaç yıl önce fidye yazılımına maruz kaldı"
Kimler Maruz Kalıyor (5 kaynak, 8 referans)	[B»] "Yaşlıların sosyal mühendislik saldırılarına daha çok maruz kaldığını biliyoruz.", "Maddi kazanç sağlama imkânı varmış gibi çeşitli öneriler sunulur ve insanlar kandırılmaya çalışılıyor.", "Hiyerarşi ve emir silsilesinin olması da yemleme tuzağına düşülmesini kolaylaştırabiliyor." [C»] "Maalesef gençler üzerinde sosyal mühendislikle yapılan yönlendirmeler çok etkili.", "Sosyal medya bunu çocuklara bir trend olarak algılatıp, uygulatabiliyor." [H»] "Londra'dan dönen bir yöneticimizin başına gelenlerdi." [I»] "Tipik olarak insanlar öylece bilgi veriyorlar." [J»] "Savunmasız birçok kişi var."
Önlemler ve Öneriler (10 kaynak, 26 referans)	[B»] "Sosyal mühendisliğe yönelik, kurum içinde, 'yemleme' yöntemi kullanılarak çeşitli sızma testleri yapıyoruz ve bu 'yemleme' yönteminin işe yaradığını görebiliyoruz." [C»] "Özellikle sosyolog, psikolog ve teknik alanlarda bilgilendirme yapılmalı.", "kamuda personel alımına çok dikkat edilmesi gerekiyor.", "Mülakat sınavlarına sınır getirilmesi lazım bana göre." [D»] "Önlemlere yönelik olarak kurumumuzda akademik bir portal oluşturuldu. Bu ortamda eğitimlerimiz yılda bir defa online olarak veriliyor ve verilen eğitime yönelik çeşitli sorular soruluyor.", "Kişinin sadece erişebileceği kadar yere erişsin, bilmesi gerektiği kadar bilgiye sahip olsun yönünde bir politikamız var." [E»] "Kiminle çalışırsak çalışalım gizlilik anlaşması imzalıyoruz.", "Sosyal Mühendislik hakkında bir şeyler söylemek istiyorum. Özellikle gençleri bu konuda sınırlandırmak gerekiyor." [F»] "BT güvenliği, bu tür e-postalar aldığımızda ya da şu adreslerden bir e-posta geldiğinde ekleri açmamamız gerektiğini belirten uyarılar yapar.", " 'Kimlik avı' testimizi hatırlayın. Kimin tıkladığını görmek için kimlik avı testleri yapılıyor." [G»] "sosyal medya kullanımı ve diğer platformlar konusunda çok muhafazakâr bir şirketiz.", "Bir sosyal medya halkla ilişkiler departmanı var, bu yüzden bir sosyal medya başkanı var.", "kuruluşun dışındaki herhangi bir kişiyle sosyal medya üzerinden herhangi bir şey hakkında konuşmamaya dair bir politikamız var.", "Üzerlerinde cep telefonu taşıyamazlar, üniformalı fotoğraf çekemezler.", "Bir öğrenme ve geliştirme departmanımız var.", "Güvenlik eğitimini online olarak yılda bir kez tazelemeniz ve sonunda da bir sınava girerek belirli bir puanı aşmanız gerekiyor." [H»] "Bağlanabilecekleri bir misafir ağı vardır, ancak kurumsal ağa bağlanmazlar.", "hem BT güvenliği hem de fiziksel güvenlik yönünden bir güvenlik eğitimi var." [I»] "e-postalarla ve bunun gibi şeylerle baş etmeye yönelik kılavuzlar var" [J»] "Sosyal mühendislik ile başa çıkmanın en belirgin yolu sağduyu olurdu sanırım.", "farkındalık kampanyası 1 numara olurdu" [K»] "sürekli bir farkındalık eğitimi ve bilginin gözden geçirilmesi, erişimin incelenmesi, erişim kontrolleridir", "sızma testleri yaptık, muhtemelen yıllık olarak", "logları tutuyor ve güncellemeleri de izliyoruz.", "Oldukça güçlü bir eğitim ve farkındalık oturumumuz var ve muhtemelen üç ayda bir, en son tehditler, spam türü e-posta, yaptığımız girişimler, en son haberler ve bu tür şeyler hakkında bir konuşma yapıyorum.", "kimlik avı saldırılarını taklit eden yazılım ürünleri de kullanıyoruz."

SOSYAL MÜHENDİSLİK

Kategoriler	Yorumlar
Kullanıldığı Alanlar	Sosyal mühendisliğin içine tüm teknolojiyi konulabileceğinden her alanı kapsayabileceği ifade edilmekte. Ağırlıklı olarak seçimlerde seçmenlerin yönlendirilmesi, beyinlerin yıkanması, insanların yönlendirilmesinde ve zihin dünyalarına yön verilmesinde, özellikle de gençlere yön vermede kullanıldığının ifade edildiğini görmekteyiz. Sosyal medya üzerinden Orta Doğu'daki olayların yönlendirilmesinden uyuşturucu kullanımına yönelik girişimlere kadar genel bir yelpazeden bahsedilmekte olup bunların yanı sıra sosyal medyayı örneğin pazarlama sektöründe olduğu gibi pozitif yönde kullananların da olduğu belirtilmektedir.
SM Ataklarında En Çok Tercih Edilen Yöntemler	Ağırlıklı olarak "oltalama", "kimlik avı", başkasının kimliğine bürünme ve benzer (ikiz) siteler oluşturmak suretiyle kişilerin şifre, kimlik ve kredi kartı bilgilerine ulaşmaya çalışıldığı, trojan içeren e-postalar ve fidye yazılımlar ile saldırılarda bulunduğu ifade edilmektedir.
Kimler Maruz Kalıyor	İfadelerden, Emir altında olan asker ve subaylar da dâhil olmak üzere SM saldırılarına özellikle çocukların, gençlerin ve yaşlıların maruz kaldığını görmekteyiz. Ayrıca savunmasız birçok insanın varlığından bahsedilmekte. Buradan hareketle SM saldırılarının tüm yaş gruplarını kapsadığını söylemek mümkün.
Önlemler ve Öneriler	"Yemleme", "kimlik avı", "sızma" testlerinin yapılarak ve ayrıca sistemlere erişim kısıtı getirilerek çeşitli önlemlerin alındığını; online eğitimlerin yapıldığını, bilgilendirme portallarının oluşturulduğunu, gizlilik anlaşmalarının yapıldığını ve sosyal medya kullanımında kısıtlayıcı politikaların geliştirildiğini görmekteyiz. Ayrıca, personel alımına ve mülakatlara dikkat edilmesi, insanlara sosyal, psikolojik ve teknik alanlarda destek verilmesi, gençlerin SM kullanımında sınırlandırılması gerektiği ifade edilmekte olup farkındalık eğitimine ise sıkça dikkat çekilmektedir.

BİLGİ GÜVENLİĞİ

Toplam: 11 Kaynak, 60 Referans

Kategoriler	Katılımcı
Sorunlar (4 kaynak, 11 referans)	[B»] "Kurum personeli içerisinde belirli bir 'teknoloji okuryazarlık' sorunu bulunmaktadır." [D»] "Bazı güvenlik programları sistemin performansını ciddi şekilde etkileyebiliyor ve vatandaşın hizmet alma noktasında da aksamalara neden olabiliyor.", "Güvenlik cihazları genelde en pahalı cihazlar oluyor." [H»] "Küçük şirketlerin kendi bilgi güvenliği teknolojileriyle başa çıkmaları çok pahalı, uzmanlığı olan çok fazla insanı işe almak zorundalar, bu yüzden bunu dış kaynak kullanarak yapmaları gerekiyor.", "Evet, karşı karşıya olduğumuz en önemli şey kimlik avı/oltalama (phishing) saldırılarıdır." [I»] "farkındalık eksikliğinin önemli bir sorun olduğunu düşünüyorum.", "Bence insanlar kendileri hakkında çok fazla bilgi veriyorlar...", "başkalarının bilmesini istemediğiniz kişisel bilgilere sahipsem, bununla çok şey yapabilirim.", "İnsanlar yaptığınız her şeyin dijital bir ayak izi olduğunu fark etmiyorlar. Nüfusun geneli bunu anlamıyor.", "gençler bununla büyüdüler, bu yüzden her zaman bilgi veriyorlar.", "Eğer dışarıda isen dışarıda olduğunu hissediyorsun. Bir tür sosyal dışlanma var ve dışarıda olan kişiler bu yüzden kendilerine bir şey olmuş olan insanlar."

• Sorumluluklar (6 kaynak, 12 referans)	[A»] “Veri’nin açıkta dolaşmaması lazım, güvenlik için bu gerekli.”, “Veri’yi elinde tutan, ona sahip olan aynı zamanda veri’nin doğruluğunu da sağlamalı, bu sorumluluğu taşımalı.”, “Tanım ve standartların oluşturulmasında da böyle bir çalışma alt yapısına ihtiyaç bulunmaktadır.”, “Sabır burada bizim için anahtar kelime”, “verilerimize sahip çıkmalıyız.” [D»] “Maliyetlere göre en iyi performansı yakalayacak ürünleri takip ediyoruz.” [E»] “Bilgi güvenliği konusunda çok iyi bir bilgiye sahip olma durumundayız.” [G»] “yüksek bir farkındalığa sahip olmanız gerektiğini düşünüyorum.” [J»] “İnsanların fark etmediği şeylerden biri, inanılmaz miktarda olduğu gibi orada ne kadar veri olduğudur ve bunu anlamak, alçakgönüllü sabır ve bilgi gerektirir” [K»] “varlıklarımızı, bilgi varlıklarımızı korumamız gerekiyor.”, “Her zaman en son gelişmeleri takip ediyoruz”, “umuma açık işler ile uğraşırken risklerin farkında olmanız gerekir.”
• Riskler (7 kaynak, 18 referans)	[A»] “Yazılımlarda backdoor’un (arka kapı) nereye gizlendiğini, nerede olduğunu bulmak ve açığa çıkarmak oldukça zor. ABD sırf bu yüzden Huawei firmasının faaliyetlerini kendi ülkesinde yasakladı.”, “Veri’nin açıkta dolaşmaması lazım, güvenlik için bu gerekli.”, “Sorun ise, scale (ölçek) büyüdüğünde ortaya çıkıyor. Büyük Veri ve veri akışını, o trafiği yönetmek esas beceri.” [B»] “Sosyal medya üzerinden kurum içerisinde bulunan ekran görüntü paylaşımları yapılmış. Bu bir bilgi güvenliği riskidir.” [C»] “devletin güvenliğini ilgilendiren çok önemli konularda elektronik, yani bilişim alanlarının kullanılmasına şiddetle karşıyım.”, “İnsan unsuruna dikkat edilmesi gerekiyor.”, “Dışarıdan Trojan mailler gönderilerek sisteme zarar verebiliyorlar, bilgiyi değiştirebiliyorlar.” [D»] “siber saldırılar ve bu saldırılar ile sistemlerin ele geçirilmesini büyük risk olarak görüyoruz.”, “Yapılacak en büyük saldırı sistemin ele geçirilmesi, hizmetin kesintiye uğratılmasıdır.”, “Fidye saldırıları bizim için önemli risk teşkil eder.” [E»] “En büyük zorluk, birinin sistemi hackleyebilmesidir.” [H»] “bilgi güvenliği konusunun her zaman bir sorun olabileceğini düşünüyorum. Birisinin sisteminize girebileceği noktalar var ve bu yüzden her zaman bu riski taşırsınız.”, “bilgi güvenliğinin devlet aktörleri, hükümetler ve özel şirketler açısından bir sonraki savaş alanı olduğunu düşünüyorum.”, “Demek istediğim, küçük şirketlerin kaçınılmaz olarak daha büyük şirketlerin geliştirdiği teknolojilere bel bağlaması gerekecek.”, “boşluklar ile arka kapıları bulmaya çalışan birileri var.”, “en zayıf halka bağlanabilirliktir. Bulut sistemine bağlanmanız, umuma açık internete bağlanmanız, işte bu zayıf halkadır.” [K»] “zombi saldırısı düzenlemek için istenmeyen (spam) e-postalar gönderdiler”, “Dolandırıcılık vakaları devam ediyor”
• Önlemler (6 kaynak, 19 referans)	[A»] “Bu konularda biraz temkinli davranmak gerekli.”, “başta sabır ve insan kaynağı gerekiyor.” [B»] “risklerin giderilmesi için kurumsal eğitim ihtiyacı bulunmaktadır.”, “Fiziki güvenlik önlemleri var, oldukça da uygun kullanılmakta.”, “Bilgi güvenliği açığına sebebiyet verenler tespit edilirse çeşitli yaptırımlarımız bulunmaktadır.” [C»] “Zorunlu zamanlarda işlerin devamı için manüel sistemin devreye girebilmesi lazım.”, “Bilişim altyapısının da yerli olması bence önemli.” [D»] “bizim siber güvenlik direktörlüğümüz var.”, “güvenlik testleri yapıyoruz”, “Sistemlere erişim konusunda, yetkisiz kişilerin erişim sağlamaması için, sadece yetkili kişilerin sisteme erişmesi için önlemler alıyoruz.”, “sızma testleri yapıyoruz.”, “Elektronik ortamda benim bilgilerim acaba ele mi geçiriliyor diye elektronik ortamdan

	ziyade kağıt üzerinde işlerini yürüten kişiler var.”, “verilerimiz sadece yurt dışına değil, kurum dışına da çıkartılmıyor.” [E»] “tüm güvenlik duvarlarına ve özellikle de her şeye sahip olması gerekiyor.”, “Sahip olduğumuz şifreleme yazılımları NSA ve FBI’ın kullandığı şifreleme sistemlerinin aynısı. SHA 128 şifreleme, bu yüksek seviyeli bir şifreleme.” [G»] “Siber güvenlik için muhtemelen her ay bir şeyler alıyoruz”, “Aylık olarak şifrelerimizi değiştiriyoruz.”, “Bilgisayarlara yeni bir şey yüklenilmesine ya da yeni bir şeyler getirilmesine kesinlikle izin verilmiyor”, “Harici satıcıların veya tedarikçilerin dizüstü bilgisayarlarıyla gelmesi ve yerel ağlarımıza bağlanmaları mümkün değildir.”

BİLGİ GÜVENLİĞİ

Kategoriler	Yorumlar
Sorunlar	Gençlerin teknoloji ile büyüdüklerinden dolayı kendileri hakkında bilgileri çok rahatlıkla dışarıya verebildikleri, sosyal medyada yer alınmaz ise “sosyal dışlanma” ile karşı karşıya kalılabileceği, belirli bir kesimin teknoloji okuryazarlık sorununun olduğu, her şeyin bir dijital ayak izinin bulunduğu ama nüfusun büyük bir kısmının bundan habersiz olduğu ve farkındalık eksikliğinin yüksekliği ifade edilmekte. En çok “kimlik avı” ve “oltalama” saldırılarına maruz kaldığı, küçük işletmelerin teknoloji ve İK açısından yetersiz kaldığı, güvenlik sistemlerinin sistem performansını düşürdüğü bunun yanı sıra güvenlik ekipmanlarının çok pahalı olduğu ifade edilmektedir.
Sorumluluklar	Veri’nin açıkta dolaşmaması, onun sıkı bir şekilde korunması, verinin artık bir “bilgi varlığı” olduğunun farkına varılması gerektiği, veriye sahip olanın onun doğruluğunu da (güvenliğini) sağlaması gerektiği belirtilmektedir. Sabır, bilgi ve yüksek bir farkındalık gerektiği, maliyetlere göre en iyi performansın sağlanması ve umuma açık işlerde daha dikkatli olunması gerektiği ifade edilmektedir.
Riskler	Verilerin açıkta dolaşmaması ve yazılımlarda arka kapı problemine dikkat edilmesi gerektiği, ölçek büyüdüğünde daha büyük sıkıntının ortaya çıktığı, Büyük Veri trafiğini yönetmenin ise esas beceri olduğu, devlet güvenliğini ilgilendiren konularda ise bilişim alt yapısının daha az kullanılması gerektiği belirtilmekte. Trojan e-postaların gönderilmesi, bilginin değiştirilmesi, dolandırıcılık vakaları, hizmetin kesintiye uğratılması, fidye yazılımlar ve siber saldırıların büyük risk oluşturduğu ifade edilirken, bilgi güvenliğinin yeni savaş alanı olduğuna dikkat çekilmektedir.
Önlemler	BG konusunda dikkatli davranmayanlara disiplin cezası yaptırımlarının uygulandığı, yerel ağlara misafirlerin bağlanmasının engellendiği, bilgisayarlara harici bellek takılmasının yasaklandığı, şifrelerin aylık olarak güncellendiği, güvenlik ve sızma testlerinin yapıldığı belirtilirken, bunlara ek olarak kriz zamanlarında işlerin manüel şekilde yürütülebilmesi için hazır olunması gerektiği ve ayrıca kurumsal eğitimin yanı sıra sabırlı ve temkinli davranmak gerektiği ifade edilmektedir.

ENDÜSTRİ 4.0

Toplam: 11 Kaynak, 71 Referans

Kategoriler	Katılımcı
Yenilikçi Teknolojilerin Adaptasyonu (9 kaynak, 17 referans)	[A»] "Kontrollü dijitalleşmeyi önemsiyoruz ve bunun ne olduğunu ne anlama geldiğini açık olarak bilmek istiyoruz." [B»] "Zihniyet değişikliği ve alışılmış davranışlardan vazgeçmek çok zor. Kültürel yapıdan dolayı bu yöndeki değişime direnç var. Yeniliklerden korkuluyor.", "direnç göstermenin ana gerekçesi, yeni ve yenilikçi teknolojileri bilmedikleri, kullanamadıkları ve takip edemediklerinden kaynaklanıyor.", "Askeri alanda çok belirgin olarak Endüstri 4.0'ın kullanıldığı bir alan yok ama daha çok 'Dijital Dönüşüm Ofisi' çalışmaları yapılıyor. Bunun gerekliliği iyiden iyiye hissedildi." [C»] "Endüstri 4.0'ın adaptasyonu için insanların zihin dünyasının bu alana dönüştürülmesi lazım" [D»] "Yeni çıkan teknolojiler için, aslında akademik toplantılara katılıyoruz, yapay zekâ, derin öğrenme, çoğu üniversite bu konuda bilinçlenmiş" [E»] "Bunun için çok fazla YouTube izliyorum, LinkedIn'e bakıyorum ve ana tedarikçilerimizle konuşuyorum ve her zaman üst düzey/kaliteli eğitimlerimizi yapıyoruz.", "her zaman teknolojinin olduğu yerin bir adım ötesinde durmaya çalışıyor ve bu tür şeyleri şirket olarak uygulamak için neler yapabileceğimize bakıyorum." [H»] "sahip olduğumuz müşteriler aracılığıyla güncellenmek bu alanda kendimizi güncellemenin yollarından bir tanesini oluşturuyor.", "kişilerden edinebileceğim belgeler, çalışmalar ve tezler var ve katılabileceğim konferanslar bulunmakta. Diğer yol ise internet üzerinden, web üzerinden." [I»] "Endüstri 4.0 terimi hakkında çok fazla karışıklık var, bu yüzden birçok farklı şirket bunun ne anlama geldiğini farklı bir şekilde anlıyor.", "Küçük işletmeler için daha zor olduğunu düşünüyorum." [J»] "Hiç kimse Endüstri 4.0'ı konuşlandıramıyor. Siemens'de müşterilerimiz var. Siemens aslında Endüstri 4.0'ı kullanmaya başladı ve ben de Siemens İrlanda'nın yöneticileriyle çalışıyorum ve onlar da aynı sorunu yaşıyorlar.", "Sanırım buna dâhil olmak ve bunu sektör genelinde kullanmak için bir tereddüt var.", "Evet, dünyada yenilikçi şirketler var, ama büyük çoğunluğu öyle değil." [K»] "Hepsi işe yaramıyor ve hepsi bizim düşündüğümüz gibi çalışmıyor. Farklı beklentilerimiz ve gereksinimlerimiz olabiliyor. Teknoloji sağlayıcısı ise teknolojiyi belirli bir durum için tasarlamış olabilir, ancak yine de ne kadar başarılı olacakları kuruluşun bunu konuşlandırılmasına ve kültürüne bağlıdır. Her teknoloji işe yarayacak diye bir şey yok."
İnsan Kaynakları (8 kaynak, 12 referans)	[A»] "insan kaynağı yeterli değil." [B»] "Diğer taraftan bu eksikliklerin giderilmesine ve direncin kırılmasına yönelik olarak verilen hizmet içi eğitimlerin yetersiz olmasını da göz ardı edemeyiz." [C»] "Yetişmiş mühendislerin de yurt dışına gitmesi bizim o alandaki zafiyetimizi arttırıyor.", "İnsan unsuruna, nitelikli insan unsuruna ihtiyaç var." [D»] "Ar-Ge yapmak ayrı bir birim ve birikim gerektiriyor." [E»] "İnsan kaynakları konusunda mümkün olduğunca taşeron kullanıyoruz." [G»] "neyin gerekli olduğunu ve neye izin verdiğimizizi, neye izin vermediğimizi belirleme konusunda eğitim alıyoruz. Nelerin düzenli olarak yapılacağını, nelerin söylenip söylenmeyeceğini düzenli olarak bildiriyoruz. Değişiklik ve güncelleme konularında bilgilendiriliyoruz. Yapılan değişiklikler ve yenilikler konusunda düzenli olarak yapılan bir eğitim prosedürümüz var.", "Farklı departmanlarda işini çok iyi yapan insanlar var ve onlar bizleri değişiklikler hakkında oldukça iyi bir şekilde bilgilendiriyorlar." [I»] "Dürüst olmak gerekirse birçok insanın bunun hakkında çok şey bildiğini düşünmüyorum. Özellikleri hakkında büyük

	bir farkındalık olduğunu düşünmüyorum.”, “Eminim bunun farkında bile olmayan çok sayıda KOBİ vardır.” [J»] “Endüstri 4.0 üzerinden iş yapmaya çalışan birçok danışman var ve kendileri de uzmanlığa sahip değiller.”, “Yeterli insan kaynakları var ama bu insanların bilgili olmaları gerekiyor. Eğitilmeleri gerekiyor ama insanlar insana yatırım yapma konusunda isteksizler.”
Yerli Teknoloji (2 kaynak, 2 referans)	[A»] “Diğer alanlarda olduğu gibi Endüstri 4.0 yapılanmalarında da milli teknoloji hamlesini çok önemsiyoruz. Kendi teknolojinizi kendiniz geliştirmediginizde, yerli yazılımlar ihya etmediğinizde sürekli pazar olarak kalmaya mahkûmsunuz.” [D»] “Biz verilerin dışarıya çıkmasına çok sıcak bakmıyoruz.”
Maliyet (4 kaynak, 8 referans)	[C»] “Teknoloji farkı açıldıkça, onu yakalamak için ekonomik olarak onu takip için de bir para ödüyorsun.” [D»] “Fayda/maliyet gözetiyorlar. Yatırım yapması gerekiyorsa, o yatırım karşılığında çok fazla bir maliyeti gerektiriyor. Bu gibi durumlarda da o kurumlar eski süreçlerine devam ediyor”, “Kurumlar belki fiyat yüksek mi geliyor bilmiyorum ama verilerini yurt dışında tutan kurumların olduğunu ben de biliyorum.”, “İnternet bir maliyet, donanım bir maliyet. Donanım yurt dışından geldiğinden, kaynağında kullanılınca daha az bir maliyet oluşuyor. Sunucuların soğutulması bir maliyet kalemi...”, “büyük şirketler buna büyük maliyetler, personeller ayırabiliyor, bu da şirketin büyüklüğüyle ve yatırımıyla alakalı.” [H»] “Bağlantı ve ölçek ekonomisi sebepleriyle verilerinizi yeniden ve yeniden bulut’a gönderirsiniz. Koskocaman sistemlerin verimli bir şekilde çalışabilmesi ve insanların bu kaynakları paylaşabilmeleri için bu gereklidir.” [I»] “çok büyük bütçelere ihtiyaç var.”, “En gelişmiş sistemler için pahalı olabilir ama yol boyunca belirli adımlar atmak için oldukça ucuz olabilir ve çok sayıda fayda elde edebilirsiniz. Bilirsiniz, neye baktığınıza bağlı olarak değişir bu.”
Riskler (8 kaynak, 19 referans)	[A»] “Endüstri 4.0 platformları için insan faktörü ortadan kalkacak olursa sorunların oluşma ihtimali var.” [C»] “Endüstri 4.0 ile ilgili yaşanabilecek riskler açısından düşünecek olursak güvenlik riski her zaman vardır.” [D»] “Yapay zekâ’nın artık insanların yerine geçeceği konuşulmakta, yapay zekâ uygulamalarında artık karar alıcıların makineler olacağı, hani bu noktada yeni çıkan teknolojilere şöyle bakılıyor, acaba bir hata çıkacak mı, çıkarsa herkesi etkileyecek mi, sorumlusu kim olacak gibi düşünceler ortaya çıkıyor.”, “Risk olarak ise, bu süreçte ortaya çıkan istisnaları yönetmek gerekiyor.” [E»] “Bazen araştırma ve geliştirme için harcanan milyonlarca ve milyarlarca tutardan sonra ortaya çıkan ürünlerin işe yaramadığını görüyoruz, bunlara talep olmayabiliyor. Yani en iyi ürüne sahip olabilirsiniz, ancak pazarlamak için bir rotanızın olması gerekir.”, “Nokia’nın ve diğer tüm şirketlerin nasıl da akıllı telefon piyasasını ve değişimi göremediklerine bir bakın. Kodak ve Nokia’ya, iki klasik örneğe bakarsanız, baskı ve dijital teknolojinin gittiği yerleri doğru bir şekilde göremediler.”, “insanlar ileriye yönelik tam olarak neler olduğunu görmek için büyük resme, eğilimlere, aynı zamanda fırsatlara da bakmıyorlarsa...” [H»] “Bulut’un evinizde geleneksel bir veri merkezine sahip olmanızın getireceği riskten daha fazlasına sahip olduğunu düşünmüyorum.”, “Etrafa yerleştirilmiş birçok sensörlerden oluşan bir Nesnelerin İnterneti sisteminiz varsa, sensörler doğası gereği çok küçüktürler ve üzerlerindeki işlem ve hafıza açısından oldukça sınırlı kaynaklara sahiptirler ve bu yüzden onlar üzerindeki şifreleme yetisi onları yerleştirdiğiniz cihazları da sınırlar.”, “Başka bir cihazın sistemdeki cihazın kimlik numarasını (Mac ID) klonlayabileceği ve bu cihaz gibi davranarak sisteme yanlış

	veri gönderebileceği şeklinde potansiyel bir zayıflık var.” [I»] “Endüstri 4.0 ile ilgili fırsat, halihazırda var olan verileri kullanma bağlamında farklı süreçleri nasıl deneyebileceğimiz ve optimize edebileceğimizdir. Riskler elbette bir maliyete sahip.”, “Büyük şirketler için bu yolu uygun görüyorlar, planda bu var ama KOBİ’ler bu noktaya nasıl ulaşacaklar?”, “Diğer bir risk, akıllı imalat sanayi 4.0’da yer alan robotlarının işimizi alacağını düşünce perspektifinden algılanmasıdır.”, “Endüstrisi 4.0 için olsun ya da olmasın bulut bilişimi ile ilgili bir sorun var. Bulut bilişim ile ilgili sorun, eğer herkese açık bir bulutsa, tüm verilerinizin bulut üzerinden başka bir yere gidiyor. Bu zaten kesinlikle şüpheli bir durum yaratıyor ve bir risk getiriyor.”, “Endüstri 4.0 açısından en büyük sorun şirketler için buna yönelik bir yol haritasının nasıl oluşturulacağıdır.” [J»] “Hiç kimse Endüstri 4.0’ı konuşlandıramıyor. Siemens’de müşterilerimiz var. Siemens aslında Endüstri 4.0’ı kullanmaya başladı ve ben de Siemens İrlanda’nın yöneticileriyle çalışıyorum ve onlar da aynı sorunu yaşıyorlar. Endüstri 4.0 teknolojisini uygulamaya isteksiz birçok insan var.”, “Verilere ve verilerin toplanmasını ve harmanlanmasını kapsayan yöntemlere ve sensörlere daha fazla bağımlı hale gelmenizdir. Güvenlik ihlalinin herhangi bir kuruluş için felaket olabileceği riski vardır.”, “Yapılması gerekenler etrafında çok fazla bulanıklık var.” [K»] “her teknoloji her bir şirket için geçerli değildir.”
• Fırsatlar (7 kaynak, 13 referans)	[B»] “Endüstri 4.0 sayesinde üretimin her aşaması takip edilebilir. Endüstri 4.0 bağlamında makineler, insan gücünü en aza indirerek sorunsuz üretim yapılmasını sağlayabilir.”, “Anlık gösterge çok önemli. Endüstri 4.0 bunu yapabilir...” [C»] “Zaman yönünden, insan unsuru yönünden, onlarca kişinin yaptığı işi yapabiliyor teknoloji.” [D»] “Normalde bir gün süren bir işlem şimdi beş dakikada bitiyor...”, “Süreçlerin kısaltılması, hatanın azaltılması, insan faktörünün daha da minimize edilmesi...” [H»] “Dünya o kadar bağlantılı hale geldi ki, şu anda gittiğiniz her yerde bağlantıya sahip olacaksınız, yani herhangi bir üretim tesisiniz veya fabrikaınıza sensörler ile bağlanabileceksiniz.” [I»] “Eğer üreticiysem süreçlerimi optimize eder ve hayatımı kolaylaştırdığından daha fazla para kazanırım” [J»] “Tasarruflar çok muazzam olacak.”, “uçak motorlarının basıldıkları General Electric’deydik. 755 bileşen 1’e, 200 tedarikçiyi 0’a indirdiler. Etkinlik ve verimlilik harika olacak, iş yükü azalacak ve zamanla gelişecek.”, “İnovasyon durgunluk ve aşağı yönlü ekonomiler tarafından yönlendirilir; bu, insanların yeni çözümler aramaya başlamasını sağlar...” [K»] “süreçlerimizi her zaman optimize etmenin ve otomatikleştirmenin ve işimizi gerçekten daha verimli hale getirmenin yollarını arıyoruz. Yani bunu yeni teknolojilerle haşır neşir olarak başarabileceksek, her zaman bunun peşindeyizdir.”, “Coğrafi veriler açısından Büyük Veriyi kullanıyoruz; merkezlerimizin nerede olması gerektiği, nüfusun nerede kalabalık olduğu, eğilimin ne yönde olduğu vb. şeyler. Bu bizi yönlendiriyor.”, “Bulut tabanlı bir iş zekâsı (BI) aracı kullanıyoruz ve dâhili olarak çok fazla veri topluyoruz ve bunu grafiksel olarak güzel bir şekilde, güzel bir iş zekâsı (BI) olarak sunuyoruz. Ancak bu veriler, iş hakkında bildiğimizi düşündüğümüz aslında bilmediğimiz şeylere yönelik birçok sürpriz getirdi.”

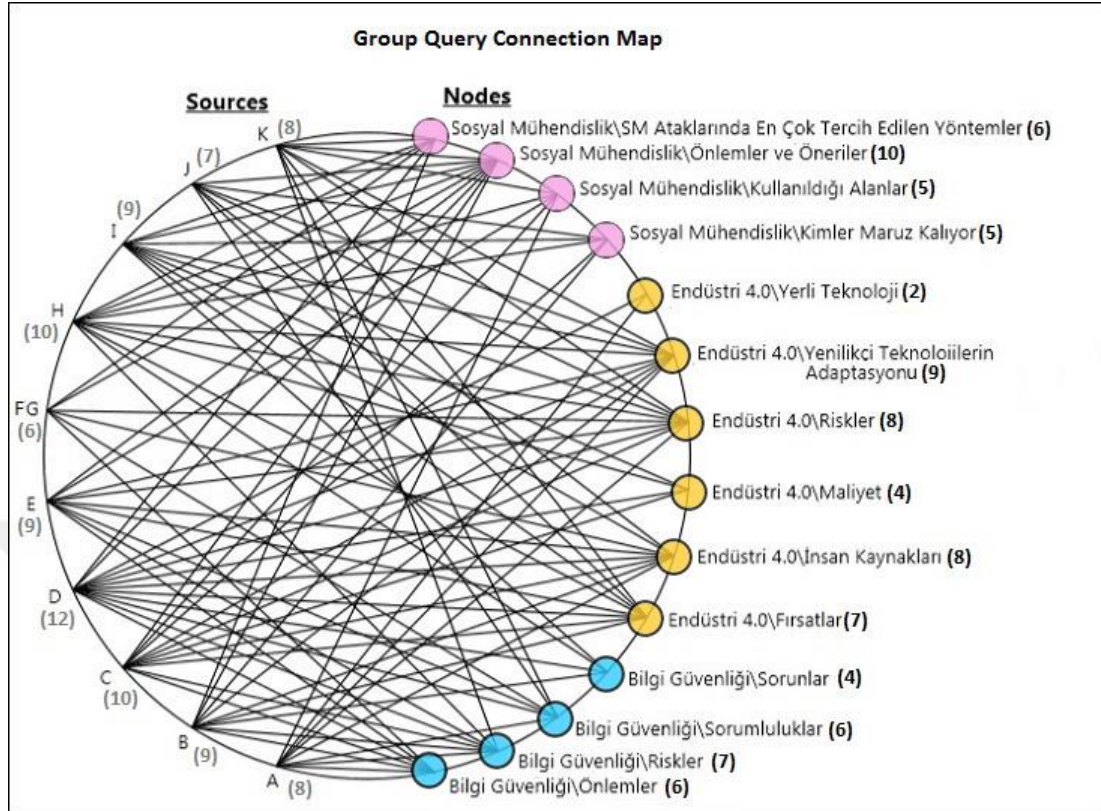
ENDÜSTRİ 4.0

Kategoriler	Yorumlar
Yenilikçi Teknolojilerin Adaptasyonu	Yenilikçi teknolojilerin takibi için internet, YouTube, LinkedIn gibi kanalların tercih edildiği, müşterilerle, tedarikçilerle konuşulduğu, konferanslara katılımların olduğu ve belirli aralıklarla eğitimlerin alındığı ifade edilmekte. Endüstri 4.0 hakkında bir karışıklığın var olduğu, tam olarak konuşlandırılmadığı ve çeşitli çekince ve tereddütlerin olduğu, her teknolojinin işe yaramayabileceği, kontrollü bir değişimden yana olduğu dile getiriliyor. Küçük işletmeler için işin daha da zor olduğu belirtiliyor. Zihniyet değişikliğinin ve alışılmış davranışlardan vazgeçmenin zor olduğu, zihin dünyasının bu alan dönüştürülmesi gerektiği, karşı çıkanlara yönelik gerekçelerin ise yeni teknolojileri bilmedikleri, takip edemedikleri veya kullanamadıkları gerekçeleriyle açıklanmaktadır.
İnsan Kaynakları	Genel olarak insan kaynağının yeterli olmadığı yönünde görüş belirtilmekte olup, esas olanın insan kaynağının niteliğinin artırılması gerektiği, hizmet içi eğitimlerin çok da yeterli olmadığı ifade edilmekte. Endüstri 4.0 hakkında yeterli farkındalığın olmadığı, hatta konunun danışmanlarının bile belirli bir uzmanlığa sahip olmadıkları dile getirilmektedir.
Yerli Teknoloji	Verilerin korunmasının yanı sıra yerli yazılımlara sahip olmanın dış pazarlara olan bağımlılığı azaltacağı ifade edilmektedir.
Maliyet	Teknolojiye yatırımın belirli bir maliyet tuttuğu, fayda/maliyet oranının gözetildiği, küçük ölçekli işletmelerin eski süreçlerini korudukları, ölçek ekonomisi sebepleriyle verilerin daha ziyade bulut üzerinde tutulmasının tercih edildiği, teknolojiye yatırımın pahalı olduğu fakat yol boyunca belirli kazanımları da getireceği ifade edilmektedir.
Riskler	İnsan faktörü ortadan kalktığında buna ilişkin sorunların (ör: sorumlunun kim olacağı vb.) oluşabileceği, akıllı robotların insanların işini elinden alabileceği, güvenlik riskinin her zaman var olduğu, mühim olanın ise ortaya çıkan istisnaların yönetilebilmesi gerektiği ifade edilmekte. Milyarlarca tutar yatırım yapmakla her zaman iyi şeyler çıkmayabileceği belirtilirken, bunun yanı sıra ürün için pazar'ın önemine dikkat çekilmekte. E 4.0 için çalışan sensör ve gömülü sistemlerin yeterli güvenlik (özellikle şifreleme açısından) içeremediği, buna rağmen bu uygulamalara bağımlı hale geldiği, bulut sisteminin veri güvenliği açısından şüpheli olduğu düşünülürken, E 4.0'ın tam olarak konuşlandırılmadığı ve şirketlerin mevcut bir yol haritasının olmadığı, genel bir bulanıklığın var olduğu ifade edilmektedir.
Fırsatlar	E 4.0 sayesinde üretim, lojistik, pazarlama vb. her aşamasının anlık olarak takip edilebileceği, insan faktörü minimize edileceği için hatasız süreçlere ulaşılabilceği, süreçlerin optimize edilebileceği, iş yükünün azalacağı, bunun yanı sıra zaman kazanımının paha biçilemez olduğu, mekandan bağımsız olarak daima bağlantıda kalınabileceği, Büyük Verinin kullanımı sayesinde de yeni iş zekasının (business intelligence) ortaya çıkacağı ifade edilmektedir.

Tablo 20. D ğ m  zeti Raporu (Node Summary Report) (NVivo 10 Uygulaması)

Node Summary / D�ğ�m �zeti					
Source Type		Number of Sources	Number of Coding References	Number of Words Coded	Number of Paragraphs Coded
Kaynak Tipi		Kaynak Sayısı	Kodlama Referans Sayısı	Kodlanan Kelime Sayısı	Kodlanan Paragraf Sayısı
Node					
Nodes\\Bilgi G�venliđi\\�nlemler					
Document		6	19	177	19
Nodes\\Bilgi G�venliđi\\Riskler					
Document		7	18	214	18
Nodes\\Bilgi G�venliđi\\Sorumluluklar					
Document		6	12	113	12
Nodes\\Bilgi G�venliđi\\Sorunlar					
Document		4	11	142	11
Nodes\\End�stri 4.0\\Fırsatlar					
Document		7	13	283	14
Nodes\\End�stri 4.0\\İnsan Kaynakları					
Document		8	12	177	12
Nodes\\End�stri 4.0\\Maliyet					
Document		4	8	150	8
Nodes\\End�stri 4.0\\Riskler					
Document		8	19	421	23
Nodes\\End�stri 4.0\\Yenilik�i Teknolojilerin Adaptasyonu					
Document		9	17	292	22
Nodes\\End�stri 4.0\\Yerli Teknoloji					
Document		2	2	33	2
Nodes\\Sosyal M�hendislik\\Kimler Maruz Kalıyor					
Document		5	8	65	8
Nodes\\Sosyal M�hendislik\\Kullanıldıđı Alanlar					
Document		5	8	101	8
Nodes\\Sosyal M�hendislik\\�nlemler					
Document		10	26	318	26
Nodes\\Sosyal M�hendislik\\SM Ataklarında En �ok Tercih Edilen Y�ntemler					
Document		6	11	104	11
			184	2440	

Şekil 64. Kodlama Sonucu Elde Edilen Kavramların Kaynaklarla Olan İlişkisi



Şekil 64’de NVivo 10 programı ile gerçekleştirilen *kodlama* sonucunda elde edilen diagram yer almaktadır. Bu diagramda kaynakların (katılımcı) tema ve kategorilere olan atıf sayıları ve ayrıca her bir kategorinin ilişkili olduğu kaynak sayıları parantez içerisinde belirtilmiştir.

4.2.8 Kodlama Kelime Frekans Dağılımları

Şekil 65’de on bir (11) farklı kaynaktan kodlama yapılırken kategorilerin oluşturulmasında kullanılan görüşme metinlerinden elde edilen ve “nodes”lara ait olmak üzere en az dört (4) harften oluşan ve frekansı en yüksek yüz (100) kelimeye ait kelime sıklığı sorgusu (word frequency query) sonucunda elde edilen görsele yer verilmiştir. Şekil 66’da ise NVivo 10 programında bu sorgulamanın nasıl yapıldığını gösteren sorgulama ekranı ve kullanılan parametrelerin yer aldığı ekran görüntüsüne yer verilmiştir.

4.3 Yorum

Bu başlık altında, araştırmaya ait bulgulara yönelik değerlendirme ve yorumlara yer verilmiştir. Değerlendirme ve yorumlar, araştırmada elde edilen bulgulara dayalı olarak yapılmıştır. İki kısımdan oluşan değerlendirme ve yorumların birinci kısmında, kategorize edilmiş olan bulgulara yönelik değerlendirme ve yorumlar yer alırken, ikinci kısımda genel değerlendirme ve yorumlara yer verilmiştir.

I. Kısım

Literatür Araştırması Sonucunda Elde Edilen SM, BG ve E 4.0'ın Kesişme Alanlarına Ait Bileşenlerin Katılımcılara Göre Önem Sıralaması (4.2.2)'na Yönelik Değerlendirme ve Yorumlar

Tablo 12 incelendiğinde katılımcıların birincil düzeyde “İnsan Faktörü” bileşenini önemsedikleri, bunun yanı sıra güvenliğe yönelik (“Ulusal Güvenlik”, “Siber Güvenlik”, “Veri ve Bilgi Güvenliği”) bileşenlerin büyük oranda önemsendiğini görmekteyiz. Blokzincir alt yapısında kullanılan ve yeni yeni duymaya başladığımız “Dağıtık ve Merkezi Olmayan Yapı” bileşeninin yeni bir kavram olması yanı sıra, teknik içerikli olmasından dolayı da daha az önemsenmiş olabileceğini düşünmekteyiz. Katılımcıların çoğunluğunun yönetici pozisyonunda olmalarına rağmen “Risk Yönetimi” bileşeninin sonlara doğru tercih edilmesi düşündürücüdür. Bunun sebebinin “risk yönetiminin” bir güvenlik parametresi gibi algılanmamış olabileceğinden kaynaklandığını düşünebiliriz.

Katılımcılar Tarafından Önerilen Bileşenler (4.2.3)'e Yönelik Değerlendirme ve Yorumlar

Katılımcılar tarafından önerilen ve Tablo 13’de gösterilen bileşenleri (“Etik”, “Digital Persona: Kimlik Doğrulama Platformu”, “İnsan Unsurunun Seçimi”, “Liyakat”, “Terörizm”, “Eğitim”, “İnsana Yatırım”, “Gerçek İş Deneyimi”) dikkatlice inceleyecek olursak, en önemli faktörün literatür çalışmasında elde edilen ve alan çalışmasında önem sıralaması yapılan bileşenlere paralellik gösterdiği ve burada da insan unsurunun ön plana çıkarıldığını görmekteyiz. Bunu iki açıdan

değerlendirmek mümkündür: Birincisi, teknoloji ne kadar gelişmiş olursa olsun, katılımcılar tarafından insan faktörünün daima işin içinde yer alacağını düşünülmesi/beklentisi; İkincisi, gün geçtikçe gelişme kaydeden makineleşme, otomasyon ve robotik'in bilinç altında, çalışanların yerini alacağı endişesinin yatması. Katılımcıların, özellikle kriz ve risk yönetimlerinde işlemlerin manuel olarak yerine getirilmesinde insana ihtiyaç duyulacağını belirtilmeleri dikkate değer diğer bir ayrıntı olarak karşımıza çıkmaktadır.

Sorun Analizinde Yer Alan Bulgular (4.2.4)'a Yönelik Değerlendirme ve Yorumlar

SM, BG ve E 4.0 ana konularından oluşan ve “SM Bağlamında BG'nin E 4.0 Tabanlı Sistemlere Uyarlama Zorluğu Sorun Analizi”nin çözümlemesinde literatür araştırması sonucu elde edilen ve katılımcılar tarafından da desteklendiği tespit edilen bulgulara (Şekil 61) baktığımızda; SM, BG ve E 4.0 alanlarına yönelik bu bulgular yan yana getirildiğinde; kavram belirsizliğinin var olduğu, süreçleri yönetmek üzere yeterli insan kaynağının olmadığı, ekonomik ve mali yetersizliklerin önemli olduğu, politik/ekonomik/çıkar saldırılarının olduğu ve yeterli referans (doğrulayıcı) kaynakların olmaması sebebiyle biraz çekimser ve kuşkulu yaklaşımların var olduğunu söylemek mümkün gözüküyor. Bu tespitleri yeni ve yenilikçi teknolojilerin Endüstri 4.0 etrafında şekillenmesinde yeterli bir zorluk oluşturulduğunun belirtileri olarak kabul edecek olursak, sorunların nasıl aşılabacağına yönelik kişi ve kurumların önüne uygun yol haritalarının konularak, tereddütlerin ortadan henüz kaldırılamadığını söylemek mümkündür. İnsanların, özellikle genç nüfusun yeni ve yenilikçi teknolojilere olumlu (biraz da riskleri göz ardı ederek) yaklaşımlarının göz ardı edilmemesi gerektiği ama bu paralelde çözüm yollarının uygulayıcılar tarafından daha belirgin bir şekilde ortaya konularak, güvenlik risklerinin ortadan kaldırılması ve standartların geliştirilmesinin genel politikalar olarak birinci sırada ele alınmasının yeni teknolojileri kullanma taraftarı olanları destekleyici nitelikte olacağını, bu yerine getirildikten sonra E 4.0'a geçişin daha kolay olacağını söylemek mümkün gözükmektedir. Şekil 62'de yer alan, katılımcıların sorun analizine yönelik olarak ele alabileceğimiz söylemlerine bakacak olursak; çeşitli tehdit ve zorlamaların olduğu, birçok insanın bu gibi durumlar karşısında savunmasız olduğu, özellikle yaşlı insanların bu olumsuzluklara daha

fazla maruz kaldığı, yenilikçi teknolojilere yönelik olarak belirli bir tereddüt ve güvensizliğin olduğunu görmekteyiz.

Katılımcıların SM, BG ve E 4.0'ın İlişkilendirilmesine Yönelik Düşüncelerine Ait Bulgular (4.2.5)'a Yönelik Değerlendirme ve Yorumlar

Katılımcıların büyük çoğunluğu özellikle SM ile BG'ni ilişkilendirmiştir. Tablo 16'da yer alan katılımcıların söylemlerine ve Tablo 17'ye dikkatlice bakılacak olursa; SM ve BG'nin neredeyse katılımcıların tamamı tarafından ilişkilendirildiğini, E 4.0'ın muhtemelen yeni bir kavram olması ve tam olarak neleri içerdiğinin bilinmemesi gerekçeleriyle E 4.0'ın SM ile ve E 4.0'ın BG ile yeterince ilişkilendirilemediğini, buna paralel olarak da SM, BG ve E 4.0'ın birbirleriyle nispeten ilişkilendirilebildiğini görmekteyiz. Ayrıca, bu üç kavramın ne şekilde birbirleri ile ilişkilendirildiğinin ise katılımcıların büyük bir kısmında merak uyandırdığını ve bu çalışmanın sonuçlanmasını sabırsızlıkla beklediklerini ifade ettiklerini de belirtmek isteriz.

Katılımcıların Endüstri 4.0 Bağlamında Yenilikçi Teknolojilere Yönelik Olumlu ve Olumsuz Görüşlerine Ait Bulgular (4.2.6)'a Yönelik Değerlendirme ve Yorumlar

Katılımcılardan bazılarının hem olumlu hem olumsuz fikir beyan ediyorlarmış gibi görünmesinin sebebini 4.2.6 numaralı başlık altında açıklamıştık. Bu açıklama dikkate alınacak olursa, katılımcıların genel olarak E 4.0 bağlamında yenilikçi teknolojilerin olumlu yanında yer aldıklarını söylemek mümkün gözükmektedir. Bu tür teknolojilerin her ne kadar güvenlik açıkları ve çeşitli riskler oluşturduğunu/oluşturabileceğini varsaysalar da bu tür teknolojilerin insanların yaşamını daha konforlu kıldığını, güncel yaşamın bu teknolojilerin “nimetlerinden” yararlanmadan devam ettirilmesinin çok zor olduğunu belirtmekte. Bu bağlamda [Katılımcı F»]'in şu cümlesi oldukça dikkat çekicidir: “*Ne kadar büyük olursa olsun hangi şirket 2 veya 3 gün çevrimdışı kalmayı başarabilir ki!*”. Yine benzer bir şekilde [Katılımcı H»]'in ifadesinin de önemli olduğu düşünülebilir: “*Olumsuz şeyler hakkında epeyce konuştuk ama genel olarak bence Endüstri 4.0 çok olumlu olacak. Tüm bu Nesnelerin İnterneti ve Endüstri 4.0 devrimi ile ilgili ummadığımız bir çok sonuçlar olabilir ama ben hâlâ Facebook örneğinde olduğu gibi*

avantajların/getirilerin negatifliklere daha ağır bastığını düşünüyorum. Avantajı, milyarlarca kişinin bağlı ve iletişim halinde olmasıdır. Ben işin olumlu tarafındayım.” İş süreçleri, verimlilik ve optimizasyon açısından ise [Katılımcı J»] ve [Katılımcı K»]’nin ifadelerini önemseyebiliriz: “Geçenlerde General Electric’deydik. 755 bileşen 1’e, 200 tedarikçiyi 0’a indirdiler. Etkinlik ve verimlilik harika olacak, iş yükü azalacak ve zamanla gelişecek.”, “... süreçlerimizi her zaman optimize etmenin ve otomatikleştirmenin ve işimizi gerçekten daha verimli hale getirmenin yollarını arıyoruz. Yani bunu yeni teknolojilerle haşır neşir olarak başarabileceksek, her zaman bunun peşindeyizdir.”

Olumsuzluk oluşturan cümleler incelendiğinde ise en çok; insan faktörünün denklemden çıkartılmasının risk yaratabileceği, insanlarda zihniyet ve davranış değişikliğinin çok zor olduğu, çeşitli güvenlik risklerinin oluşabileceği, yeni teknolojileri geliştiren şirket ya da ulusların bu teknolojileri daima kendi çıkarları doğrultusunda kullanacaklarına dair düşüncelerin yer aldığını görmekteyiz.

II. Kısım

Literatür araştırması sonucu SM, BG ve E 4.0’ın kesişme alanına yönelik tespit edilen en önemli on bir bileşenin önem sıralaması nasıl olmalıdır sorusuna katılımcıların verdiği cevapta ilk üç sırayı “İnsan Faktörü”, “Ulusal Güvenlik” ve “Siber Güvenlik”in yer aldığını görmekteyiz. İnsan faktörü bileşeninin birinci sırada yer almasının en belirleyici sebebinin yapay zekâ destekli tam otomasyon kullanımına henüz istenilen düzeyde geçilememiş olması, insana duyulan güven, teknolojinin insana şu an için ancak asistan olarak yardım edebildiği, esas karar alıcının halen büyük oranda insan olduğu, insan unsuru denklemden çıkarılırsa insanların işlerini kaybedeceği vb. kaygılardan kaynaklandığını görmekteyiz.

E 4.0 için orta vadede insan faktörünün birinci sırada yer almayacağını öngörebilirken, BG ve SM için aynı şeyi söylemenin henüz erken olduğunu düşünmekteyiz. Özellikle yüksek güvenliqli iş ve işlemlerin icrasında ve kriz anlarında manüel sistemlere olan ihtiyaçlar dikkate alınacak olursa, insan faktörünün tam anlamıyla göz ardı edilebilmesinin şu an için mümkün olmadığını söyleyebiliriz.

Katılımcılar tarafından önerilen diğer bileşenler (Etik, Digital Persona, İnsan Unsurunun Seçimi, Liyakat, Terörizm, Eğitim, İnsana Yatırım, Gerçek İş Deneyimi) dikkate alındığında da aynı çıkarımda bulunmak, yani önerilen diğer bileşenlerin neredeyse tamamının insan odaklı olduğunu söylemek mümkün gözükmemektedir. İnsan merkezli bu düşüncenin; insanların işini kaybetmek istememeleri, önemsenmeye ihtiyaç duymaları, teknolojiye güvenin yetersizliği (çeşitli olumsuz deneyimler ya da teknoloji okuryazarlıklarının yetersiz olması vb gerekçelerle), yapay zekâ entegrasyonunun henüz tüm alanlara uygulanamadığı gibi gerekçelerle açıklamak mümkündür.

Literatür araştırması sonucunda (“Sosyal Mühendislik Bağlamında Bilgi Güvenliğinin Endüstri 4.0 Tabanlı Sistemlere Uyarlama Zorluğu”na yönelik olarak) hazırlanan sorun-sonuç analizinde yer alan bulgulara katılımcıların da büyük oranda onaylayıcı fikirlerle katılım gösterdiği, bunun yanı sıra bazı ilave çıkarımlarda bulundukları tespit edilmiştir.

Alan çalışması sonucunda SM ve BG’nin katılımcıların büyük bir kısmı tarafından ilişkilendirildiğini (%73), E 4.0, SM ve BG ise birbirleriyle nispeten ilişkilendirildiğini (%36) görmekteyiz. Literatür araştırmasında ise BG’nin E 4.0 için vazgeçilmez bir unsur olduğu karşımıza çıkmakta. Buradaki farkın E 4.0 kavramının katılımcılar tarafından çerçevesinin tam olarak çizilememesiyle ilişkilendirilmesi gerektiği düşünülmektedir. Alan araştırmasına yönelik katılımcı sayısı artırılarak yapılacak benzer bir çalışmada bu oranın daha yüksek çıkabileceğini düşünmekteyiz.

Katılımcıların genel olarak E 4.0 bağlamında yenilikçi teknolojilerin olumlu yanında yer aldıklarını, bu tür teknolojilerin her ne kadar risk içerse de insanlığa sağladığı kolaylık ve konfordan (hız, performans, verimlilik, maliyet, anlık veri vb.) vazgeçmenin mümkün olmadığının sıkça ifade edildiğini görmekteyiz.

Katılımcılardan elde edilen veriler ışığında; SM’nin kullanıldığı alanların başında seçimler, beyinlerin yıkanması, insanların yönlendirilmesi ve özellikle gençlere yön verilmede kullanıldığı sonucu ortaya çıkmaktadır. SM’de en çok tercih edilen atakların başında “oltalama”, “kimlik avı”, “ikiz web siteleri”nin oluşturulması, “fidye yazılımlar”, kimlik, kredi kartı ve şifre bilgilerine erişimin geldiğini görmekteyiz. Tüm yaş grubunun bu saldırılara maruz kaldığını ifade eden

katılımcılar önlem olarak ise sızma testleri, online eğitimler, sosyal medya kullanımında kısıtlayıcı politikalar ve farkındalık eğitimini ön plana çıkartmaktadır. BG açısından en bilinen sorunların başında insanların kişisel bilgilerini çok kolayca paylaşabilmeleri, sosyal dışlanma riski, yetersiz teknoloji okuryazarlığı ve küçük işletmelerin teknoloji ve İK açısından yetersiz oldukları ifade edilmekte olup, sorumluluklar açısından ise verinin sıkı bir şekilde korunması, umuma açık işlemlerde daha dikkatli olunması gerektiği belirtilmektedir. Bilgi güvenliğine yönelik en önemli risk olarak yazılımlarda yer alan “arka kapı” problemi, Büyük Veri trafiğinin yönetilmesi, devlet güvenliği, hizmetlerin kesintiye uğratılması ve siber saldırıların geldiği görülmektedir. Önlem olarak ise yerel ağlara yabancı girişlerin engellenmesi, güvenlik ve sızma testlerinin düzenli olarak yapılması, kriz zamanlarının yönetilebilmesine yönelik hazırlıkların tamamlanması ve kurumsal eğitimin önerildiğini görmekteyiz. E 4.0 bağlamında yenilikçi teknolojilerin adaptasyonu için konferanslar ve eğitimlerin önemli olduğu ama E 4.0 hakkında belirli bir kavram kargaşasının olması yanı sıra insanlardaki zihniyet değişikliğinin güç olmasından dolayı bu geçişin zorlaştığı yönünde görüşler bulunmaktadır. E 4.0 alanında genel olarak İK’nın yetersiz olduğu, özellikle niteliğin artırılması gerektiği ifade edilmektedir. Yerli teknolojilerin önemsenmesi gerektiğine dikkat çekilirken, maliyet açısından yeni teknolojilere yatırımın ilk başta pahalı olduğu ama zamanla bunu karşılayabileceği ifade edilmektedir. Risk açısından ise robotların insanların işini elinden alacağı yönünde görüşler bulunmasının yanı sıra, her yeni teknolojinin başarılı olacağına yönelik bir garantinin söz konusu olmadığı, küçük işletmelerin yenilikçi teknolojilere ayak uydurmada yetersiz ve büyük şirketlere bağımlı kaldıkları, bulut sistemlerinin ise veri güvenliği açısından güvenilmez olduğu ifade edilmektedir. E 4.0 alanına yönelik fırsatların başında ise süreçlerin hatasız yönetilmesine daha fazla yaklaşılabileceği, insan iş yükünün azalabileceği, mekândan bağımsız çalışmanın mümkün olabileceği ve bu süreçleri daha verimli yönetebilecek yeni iş süreçlerinin oluşturulabileceği belirtilmektedir.

Katılımcıların Endüstri 4.0 bağlamında yenilikçi teknolojilere yönelik olumlu ve/ya olumsuz görüşleri incelendiğinde dikkat çekici olduğu düşünülen söylemlere yönelik olarak şu yorumları yapmak mümkün gözükmektedir: Endüstri 4.0 özellikle BT departmanlarında çalışmayanlara genel olarak yabancı bir kavram olarak

gözüküyor. Katılımcılar, E 4.0'ı kelime olarak duyduklarını ama kavram olarak tam ne anlama geldiğini bilmediklerini ifade etmekte. Örneğin; büyük bir kuruluştaki perakende yöneticisi olup, aynı zamanda bu departmanın BT sorumlusu da olan [Katılımcı F»] *“Endüstri 4.0 kelimesini sözlü olarak duydum... farklı teknolojik faktörlerle ilgili olduğunu duymuştum...”* şeklinde bir ifade kullanılmıştır. Endüstri 4.0'ın kavram olarak neleri kapsadığı konusu BT departmanlarında çalışan bazı yöneticiler için bile tam olarak açık gözüküyor. Öyle ki, büyük bir işletmenin BT departmanı yöneticisi dahi Endüstri 4.0 konusuna genel olarak hâkim gözüküyor. Endüstri 4.0'ın sadece kendi işletmelerini ilgilendiren ilgili bileşeni/bileşenleri hakkında kısmi bilgi sahibi oldukları gözlemlenmiştir. Örneğin, [Katılımcı K»], *“Nesnelerin İnterneti ve robotik teknolojilerini duydum fakat Endüstri 4.0 benim hiç duymadığım yeni bir terim...”* ifadesini kullanmıştır. Özellikle küçük işletmeler gelişen teknolojiler karşısında İK ve finans yönünden zayıf oldukları için büyük firmalara bel bağlamak zorunda kalacaklar gibi gözüküyor. Bir bakıma güvenliklerini de bu firmalara teslim etmek zorunda olacaklar. [Katılımcı H»]'nin bu yöndeki görüşleri şu şekilde; *“Birçok küçük işletme bulut çözümlerini kullanıyor. Finans sistemlerini ve İK'yı bulut üzerinden yönetecekler. Microsoft, Google, Amazon veya başka herhangi bir bulut sağlayıcısı şirket tarafından oluşturulan güvenliğe güvenmek zorunda kalacaklar. Küçük şirketlerin kendi bilgi güvenliği teknolojileriyle başa çıkmaları çok pahalı, uzmanlığı olan çok fazla insanı işe almak zorundalar, bu yüzden bunu dış kaynak kullanarak yapmaları gerekiyor.”*

SONUÇ VE ÖNERİLER

E 4.0'ın en önemli bileşenlerinden biri olan Nesnelerin İnterneti tek başına ele alınacak olsa dahi, yakın gelecekteki E 4.0'ın ne kadar hassas ve oldukça kompleks bir yapıda olacağı ortadadır. Küçük bir SM (müdahalesi) ile BG tehlikeye girecek, bağlı tüm alt birimler bu durumdan olumsuz etkilenebilecektir. Tıpkı post modern yönetim kuramlarından biri olan *düzensizlik içerisinde düzeni* tarif eden, evrenin doğrusal olmayan (non-lineer) yönlerini açıklamaya çalışan *kaos teorisi* ve onun içerisinde yer alan Edward Lorenz'in *kelebek etkisi* teorisi'nde olduğu gibi. Yine aynı şekilde, Mayo, Barnard ve Bartalanffy'nin (1937), Norbert Wiener'in (1948) olay ve birimlerin birbirleri ile olan ilişkisini dış çevre şartları ile ilişkili olarak incelediği, sistemin birbirlerine bağlı alt sistemlerden oluştuğunu ve aralarında sıkı bir ilişkinin bulunduğu, entropi, açık-sistem, girdi-çıkıtı ve geri beslemenin de söz konusu olduğu modern yönetim kuramlarından biri olan *sistem yaklaşımı*'nda olduğu gibi. Sinir hücrelerinin (nöron) oluşturduğu ağ yapıda gördüğümüz gibi, Nesnelerin İnterneti aracılığı ile şekillenen E 4.0 ağ yapısında da benzer şekilde meydana gelebilecek iletişimsizlik ve kesintiler ya da sistem üzerinde üretilerek dolaşıma sokulacak verinin/bilginin manipüle edilebileceği olasılığı bile tüm sistemin defalarca gözden geçirilerek kontrol altına alınmasını ve istikrarlı bir şekilde güvenli (sağlıklı) halde tutulması zarureti ortaya çıkarmaktadır. Bu zaruret bizi bu doğrultuda ele alınacak önleyici (proaktif) girişimlerin sürekli güncellenmesinin "normal işleyişin sürekliliği" açısından son derece önemli ve hayati olduğu sonucuna ulaştırmaktadır.

Literatür araştırması sonucunda SM, BG ve E 4.0'ın kesişme alanlarına yönelik tespit edilen ve öne çıkan on bir bileşenin (Teknoloji Okuryazarlığı, İnsan Faktörü, Kimlik Hırsızlığı, Veri ve Bilgi Güvenliği, Fiziksel Güvenlik, Siber Güvenlik, Ulusal Güvenlik, Dağıtık ve Merkezi Olmayan Yapı, Standartların Geliştirilmesi, Risk Yönetimi, Bütüncü Yaklaşım) önem sırası nasıl olmalıdır sorusuna katılımcıların verdikleri cevaplar (Tablo 12) dikkate alındığında önem sıralamasında SM ve BG için en önemli halka olan (en zayıf halka olarak da bilinmektedir) "İnsan Faktörünün" birinci sırada yer aldığı, buna karşılık yine SM ve BG alanlarında oldukça önemli olduğu bilinen "Kimlik Hırsızlığı"nın yeterince

önemsenmediği ya da dikkate alınmadığı görülmektedir. Yine önem sıralamasında katılımcılara göre en sonlarda yer alan fakat *blokzincir* platformunda oldukça büyük önem arz eden “Dağıtık ve Merkezi Olmayan Yapı”nın ise yeterince bilinmediği ya da gerektiği kadar anlaşılamadığı gözlemlenmiştir. Buna mukabil “Teknoloji Okuryazarlığı” ile “Veri ve Bilgi Güvenliği”nin öneminin kavrandığı, bu bileşenlerin önem sıralamasında ilk beş sıra içerisine kümelendiği görülmektedir. Önem sıralamasında ilk üç sırada yer alan bileşenlere (“İnsan Faktörü”, “Ulusal Güvenlik” ve “Siber Güvenlik”) bakılacak olursa, bir tür güvensizlik ve sürekli saldırıya maruz kalma riskinin var olduğu katılımcılar tarafından hassasiyetle gözetilmekte ve dile getirilmektedir.

Evrendeki enerji sabit kalmakla birlikte tek yönde biçim değiştirmekte, kullanılabilir olandan kullanılamaz olana doğru değişim göstermektedir. Termodinamiğin ikinci yasasına göre enerji akışı mutlaka sıcaktan soğuğa, konsantre olandan dağınık olana, düzenliden düzensize doğrudur. Bir enerji kaybı olmaksızın ortaya çıkan ama fayda sağlamayan bu enerji *entropi* olarak adlandırılmaktadır (Rifkin, 2015, s. 18-19). Benzer bir akışın SM’den BG’ye, oradan ise E 4.0’a olabileceğini hem literatür hem alan araştırması sonuçları bize göstermiştir. Buradaki *akış* “bilginin dolaşımı” olarak ele alınacak olursa, durum daha da önemli bir hal almaktadır: Manipüle edilmiş, bozulmuş ya da eksik bilgi bir tür entropi olarak karşımıza çıkmakta ve bir sonraki hedefe aktarılması gerekenler uygun bir şekilde (gerektiği gibi) aktarılamamaktadır. Böyle bir durumda, bütünün korunması için parçaların dikkatli bir şekilde tek tek ele alınmasının yanı sıra tüm süreçlerin ve yapının eş güdümlü olarak gözetilmesi de gerekmektedir.

Günümüzde, bilgisayar yazılımlarının iletişim ile birleşmesiyle sosyal medya gelişti. İnternetin ticaret için daha fazla kullanılması ve bilgi paylaşımı, büyük verilerin ve istismarının ve ayrıca mahremiyet ve kontrol ile ilgili zor sosyal soruların ortaya çıkmasına neden oldu. Şifreleme, güvenlik duvarları, bilgisayar korsanlığı ve siber saldırılar günlük kaygılarımızın bir parçası haline geldi ve veri bilimi akademik bir disiplin oldu (Turing, 2018, s. 157). Veri bilimi disiplini sayesinde SM, BG ve E 4.0’ın birlikte ele alınarak sorunlara bütüncü bir yaklaşımla çözümler üretilebileceğini hem literatür hem alan araştırması teyit etmektedir. Domingos (2017)’a göre, anlamadığınız şeyi kontrol edemezsiniz ve tam da bu

nedenle, bir vatandaş, bir profesyonel ve mutluluğu arayan bir insan olarak yapay öğrenmeyi anlamamız gerekmektedir (s. 19). Günümüz işletmelerinin lider işletmeler arasına girebilmeleri için benzer bir kontrolü SM, BG ve E 4.0 için yapması gerektiğini düşünmekteyiz. SM ve BG'ye dayalı E 4.0 platformlarını anlamak ve mümkün olduğunca kontrol altında tutabilmek işletmeler ve devletler için bir çok açıdan altın anahtarı elinde tutmak anlamına da gelmektedir. Süreç yönetimi ise; ilk başta onu anlamak, kontrol etmek, yönetmek ve sonrasında da getirilerinden faydalanmak şeklinde cereyan etmektedir.

Süreç, içinde hareket ve zaman kavramlarını barındırmaktadır. Yani, herhangi bir amacı gerçekleştirmek için gerekli olan bileşenleri. Süreç yönetimindeki asıl amaç birim zamandaki çıktıyı kaliteden ödün vermeden artırmaktır; buna kısaca verimlilik denilmektedir. Ne kadar verimli iseniz maliyet konusunda rakiplere göre avantaj da sağlamış olursunuz ve bu da şirketin asıl amacı olan net karlılığı artırıcı bir etki yaratır (Akyıldız, 2018, s. 68). Verimlilik ve net karlılığın arttırılmasında dijitalleşmeyi hedefleyen işletmelerin SM, BG ve E 4.0 süreçlerini eş zamanlı ve etkileşimli (interactive) bir şekilde ele almaları ve yönetmeleri gerekmektedir. Aksi takdirde, ne ayakları yere basan sağlam bir rekabet avantajı elde etmekten, ne de lider bir işletme olmaktan bahsetmek söz konusudur. Dijitalleşme ve dijital süreç yönetiminin bu açıdan temel unsurları oluşturduğunu söylemek mümkündür. SM, BG ve E 4.0 çatısı altında yer alan dijitalleşme ve dijital dönüşüm, bir harç görevi görerek, oyun kurucu ve lider şirketler için vazgeçilmez, en kötü ihtimalle göz ardı edilemez bir unsur olarak karşımıza çıkmaktadır. Memiş (2018, s. 40) dijitalleşmeyi, bilgi ve iletişim teknolojileri, yapay zekâ, robotik, Nesnelerin İnterneti gibi yeni teknolojilerin ürün, hizmet ve süreçleri dönüştürmesi ve değer zincirlerinin dijital hale gelmesi (s. 40) olarak tanımlamakta ve dijitalleşme için şu bilgilere yer vermektedir:

Dijitalleşmeyi mümkün kılan teknolojiler yatay teknolojiler yani farklı sektörleri aynı anda dönüştürme potansiyeline sahip teknolojilerdir. Bu, ekonomik yansımaların bu denli güçlü olmasının en önemli nedenidir. Bu teknolojiler, otomotivden tekstile kadar farklı sektörlerde verimlilik artışlarına neden olmaktadır. Ekonomik etkinin en büyük kaynağını da verimlilik artışları oluşturmaktadır. Dijital dönüşüm sadece üretim süreçlerini değiştirerek verimlilik artışlarına neden olmuyor, günümüzde artık değer zincirlerinin tamamını değiştiriyor. Bunun yanı sıra, yeni teknolojiler sadece üretim yöntemlerini değil, politika tasarım süreçlerinden şirket davranışlarına, idari yapılardan ticaretin yapılma biçimine kadar hayatın her alanını yeniden şekillendiriyor.

Dijital dönüşüm, fiziksel dünyadaki insanların, süreçlerin, ürünlerin sanal ortamda var olması, takip edilebilmesi ve otonom olarak çalışmaya ve hizmet sunmaya devam etmesi olarak da düşünülebilir (Ayhan, 2018, s. 109). Ayhan (2018), dijitalle evrilmiş bir dünyada, yeni *devri* (günümüzde bu yeni *devri* SM, BG ve E 4.0'ın eşgüdümü ve alt bileşenlerinin temsil edeceğini bu çalışma bize göstermiştir) ıskalamak gibi bir lüksün olmadığını, değişime ayak uyduramadığından dolayı, sadece ABD'de en yüksek ciroya sahip 500 kurumun yarısından fazlasının son 20 yıl içerisinde kaybolup gittiğini hatırlatmakta ve ayrıca, sürece ayak uyduramayan işletmelerin küresel ekosistem içerisinde yer bulmalarının çok zor olacağını, işletmelerin ancak bu dönüşüm sayesinde büyüme, yatırım, istihdam, verimlilik, rekabet avantajı, yüksek üretim hızı ve esneklik, yüksek kalite ve düşük fire oranlarına ulaşabileceğini (s. 110) vurgulamaktadır.

Sosyal medya platformlarının zaman içerisinde bireyler hakkında devletlerden daha fazla şey bilir hale gelmesi ve birçoğunun merkezinin ABD'de olması diğer devletleri rahatsız etmeye devam etmektedir. Londra merkezli Cambridge Analytica isimli şirketin Facebook'tan yasal olarak temin ettiği kişisel verileri, kişiselleştirilmiş reklamlar ile ABD'de 2016 Başkanlık seçimlerinde seçmen tercihini manipüle etmek üzere kullandığı ortaya çıkmıştır (Aydın, 2018, s. 153). Bu örnek bize sosyal medya platformlarında mahremiyetin yeterince dikkate alınmadığı, BG'nin (istemli ya da istemsiz olarak) tam olarak sağlanamadığı, SM içinde yer alan manipülasyon teknikleri kullanılarak E 4.0 çatısı altında yer alan veri analitiği, yapay zekâ vb. unsurlar kullanılarak seçmen tercihlerine ve dolayısıyla devlet politikalarına nasıl yön verilebildiğini göstermektedir. Bu örnekte yer alan süreçlerin bir kısmının yasal olması insanların ve devletlerin rahatsız olmasının önüne geçememektedir. Alan araştırmasında katılımcıların büyük bir çoğunluğunun da benzer konulara dikkat çekerek, özellikle SM'nin politik manipülasyonlarda ve seçmenleri yönlendirmede çokça kullanıldığını ve bunun rahatsızlık verici boyutlarda olduğunu ifade ettiklerini görmekteyiz.

SM, BG ve E 4.0 için (E 4.0 için bu durum gelecekte değişebilecek olsa da) İK ve İK yönetiminin (işe alım, özlük işleri, eğitim, işten çıkartma vb. tüm süreçler) en önemli bileşenlerin başında yer aldığını ve hiçbir zaman göz ardı edilemeyeceğini görmekteyiz. “Entelektüel sermaye” ve “kurumsal varlık” olarak da kabul edilen

insan faktörü Schmidt ve Rosenbergn (2018, s. 255) tarafından da oldukça önemsenmekte ve “en değerli kaynağınız çalışanlarınız olduğu için -bu durum her zaman böyledir- bu kaynakları doğru şekilde kullanan akıllı bir sistem geliştirmek başarı yolunda atılması gereken en önemli adımdır” şeklinde ifade edilmektedir.

Entegre bir pazar ekonomisindeki hiçbir şirket, alt yapısız başarılı olamaz. Altyapılar kamu malıdır ve devletin yetkilendirmesi ve pazarın kolaylaştırılmasıyla yapırlar (Rifkin, 2015, s. 79). E 4.0’ın entegrasyonunda en çok zorlanan küçük işletmeler için E 4.0’a yönelik alt yapının (en azından temel unsurlarının) ve pazara erişimin kolaylaştırılmasının devlet tarafından desteklenmesinin önemli olduğunu bu çalışma bize göstermektedir. Ford (2018) üretimde kullanılan makinelerin geliştikçe, bu makineleri kullanan işçilerin üretkenliklerinin de arttığını ve böylece işçilerin daha değerli hale geldiğini ve daha yüksek ücret talep edebildiklerini (s. 10), fakat yeni çağın en tanımlayıcı özelliğini, işçilerin yerlerini makinelere bırakacak olmasını (s. 12) hatırlatarak, teknolojiye dair en temel varsayımlardan biri olan “Makine işçinin üretkenliğini artıran bir araçtır”ı da sorgulamak gerektiğini belirtiyor. Bu gerekçelerle E 4.0’a yönelik politikalar geliştirilirken istihdam sorununun yaşanmaması için işletme/devlet bünyesinde görev yapan planlayıcıların bu konuyu büyük bir titizlikle ele almaları ve yakın gelecek için yol haritasını buna göre hazırlamaları uygun olacaktır.

Amazon ve eBay, aynı gün içerisinde teslimat denemeleri yapıyor. Böylece fiziksel mağazacılığın sanal mağazalara karşı olan son büyük avantajını da bertaraf etmeyi umuyorlar (Ford, 2018, s. 35). Yeni nesil *dronlar* sayesinde saatler içerisinde yapılabilecek ürün teslimatı sayesinde, müşterinin ürünü satın aldığı anda yaşamış olduğu tatmin duygusunu da fiziksel mağazacılığın elinden almış olacaklar. Özellikle e-ticaret yoğun işletmelerin bu gelişmeleri dikkatle ele alması ve zamanın gerisinde kalmamaları önemli bir ayrıntıdır. Yine Endüstri 4.0 ile hayata geçirilecek dönüşümlerden bir diğeri için Ford (2018), tam otomatik self-servis perakende sektörünün hızla büyümesini gösteriyor ve otomatların perakende pazarında maruz kalınan üç büyük maliyet unsuru olan yer maliyeti, çalışanların ücreti ile müşteri ve çalışanların yaptığı hırsızlıkları ciddi biçimde aşağıya çekeceğini (s. 37) öne sürüyor.

Ford (2018)’a göre, eğer, ilerleyen teknoloji tahmin edildiği gibi sanayileşmiş ülkelerdeki eşitsizliği daha da büyütürse, o zaman finans gücünü elinde bulunduran

kesimin siyasi nüfuzu daha da artacak demektir. Böyle bir durumda orta ve alt sınıfın gelir dağılımında iyileşme sağlayabilecek politikaların yürürlüğe girmesi iyice zorlaşacaktır (s. 82). Bu varsayımdan hareketle, Endüstri 4.0 çatısı altında yer alacak *blockchain* teknolojisinde yer alan dağıtık ve merkezi olmayan ve aracısız yapılar daha da önem kazanacak diyebiliriz. Ford (2018)'a göre, karşılaştırmalı üstünlük teorisinde, diğer insanlara kıyasla “en az kötü” olunan alanda uzmanlaşmak iş bulmayı her zaman mümkün kılmaktadır. İnsanların bu şekilde davrandığında, diğerlerinin de daha fazla uzmanlaşması ve para kazanması için fırsat verilmiş olacaktır (s. 96). Ford yine benzer şekilde, ekonomi tarihi boyunca, insanları daha fazla uzmanlaşmaya ve kendi aralarında daha çok ticaret yapmaya iten şeyin *karşılaştırmalı üstünlük* olduğunu belirtiyor. Ford'un bu tespit ve öngörülerini öyle gözüküyor ki, uzmanlaşmanın, robotik ve siber fiziksel sistemlerin yer aldığı Endüstri 4.0'da önemli yer tutan makinelere geçmesiyle birlikte geçerliliğini büyük oranda yitirecektir. Yine aynı şekilde, uzmanlaşmış kişilerin yerini uzmanlaşmış makinelerin almasıyla, karşılaştırmalı üstünlük teorisi de büyük bir yara alacaktır.

GPS'lerin hacklenmesi, trafiğin kasten belirli bir güzergâha yönlendirilerek bilinçli tıkanıklığa sebebiyet verilmesi, *jammer*'lar ile iletişimin kesilmesi, sağlık kayıtlarının değiştirilmesi, gemi ve uçakların rotalarından çıkartılabilmesi vb. teknolojik saldırıların her türlü güvenliği risk altına sokabildiğini görmekteyiz. Goodman (2016) ise bu olguyu şu şekilde tarif etmektedir: Artık teknolojiyi kullanarak insanlığa faydalı olmak isteyenler ile başkalarına zarar vermeyi önemsemeden araçları kötüye kullanmayı tercih edenler arasında yepyeni bir savaş başlamış durumda. Teknolojinin ruhu ile geleceği için bir savaş yaşanıyor. Şimdiye dek gizlice, yeraltında devam eden ve sıradan insanlardan saklanan bu savaş artık gittikçe gün yüzüne çıkıyor ve kızışıyor (s. 13). Sanal dünyadaki tehdit unsurlarının analizi yapıldığında ise, karşımıza hacktivistler, suçlular, vekil savaşçılar, teröristler ve hatta devletler çıkmaktadır. Bunların hepsi de, mevcut teknolojik altyapıdaki açıkları sonuna kadar kullanmaktadır. Finansal veriler, kimlik bilgileri, çocukların bebeklik fotoğrafları ve elektrik şebekeleri oldukça kolay hedef olarak savunmasız bir şekilde risk altında bekliyor. Küresel bilgi şebekesine olan bağlantı genişliği ve derinliği önümüzdeki yıllarda ciddi oranda büyüyecek ve her tarafımızı sarmış olan

teknoloji üstel büyüme ile başımızı döndürecek bir teknoloji dalgasına dönüşebilecektir (Goodman, 2016, s. 56).

Özellikle SM ve BG için alınabilecek en basit önlemlerin güvenliğe yönelik tehditlerin *kelebek etkisini* tahmin edilenden çok daha yüksek bir oranda önleyebileceğini söyleyebiliriz. Bu yaklaşımımızı şu örnekle açıklamak oldukça mümkün gözükmemektedir: Günümüzde Büyük Verinin yüzleştiği en büyük tehlike, hırsızlık ve sızıntılardan kaynaklanıyor. Ancak bunlar daha henüz başlangıç. Gelişmeler devam ettikçe, çok daha vahim sonuçlar doğurabilecek tehlikelerle karşılaşacağız. (...) Yaklaşan fırtına bizleri daha fazla savunmasız bırakacağı gibi, veri bağımlı dünyanın temellerine olan inancımızı da henüz anlamadığımız bir şekilde sarsacaktır (Goodman, 2016, s. 180). İran'ın Natanz'daki U-235 zenginleştirilmesinde kullanılan santrifüjlerin Stuxnet solucan yazılımı ile sabote edilmesi (internete çıkışı olmayan bir ağ üzerinde çalıştırıldığından) yalnızca bir flash belleğin tek bir bilgisayardaki USB girişine takılması sayesinde gerçekleştirilebildi (Goodman, 2016, s. 182).

Küçük farkındalıklar yaratmanın büyük kazanımlara destek olacağını, diğer yandan ise basit bir SM atağının sistemleri kullanılmaz hale getirmek için yeterli bir araç olabileceğini anlamamız gerekiyor. Goodman (2016)'ın şu açıklamaları bu manada oldukça dikkat çekicidir: Zaman ilerledikçe, bugün bilgisayar suçlarındaki tüm alanların biyolojik birer karşılığı olacaktır. Şöyle ki; genetik bilgilerin hacklenmesi, özellikle de kimlik doğrulama için DNA'nın yaygın bir şekilde kullanılacağı düşünüldüğünde yarının kimlik hırsızlığı bu yönde gelişebilecektir. Nitekim kimlik hırsızlığının ulaşabileceği en uç noktada insan klonlama yatıyor. Bu yol üzerindeki teknik engeller hızla ortadan kaldırılırken, polis ve toplumun buna karşı pek bir hazırlığı bulunmuyor. Bütün insanlık olarak, dünyanın işletim sistemini korumak için gereken adımların şimdiden atılmaya başlanması gerekiyor (s. 485). Durumun ciddiyeti fark edildiğinde pek çok şey için geç kalınmış olabilir. Aynen, Fransız okullarında öğrencilere üstel büyümenin ne olduğunu anlatabilmek için kullanılan havuzun nilüfer çiçekleriyle kaplanması örneğinde olduğu gibi; otuz günlük süreç boyunca yirmi dokuzuncu güne kadar havuzun ancak yarısının kaplandığı, ancak o tek bir günde ise, tahminlerin dışında, havuzun tamamının

kaplandığının gözlemlenmesi gibi. Bu ve benzeri durumları bir “siyah kuğu” olarak da değerlendirmek mümkündür.

Tehlikeler her zaman basit bir araç ya da gerekçeden vuku bulmamakta, daha karmaşık bir yapıda da seyredebilmektedir. Rose (2016) karmaşıklığı (*complexity*) anlayabilmek için onun yakın ilişkide olduğu çapraşıklığı (*complicatedness*) da anlamak gerektiğini ileri sürmektedir. Rose, çapraşık sistemlerin birçok hareketli parçaya sahip olduğunu ancak bunların diziliminin anlaşılabilir bir yapı içerdiklerini, karmaşık sistemlerin ise birçok öğeden oluştuğu ve alt sistemlere sahip olduğunu, bu sebeplerden dolayı karmaşık sistemleri öngörmenin çok zor olduğunu ifade etmektedir. Bu duruma örnek olarak ise, küresel ekonominin karmaşık bir sistem olduğunu, 2011 yılında Yunanistan’ın 300 milyar dolar olan borcunun yarısını ödememe tehdidinde bulunduğu, küresel borsaların bir trilyon dolar kaybettiğini hatırlatmaktadır (s. 21-22). Rose, aslında burada karmaşık sistemlerin kaldıraç etkisine de dikkatleri çekmektedir. SM, BG ve E 4.0 arasındaki bağlantıların meydana getirdiği karmaşıklığı (karışıklığı değil) doğru analiz edip, interaktif bir düzen içerisinde hareket ettiğini kavrayarak gerekli önlemleri alabilmek, onun negatif yönde oluşturabileceği bir dizi hassasiyetleri öngörebilmekle doğru orantılıdır. Depremi önemli olması kadar, artçıların da dikkate alınması gerekmektedir. Zira taşı delen suyun gücü değil damlaların sürekliliğidir. Domino etkisini de hiç bir zaman göz ardı etmememiz gerekmektedir.

Rose (2016, s.38), *kaos teorisi*’nin, kendi kendini örgütleyen bir sistemin farklı parçaları arasında bağlantı kuramamasının kaosa ve katılaşmaya yol açacağını söylediğini belirtmektedir. Benzer bir durumun SM, BG ve E 4.0 ilişkisi için de geçerli olduğunu söyleyebiliriz ve bu üç alanın yönetiminin eş güdümlü olarak ele alınmadığında, güvenlik (veri, bilgi, fiziksel vb.) açısından belirgin bir “katılaşmanın” meydana gelebileceğini öngörmek zor değildir. Bu katılaşma gerekli esnekliğin sağlanamamasına ve ardından kırılmalara sebebiyet verebilecek, sonrasında ise bir çöküş (*collapse*) söz konusu olabilecektir.

Özellikle BG açısından bir ülke vatandaşlarının nüfus kimlik kayıt bilgileri, tapu sicil kayıtları, iletişim bilgileri (telefon numaraları, e-posta ve ev/iş adresleri), sağlık kayıtları, kan örnekleri toplu olarak dışarıya (üçüncü kişi, kurum ya da devletlere) sızdırılıyor ve bu bilgiler ortalıkta dolaşıyorsa ve benzer bir şekilde banka

kayıtlarında yer alan kişisel bilgiler ticari amaçlı olarak ve etik değerler gözetilmeksizin bazı şirketlere satılabiliyor ise, veri güvenliği açısından oldukça sorunlu bir durumun varlığından söz edebiliriz. Vize uygulayan devletlere vize başvurusunda bulunabilmek için gerekli evraklar arasında yer aldığı öne sürülerek, uluslararası karşılıklılık ilkesine de aykırı olarak tek taraflı olarak talep edilen diğer kişisel veriler (biyometrik fotoğraflar, biyometrik veriler, şirket ya da özel banka hesap dökümleri, tapu ve mal varlıkları kayıtları, vukuatlı nüfus cüzdanı bilgileri, maaş bordrosu, iş yeri, ev adresi, iletişim bilgileri, mevcut tüm pasaportlar, aile ve çocuklara ait bilgiler, yurt dışındaki akrabalara ait bilgiler ve hatta sosyal medya hesap bilgileri vb.) de bunun üzerine eklenecek olursa, stratejik savaş ne yazık ki daha başlamadan kaybedilmiş demektir. Uluslar çok zorunlu olmadıkça konvansiyonel/sıcak savaşlar yerine artık veri/bilgi temelli savaşları tercih etmektedir. Sosyal medyada, kişilerin rızası ya da sosyal mühendislik yönlendirmeleriyle çevrimiçi yayımlanan diğer kişisel veriler ise artık işin eğlenceli kısmını oluşturmaktadır! Yalnızca terör ve benzeri olaylardan insanları korumak adına önlem almak ve istihbarat toplamak için yapıldığı iddia edilen bu girişimler pek inandırıcı ve akla yatkın gelmiyor. Ülkelerin anayasalarında “*Kişisel ve kurumsal bilgi güvenliğinin sağlanmasına yönelik olarak kamu/özel kurum ve kuruluşların gerekli önlemleri alma, devletin ilgili birimlerinin ise bunları denetleme yükümlülükleri bulunmaktadır...*” ya da benzeri bir ifadenin yer alması artık gerekli ve kaçınılmazdır. Veriler artık “varlık” olarak değerlendirilmektedir. Özellikle şirketlerin veri bankaları artık şirket varlıkları olarak yorumlanmaktadır. “Devlet, vatandaşların can ve mal güvenliğini sağlamakla yükümlüdür” desturunun yanına veri güvenliğinin sağlanması da eklenmelidir.

Ekonominin dönüşümü dördüncü sanayi devrimi olarak tanımlanmaktadır. Dünya Ekonomik Forumu'nun kurucusu ve başkanı Klaus Schwab'a göre, şu anda, "fiziksel, dijital ve biyolojik dünyalar arasındaki çizgileri bulanıklaştıran teknolojilerin bir araya gelmesi" ile karakterize edilen dördüncü sanayi devrimini yaşıyoruz (Turing, 2018, s. 196). Dördüncü sanayi devrimi ya da bilinen diğer adıyla Endüstri 4.0'dan en yüksek verimi alabilmek için SM, BG ve E 4.0'ın birlikte ele alınması gerektiğini ve bu üç kavramı bütünün parçaları olarak görmenin,

görebilmenin oldukça önemli olduğunu bu çalışma bizlere açık bir şekilde göstermektedir.

Yapılan bu çalışmaya alan araştırması bulguları açısından bakıldığında belirli sınırlılıklar mevcuttur: Bulgular, iki farklı ülkeden, toplamda on kurum ve on bir katılımcının çerçevesinden bakılarak yansıtılmıştır. Her ne kadar tatmin edici bir çok bulgu elde edilmiş olsa da, daha çeşitli verilerin üretilebilmesi için bu çalışmada yer alan bulgulara dayalı önerilere yenilerini eklemek amacıyla, sonraki çalışmalarda daha fazla sayıda kurum ve kişiyle görüşme yapılabilir ve/veya anketler yoluyla çalışma genişletilebilir. Ayrıca, imkânlar el verdiği sürece alan araştırmasını daha çok ülkeye yayarak yapmanın, daha fazla “saklı” bilgi elde etmede ve bulguları çeşitlendirmede faydalı olacağı düşünülmektedir.

KAYNAKÇA

Kitap

- ABUŞKA, K. (2010). *Kamuoyu oluşturma çalışmaları ve toplum mühendisliğinin gelişimi*. (yayımlanmamış yüksek lisans tezi). Polis Akademisi, Güvenlik Bilimleri Enstitüsü, Güvenlik Stratejileri ve Yönetimi Anabilim Dalı, Ankara.
- AKSU, H. (2013). *Big Data ve Diğer Yeni Trendler*. İstanbul: Pusula Yayıncılık.
- AKYILDIZ, M. (2018). Süreçlerin Dijitalleşmesi. Aksu, H. (Der.), *Dijitopya: Dijital Dönüşüm Yolculuk Rehberi* içinde (s. 68-70). İstanbul: Pusula.
- ALBERT, M. (2018). *Mümkün Ütopya: yaşanabilir bir toplum için stratejiler*. (B. Baysal, Çev.). İstanbul: Kolektif.
- ALTINKAYNAK, M. (2018). *Uygulamalı Siber Güvenlik ve Hacking* (5. bs.). İstanbul: Abaküs.
- ALTUNIŞIK, R., ÇOŞKUN, R., YILDIRIM, E. ve BAYRAKTAROĞLU, S. (2010). *Sosyal Bilimlerde Araştırma Yöntemleri* (6. bs). Sakarya: Sakarya Kitapevi.
- APAK, D. (2018). *Soğuk savaş döneminde algı yönetimi ve haber-propaganda ilişkisi*. (yayımlanmamış doktora tezi). Marmara Üniversitesi, Sosyal Bilimler Enstitüsü, Gazetecilik Anabilim Dalı, İstanbul.
- APİLİOĞULLARI, L. (2018). *Dijital Dönüşümün Yol Haritası Endüstri 4.0: Değişimin Değiştirdikleri*. İstanbul: Aura Kitapları.
- ASLANBAKAN, E. (2017). *Bilgi Güvenliği ve Uygulamalı Hacking Yöntemleri* (2. bs.). İstanbul: Pusula.
- AWAD, A. I. (2018). Introduction to information security foundations and applications. Awad, A. I. ve Fairhurst, M. (Der.), *Information Security: foundation, technologie and applications* içinde (s. 3-11). London: The Institution of Engineering and Technology.
- AYDIN, A. (2018). Devletin Dijitalleşmesi. Aksu, H. (Der.), *Dijitopya: Dijital Dönüşüm Yolculuk Rehberi* içinde (s. 149-153). İstanbul: Pusula.
- AYHAN, M. (2018). Endüstri 4.0 Vizyonu. Aksu, H. (Der.), *Dijitopya: Dijital Dönüşüm Yolculuk Rehberi* içinde (s. 109-111). İstanbul: Pusula.
- BAKİOĞLU, F., Ö., K. (2015). Bilgi Yönetimi ve İş Süreçleri Etkileşimi, Gülseçen, S. (Der.), *Bilgi Yönetimi: bilgi tüketicileri, büyük veri, inovasyon ve kurumsal zekâ* içinde (s. 79-90). İstanbul: Papatya.

- BAKTIR, H., Ö. (2013). Bilgi Paylaşım Ortamı Olarak Bilgisayar. Gülseçen, S. (Der.), *Bilgi ve Bilginin Yönetimi: knowledge management* içinde (s. 97-143). İstanbul: Papatya.
- BANGER, G. (2018b). *Endüstri 4.0 Uygulama ve Dönüşüm Rehberi*. Eskişehir: Dorlion Yayınları.
- BARIŞKAN, M. A. (2017). *Türkiye’deki siber güvenlik bilinci ve sosyal mühendislik ataklarına karşı savunma önlemlerinin geliştirilmesi*. (yayımlanmamış yüksek lisans tezi). İstanbul Üniversitesi, Fen Bilimleri Enstitüsü, Bilgisayar Mühendisliği Anabilim Dalı, İstanbul.
- BİSWAS-DIENER, R. (2018). The brain and nervous system. In R. Biswas-Diener & E. Diener (Der.), *Noba textbook series: Psychology* içinde. Champaign, IL: DEF publishers. DOI: nobaproject.com
- BOSTROM, N. (2018). *Süper Zekâ: Yapay Zekâ Uygulamaları, Tehlikeler ve Stratejiler*. (F. B. Aydar, Çev.). İstanbul: Koç Üniversitesi Yayınları.
- BÖLÜKBAŞI, F. (2012). *Teknoloji Okuryazarlığına İlişkin İlköğretim Öğretmenlerinin Görüşleri: Ankara İli, Çankaya İlçesi Örneği*. (yayımlanmamış yüksek lisans tezi). Gazi Üniversitesi, Eğitim Bilimleri Enstitüsü, Eğitim Bilimleri ABD, Eğitim Teknolojisi Bilim Dalı, Ankara.
- BRYMAN, A. (1992) Quantitative and Qualitative Research: Further Reflections on Their Integration, J. Brannen (Der.). *Mixing Methods: Qualitative and Quantitative Research* içinde (s. 57-78). Avebury: Aldershot.
- CANBAZ, N. (2010). *Yetişkin Eğitimi Kurslarına Devam Eden Kadın Kursiyerlerin Teknoloji Okuryazarlığı Eğitim İhtiyacını Belirleme*. (yayımlanmamış yüksek lisans tezi). Çanakkale Onsekiz Mart Üniversitesi, SBE, Eğitim Bilimleri ABD, Eğitim Yönetimi ve Denetimi Bilim Dalı, Çanakkale.
- CIALDINI, R. B. (2018). *İknanın Psikolojisi: teori ve pratik bir arada*. (Y. Fletcher, Çev.). İstanbul: MediaCat.
- CRESWELL, J. W. (2015). *Nitel Araştırma Yöntemleri* (2. bs). (M. Bütün ve S. B. Demir, Çev. Ed.). Ankara: Siyasal Kitapevi.
- CRYSTAL, D. (2018). *Dilin Kısa Tarihi*. (T. Göbekçin, Çev.). İstanbul: Alfa.
- CSIKSZENTMIHALYI, M. (2017). *Good Business: Liderlik, Akış ve Anlam Yaratma* (2. bs). (N. Tümay, Çev.). İstanbul: Okuyanıs.
- ÇAKIR, F. S. (2018). *Yapay sinir Ağları: Matlab Kodları ve Matlab toolbox Çözümleri*. Ankara: Nobel.

- ÇAVUŞ, G. (2018). Medyada Güven Erozyona Uğrarken Doğrulama Platformları Neden Önemli? Çoban, S. (Der.), *Medya ve Yalanlar* içinde (s. 55-73). İstanbul: SiyahBeyaz.
- ÇOBAN, S. (2018). *Medya ve Yalanlar*. İstanbul: SiyahBeyaz.
- ÇOBAN, S. (2018). Medya, Yalan, Gerçek, Propaganda ve Faşizm. Çoban, S. (Der.), *Medya ve Yalanlar* içinde (s. 11-29). İstanbul: SiyahBeyaz.
- ÇUBUKÇU, F. (2018). *Bilgi Güvenliği Yönetim Sistemi: ISO 27001:2013 uygulama kılavuzu*. İstanbul: Pusula.
- DAVENPORT, T. (2014). *Big Data at Work: Efsaneye son vermek, fırsatları keşfetmek*. (M. Çavdar, Çev.). İstanbul: THY Yayınları.
- DİNÇMEN, M. (2010). Bilgi Yönetimine Giriş. Dinçmen, M. (Der.), *Bilgi yönetimi ve uygulamaları* içinde (s. 13-27). İstanbul: Papatya.
- DOMINGOS, P. (2017). *Master Algoritma: Yapay Öğrenme Hayatımızı Nasıl Değiştirecek?* (2. bs.). (T. Göbekçin, Çev.). İstanbul: Paloma Yayınevi.
- ERBAŞLAR, G. ve DOKUR, Ş. (2016). *Elektronik Ticaret: Genel Bilgiler, Hukuksal Düzenlemeler, Belge Düzeni ve Muhasebe İşlemleri* (3. bs.). Ankara: Nobel.
- ERTAN, H. (2016). *Stratejik algı yönetimi: telekomünikasyon sektöründe müşteri deneyim yönetimi aracılığıyla stratejik algı yönetimi üzerine bir araştırma*. (yayımlanmamış yüksek lisans tezi). Bahçeşehir Üniversitesi, Sosyal Bilimler Enstitüsü, Genel İşletmecilik, İstanbul.
- FORD, M. (2018). *Robotların Yükselişi: Yapay Zekâ ve İşsiz Bir Gelecek Tehlikesi*, (C. Duran, Çev.). İstanbul: Kronik.
- FREY, T. (2016). *Gelecekle İletişim*. (C. Turan, Çev.). İstanbul: Nail.
- FURNELL, S. (2018). Information security foundation, theories and future vision. Awad, A. I. ve Fairhurst, M. (Der.), *Information Security: foundation, technologie and applications* içinde (s. 13-39). London: The Institution of Engineering and Technology.
- GOODMAN, M. (2016). *Geleceğin Suçları: Dijital Dünyanın Karanlık Yüzü*. İstanbul: Timaş Yayınları.
- GÜRBÜZ, S. ve ŞAHİN, F. (2016). *Sosyal Bilimlerde Araştırma Yöntemleri: Felsefe-Yöntem-Analiz* (3. bs.). Ankara: Seçkin.
- GÜREL, M. (2017). *Dijital Kehanet: Hepimiz Siborguz*. İstanbul: Destek Yayınları.

- HADNAGY, C. (2017). *Sosyal Mühendislik: insan kandırma sanatı* (2. bs). (B. Erol ve F. Tuncer, Çev.). İstanbul: Paloma.
- HARARI, Y. N. (2018). *21. Yüzyıl için 21 ders*. (S. Siral, Çev.). İstanbul: Kolektif.
- ISLAM, R. (2018). Cybersecurity: timeline malware analysis and classification. Awad, A. I. ve Fairhurst, M. (Der.), *Information Security: foundation, technologie and applications* içinde (s. 215-239). London: The Institution of Engineering and Technology.
- JAMES, A., BULAJOUL, W., SHEHU, Y., LI, Y. ve OBANDE, G. (2018). Security challenges and solutions for e-business. Awad, A. I. ve Fairhurst, M. (Der.), *Information Security: foundation, technologie and applications* içinde (s. 121-147). London: The Institution of Engineering and Technology.
- KAHNEMAN, D. (2018). *Hızlı ve Yavaş Düşünme* (8. bs). (O. Ç. Deniztekin ve F. N. Deniztekin, Çev.). İstanbul: Varlık.
- KAKU, M. (2017). *Zihnin Geleceği: bilimin zihni anlamaya ve geliştirmeye yönelik arayışları* (5. bs). (E. Kumral, Çev.). Ankara: Odtü Yayıncılık.
- KARA, M. (2018). *Kurumsal Bilgi Güvenliği: Yönetimsel ve Teknik Yönleriye*. İstanbul: Papatya.
- KOCH, R. ve LOCKWOOD, G. (2018). *Sadeleştirir: başarılı işletmelerin büyük sırrı*. (Z. Koçak, Çev.). İstanbul: CeoPlus.
- KÖKSALDI, S., Polat, M., Meydanlı, İ. İ. ve Duman, B. (2010). Bilgi Yönetimi Yapısının Ölçülmesi. Dinçmen, M. (Der.), *Bilgi yönetimi ve uygulamaları* içinde (s. 211-228). İstanbul: Papatya.
- KURZWEIL, R. (2019). *Bir Zihin Yaratmak: İnsan Düşüncesinin Esrarı* (2. bs). (D. Gostolüpçe, Çev.). İstanbul: İstanbul Bilgi Üniversitesi Yayınları.
- LAUDON, K., C., LAUDON, J., P. (2011). *Yönetim Bilişim Sistemleri: dijital işletmeyi yönetme. Management Information Systems: managing the digital firm*. (12. bs). (U. Yozgat, Çev. Ed.). Ankara: Nobel.
- LILLEKER, D. G. (2013). *Siyasal İletişim: temel kavramlar*. (K. Bölükbaş, Çev.). İstanbul: Kaknüs İletişim.
- LÖKKE, E. (2018). *Mahremiyet: dijital toplumda özel hayat*. (D. Başak, Çev.). İstanbul: Küy.
- MANN, I. (2008). *Hacking the Human: social engineering techniques and security countermeasures*. Publisher: Gower, Hampshire.

- MARR, B. (2017). *Büyük Veri İş Başında: 45 Yıldız Şirket Büyük Veri'yi Nasıl Kullandı?*. (B. Gündüz, Çev.). İstanbul: MediaCat.
- MARR, B. (2018a). Beyond the Big Data Buzz: How Data is Disrupting Business in Every Industry In the World.
<https://www.bernardmarr.com/img/Beyond%20the%20Big%20Data%20Buzz.pdf> (Erişim: 08.05.2019).
- MEMİŞ, S. A. (2018). Dijitalleşmenin Ekonomik Boyutu. Aksu, H. (Der.), *Dijitopya: Dijital Dönüşüm Yolculuk Rehberi* içinde (s. 40-43). İstanbul: Pusula.
- MEYDANLI, İ. İ. (2018). Üretim Sektöründe Başarılı Bir İnovasyon Hikâyesi. Aksu, H. (Der.), *Dijitopya: Dijital Dönüşüm Yolculuk Rehberi* içinde (s. 345-347). İstanbul: Pusula.
- MITNICK, K. D. ve SIMON, W. L., (2001). *The Art Of Deception: Controlling the human of security*. Wiley.
- MORENO, J., A. SERRANO, M., ve FERNÁNDEZ-MEDINA, E. (2018). Recent security issues in Big Data: from past to the future of information systems. Awad, A. I. ve Fairhurst, M. (Der.), *Information Security: foundation, technologie and applications* içinde (s. 149-171). London: The Institution of Engineering and Technology.
- OK, K. (2013). Bilgi ve Bilgi Yönetimine Giriş. (Ed. Gülseçen, S.) *Bilgi ve bilginin yönetimi* içinde (s. 19-36). İstanbul: Papatya.
- ÖZARSLAN, M. Z. (2014). *Kitleleri harekete geçirme aracı olarak sosyal algı yönetimi*. (yayımlanmamış yüksek lisans tezi). İstanbul Ticaret Üniversitesi, Sosyal Bilimler Enstitüsü, Uluslararası İlişkiler Anabilim Dalı, İstanbul.
- ÖZDOĞAN, O. (2016). *Büyük Veri Denizi: veri yönetimi hakkında her şey*. Ankara: Elma Yayınevi.
- ÖZDOĞAN, O. (2018). *Endüstri 4.0: Dördüncü Sanayi Devrimi ve Endüstriyel Dönüşümün Anahtarı* (2. bs). İstanbul: Pusula.
- ÖZTEMEL, E. (2010). Bilgi Yönetimi Modelleri. Dinçmen, M. (Der.), *Bilgi yönetimi ve uygulamaları* içinde (s. 29-70). İstanbul: Papatya.
- ÖZTUNA, B. (2017). *Endüstri 4.0: Dördüncü Sanayi Devrimi İle Çalışma Yaşamının Geleceği*. Ankara: Gece Kitaplığı
- PAKTİN, S. ve KARACA, H. S. (2018). Post-Truth, Medya ve İktidar. Çoban, S. (Der.), *Medya ve Yalanlar* içinde (s. 121-159). İstanbul: SiyahBeyaz.

- PUNCH, K. F. (2014). *Sosyal Araştırmalara Giriş: Nicel ve Nitel Yaklaşımlar* (3.bs). (D. Bayrak, H.B. Arslan, Z. Akyüz, Çev.). Ankara: Siyasal Kitabevi.
- QUIEL, S. (2013). *Social Engineering in the Context of Cialdini's Psychology of Persuasion and Personality Traits*. Bachelor Thesis. Hamburg University of Technology.
<https://pdfs.semanticscholar.org/2c8c/a5aaf22aa144d06eea1bd5757aa704ec2a9d.pdf> (Erişim: 29.01.2019).
- ROSE, J. (2016). *İyi Akort Edilmiş Şehir: modern bilim, kadim uygarlıklar ve insan tabiatı bize geleceğin şehir yaşamı konusunda neler anlatıyor*. (T. Gezer, Çev.). İstanbul: Optimist.
- RIFKIN, J. (2015). *Nesnelerin interneti ve işbirliği çağı*. (L. Göktem, Çev.). İstanbul: Optimist.
- SAHLINS, M. (2016). *Taş Devri Ekonomisi* (2. bs.). (T. Doğan ve Ş. Özgün, Çev.). İstanbul: Bgst Yayınları.
- SAY, C. (2018). *Yapay Zekâ* (7. bs). İstanbul: Bilim ve Gelecek Kitaplığı.
- SCHMIDT, E. ve ROSENBERG, J. (2018). *Google Nasıl Yönetiliyor?* (5. bs), (C. Özdemir, Çev.). İstanbul: Timaş Yayınları
- SUSSKIND, J. (2018). *Future Politics: living together in a world transformed by tech*. UK: Oxford University Press.
- TOSUN, A. (2015). *A survey about the integration of social engineering attacks with cyber security exploiting Turkish vulnerabilities in Turkey*. (yayımlanmamış yüksek lisans tezi). Middle East Technical University, Informatics Institute, The Department of Information Systems, Ankara.
- TURING, D. (2018). *The Story of Computing: From the Abacus to Artificial Intelligence*. London: Arcturus Publishing Limited.
- WIGGINS, L. and HUNTER, H. (2016). *Relational Change: the art and practice of changing organizations*. Bloomsbury Publishing.
- YAZICIOĞLU, O., BORAT, O. ve KILIÇ, H. C. (2014). *Bilgi Yönetimi*. Ankara: Nobel.
- YENİSEY, M., M. (2010). Kurumsal Zeka – Veri Madenciliği. Dinçmen, M. (Der.), *Bilgi yönetimi ve uygulamaları içinde* (s. 137-158). İstanbul: Papatya.
- YILDIRIM, A. ve ŞİMŞEK, H. (2011). *Sosyal Bilimlerde Nitel Araştırma Yöntemleri* (8. bs). Ankara: Seçkin Yayıncılık.

- YILDIRIM, A. ve ŞİMŞEK, H. (2013). *Sosyal Bilimlerde Nitel Araştırma Yöntemleri* (9. bs). Ankara: Seçkin Yayıncılık.
- YILMAZ, A. (2017). *Yapay Zekâ*. (2. bs). İstanbul: Kodlab.
- YILMAZEL, Ö. (2019). Büyük Veri ve Endüstri 4.0, Çoban, S., Ağacakaya, S., Karakoç, E., Karasioğlu, F., Çoban, A. (Der.), *Sosyal, Beşeri ve İdari Bilimler Alanında Araştırma ve Değerlendirmeler Cilt 1* içinde (s. 157-170). Ankara: Gece Akademi
- YİĞİTBAŞI, İ. (2015). Bilginin Korunması, Gülseçen, S. (Der.), *Bilgi Yönetimi: bilgi tüketicileri, büyük veri, inovasyon ve kurumsal zekâ* içinde (s. 57-78). İstanbul: Papatya.
- ZENCİRKIRAN, M. (2018). *Sosyoloji* (7. bs). Bursa: Dora.
- Süreli Yayın**
- ALAVI, R., ISLAM, S., MOURATIDIS, H. ve LEE, S. (2015). *Managing Social Engineering Attacks- Considering Human Factors and Security Investment*. Proceedings of the Ninth International Symposium on Human Aspects of Information Security & Assurance (HAISA 2015), 161-171.
- AVŞAR, Z. (2014). Medya Okuryazarlığı. *İletişim ve Diplomasi*, 2. <http://www.iletisimvediplomasi.com/medya-okuryazarligi-prof-dr-zakir-avsar/> (Erişim: 15.02.2019).
- BAHRIN, M. A. K., OTHMAN, M. F., AZLI, N. H. N., TALİB, M. F. (2016). Industry 4.0: A Review on Industrial Automation and Robotic. *Jurnal Teknologi*, 78(6-13), 137-143. DOI: 10.11113/jt.v78.9285 https://www.researchgate.net/publication/304614356_Industry_40_A_review_on_industrial_automation_and_robotic (Erişim: 30.05.2019).
- BARBER, R. (2001). Social engineering: A People Problem? *Elsevier, Network Security*, 2001(7), 9-11. [https://doi.org/10.1016/S1353-4858\(01\)00716-4](https://doi.org/10.1016/S1353-4858(01)00716-4) <https://www.sciencedirect.com/science/article/pii/S1353485801007164> (Erişim: 11.01.2019).
- BARRETT, N. (2003). Penetration testing and social engineering: Hacking the weakest link. *Elsevier, Information Security Technical Report*, 8(4), 56-64. [https://doi.org/10.1016/S1363-4127\(03\)00007-4](https://doi.org/10.1016/S1363-4127(03)00007-4) <https://www.sciencedirect.com/science/article/pii/S1363412703000074> (Erişim: 11.01.2019).
- BERNIATO, S. (2018). Aktif Savunma ve Karşı Hackleme Rehberi. *Harvard Business Review Türkiye*, Ağustos 2018, 50-53.

- BERNIATO, S. ve PERRY, M. (2018). Rakamlarla Güvenlik Trendleri. *Harvard Business Review Türkiye*, Ağustos 2018, 54-60.
- BOCHMAN, A. (2018). İnternet Güven(siz)liği. *Harvard Business Review Türkiye*, Ağustos 2018, 40-49.
- CONTEH, N. Y. (2016). The Dynamics of Social Engineering and Cybercrime in the Digital Age. *IRACST - International Journal of Computer Science and Information Technology & Security (IJCSITS)*, 6(1), 435-439.
- DADKHAH, M. ve QULIYEVA, A. (2014). Social engineering in academic world. *Journal of Contemporary Applied Mathematics*, 4(2), 3-5.
<http://journalcam.com/wp-content/uploads/2018/01/1.pdf>
 (Erişim: 08.01.2019).
- EĞRİSÖĞÜT, A. T. ve KAZAN, R. (2007). Bulaşık makinesinin bulanık mantık ile modellenmesi. *Mühendis ve Makine*, 48(565), s. 3-8.
https://www.mmo.org.tr/sites/default/files/deb1c54814305ca_ek.pdf
 (Erişim: 24.05.2019).
- EMERALDINSIGHT (2015). "Are you being manipulated?: Social marketing, social engineering and democratic government", *Strategic Direction*, Vol. 31 Issue: 7, 14-16. <https://doi.org/10.1108/SD-05-2015-0077>
- FLORES, W. R. ve EKSTEDT, M. (2016). Shaping intention to resist social engineering through transformational leadership, information security culture and awareness. *Elsevier, Computers & Security*, 59, 26-44.
<http://dx.doi.org/10.1016/j.cose.2016.01.004>
https://ac.els-cdn.com/S0167404816000067/1-s2.0-S0167404816000067-main.pdf?_tid=3d24241e-b41f-4443-a4c0-ea00b85d5963&acdnat=1539254119_4f6065981fc5e120c52a79d2bc7a85cb
 (Erişim: 10.01.2019)
- GLADDEN, M. E. (2019). Anthropology of Technologically Posthumanized Future Societies. *MDPI, Social Sciences*, 8(148), doi:10.3390/socsci8050148
- GOLD, S. (2010). Social engineering today: psychology, strategies and tricks. *Elsevier, Network Security*, 2010(11), 11-14.
[https://doi.org/10.1016/S1353-4858\(10\)70135-5](https://doi.org/10.1016/S1353-4858(10)70135-5)
https://ac.els-cdn.com/S1353485810701355/1-s2.0-S1353485810701355-main.pdf?_tid=76a6974f-7565-421a-8fa6-f40e8b843b29&acdnat=1539254429_8eca1e85cab21a7a2ddab5c8cb575c7
 (Erişim: 10.01.2019)
- HATFIELD, J. M. (2018). Social engineering in cybersecurity: The evolution of a concept. *Computer & Security*, 73, 102-113.
<https://www.sciencedirect.com/science/article/pii/S0167404817302249>
 (Erişim: 08.01.2019).

- JAIN,A., TAILANG, H., GOSWAMI, H., DUTTA, S., SANKHLA, M.S.ve KUMAR, R. (2016). Social Engineering: Hacking a Human Being through Technology. *IOSR Journal of Computer Engineering (IOSR-JCE)*, 18(5), 94-100.
DOI: 10.9790/0661-18050594100
https://www.researchgate.net/profile/Rajeev_Kumar153/publication/309234725_Social_Engineering_Hacking_a_Human_Being_through_Technology/links/5806568908aeb85ac85f4742/Social-Engineering-Hacking-a-Human-Being-through-Technology.pdf (Eriřim: 09.01.2019).
- KARAARSLAN, E. ve AKBAř, M., F. (2017). Blokzincir Tabanlı Siber Güvenlik Sistemleri. *Uluslararası Bilgi Güvenlięi Mühendislięi Dergisi*, 2(3), 16-21.
- KESER, H. ve GÜLDÜREN, C. (2015). Bilgi Güvenlięi Farkındalık Ölçeęi (BGFÖ) Geliřtirme Çalışması. *K. Ü. Kastamonu Eęitim Dergisi*, 23 (3), 1167-1184.
- KROMBHOLZ, K., HOBEL, H., HUBER, M. ve WEIPPL, E. (2015). Advanced social engineering attacks. *Journal of Information Security and Applications*, 22, 113-122.
<https://www.sciencedirect.com/science/article/pii/S2214212614001343/pdf?md5=bbbef8df938fa6a1cda6ff7a33c33709&pid=1-s2.0-S2214212614001343-main.pdf> (Eriřim: 08.01.2019).
- KUMAR, A., CHAUDHARY, M. ve KUMAR, N. (2015). Social Engineering Threats and Awareness: A Survey. *European Journal of Advances in Engineering and Technology*, 2(11), 15-19.
<http://www.ejaet.com/PDF/2-11/EJAET-2-11-15-19.pdf> (Eriřim: 09.01.2019).
- KUMAR, V., CHAISIRI, S. ve KO, R. (2017). A data-centric view of cloud security.
- MAJOR, S. D. A. (2009). Social Engineering: hacking the wetware! *Information Security Journal: A Global Perspective*, 18(1), 40-46,
DOI: 10.1080/19393550802623214
- MANSOUR, R. F. (2016). Understanding how big data leads to social networking vulnerability. *Elsevier, Computers in Human Behavior*, 57, 348-351.
https://ac.els-cdn.com/S0747563215303265/1-s2.0-S0747563215303265-main.pdf?_tid=cd34b049-1f04-47c8-b779-404379feb9ba&acdnat=1539254554_e540b26b97c0094ad7255fcf26749607 (Eriřim: 10.01.2019).
- MERWE, J. ve MOUTON, F. (2017). *Mapping the Anatomy of Social Engineering Attacks to the Systems Engineering Life Cycle*. Proceedings of the Eleventh International Symposium on Human Aspects of Information Security & Assurance (HAISA 2017)

- MOSKVITCH, K. (2017). When Machinery Chats, *Engineering & Technology*, March 2017, 12, 68-70, www.EandTmagazine.com
- MOUTON, F., MALAN, M. M., KIMPPA, K. K. ve VENTER, H. S. (2015). Necessity for ethics in social engineering research. *Computer & Security*, 55, 114-127.
<https://doi.org/10.1016/j.cose.2015.09.001>
<https://www.sciencedirect.com/science/article/pii/S0167404815001224/pdf?md5=66e53de8b658c89b80c5afe0f7fae020&pid=1-s2.0-S0167404815001224-main.pdf> (Eriřim: 08.01.2019).
- ÖZER, M. A. (2012). Bir Modern Yönetim Teknięi Olarak Algılama Yönetimi ve İç Güvenlik Hizmetleri. *Karadeniz Arařtırmaları*, 33, 147-180.
http://www.karam.org.tr/Makaleler/659211216_012%20ozer.pdf (Eriřim: 02.01.2019).
- ÖZTEMEL, E. (2018). Endüstri 4.0 ve Yapay Zekâ. *Tübitak Bilim ve Teknik*, Haziran 2018, Sayı 607, 78-85.
- PAĞDA, Z. (2018). Yapay Zekâ ve İnsansız İnsan Kaynakları. *Harvard Business Review Türkiye*, Ağustos 2018, 103-107.
- SADIKU, M. N., SHADARE, A. E. ve MUSA, S. M. (2016). Social Engineering: An Introduction. *Journal of Scientific and Engineering Research*, 3(3), 64-66.
- SCOTT SEİDENBERGER, S. (2016). A New Role For Human Resource Managers: Social Engineering Defense. *Cornell HR Review*.
<https://digitalcommons.ilr.cornell.edu/cgi/viewcontent.cgi?article=1091&context=chrr> (Eriřim:30.01.2019)
- ŞERBAN, V. G. ve ŞERBAN, O. (2014). Social Engineering a General Approach. *Informatica Economică*, 18(2) , 5-14.
doi:10.12948/issn14531305/18.2.2014.01
<http://www.revistaie.ase.ro/content/70/01%20-%20Greavu,%20Serban.pdf> (Eriřim: 07.01.2019).
- TAYOURI, D. (2015). The human factor in the social media security – combining education and technology to reduce social engineering risks and damages. *Elsevier, Procedia Manufacturing*, 3, 1096-1100.
doi: 10.1016/j.promfg.2015.07.181
https://ac.els-cdn.com/S2351978915001821/1-s2.0-S2351978915001821-main.pdf?_tid=76223506-f0ee-4e6a-bf57-af80c71497c8&acdnat=1539254211_d161ad574535feadc73dc1ef57258eb5 (Eriřim: 10.01.2019).

YILDIRIM, A. (1999). Nitel Araştırma Yöntemlerinin Temel Özellikleri ve Eğitim Araştırmalarındaki Yeri ve Önemi. *Eğitim ve Bilim*, 23(112). eb.ted.org.tr/index.php/EB/article/download/5326/1485 (Erişim: 25.06.2019).

WANG, S., WAN, J., ZHANG, D., LI, D., ZHANG, C. (2016). Towards smart factory for industry 4.0: a self-organized multi-agent system with big data based feedback and coordination. *Computer Networks, ScienceDirect, Elsevier*, 104, 158-168. <https://www.sciencedirect.com/science/article/pii/S1389128615005046> (Erişim: 12.05.2019).

ZADEH, L. A. (1965). Fuzzy Sets. *Information and Control*, 8, s. 338-353. <https://people.eecs.berkeley.edu/~zadeh/papers/Fuzzy%20Sets-Information%20and%20Control-1965.pdf> (Erişim: 24.05.2019).

İnternet

ABBAK, C. (23 Şubat 2015). Nitel Araştırma Yöntemlerinde Örneklem Seçimi. <https://www.slideshare.net/canabbak/ntel-aratirma-yntemlernde-rneklem-sem> (Erişim: 18.06.2019).

ACM Council. ACM code of ethics and professional conduct. <http://www.acm.org/about/code-of-ethics> (Erişim: 08.01.2019).

AHMED, N. (2013). Social Engineering. https://courses.cs.ut.ee/MTAT.03.246/2014_spring/uploads/Main/Lect12.pdf (Erişim: 25.10.2018).

ANDREWS, C. (2017, Mayıs 17). Are political social media campaigns a threat to democratic elections? <https://eandt.theiet.org/content/articles/2017/05/are-political-social-media-campaigns-a-threat-to-democratic-elections/> (Erişim: 07.01.2018)

ASHFORD, W. (2018, Nisan 09). More than one in 10 employees fall for social engineering attacks. *Computer Weekly*. <https://www.computerweekly.com/news/252438572/More-than-one-in-10-employees-fall-for-social-engineering-attacks> (Erişim: 24.12.2018)

BAHETI, R. ve GILL, H. (2011). Cyber-physical Systems. <http://www.ieeecss.org/sites/ieeecss.org/files/documents/IoCT-Part3-02CyberphysicalSystems.pdf> (Erişim: 23.05.2019).

BANGER, G. (2017a). İşletme Nasıl Dönüşecek? <https://bizobiz.net/isletme-nasil-donusecek/> (Erişim: 10.05.2019).

BANGER, G. (2017b). Yakın Geleceğin Akıllı Makineleri <https://bizobiz.net/yakin-gelecegin-akilli-makineleri/> (Erişim: 10.05.2019).

- BANGER, G. (2018a). Endüstri 4.0 Konusunda Yanlışlar ve Yanılsamalar. <https://bizobiz.net/endustri-4-0-konusunda-yanlislar-ve-yanilsamalar> (Erişim: 09.05.2019).
- CORY, N., D. Atkinson, R. D., Castro, D. (27 Mayıs 2019). Principles and Policies for “Data Free Flow With Trust”, ITIF (Information Technology & Innovation Foundation). <https://itif.org/publications/2019/05/27/principles-and-policies-data-free-flow-trust> (Erişim: 26.10.2019).
- CISCO (2016). Internet of Things. <https://www.cisco.com/c/dam/en/us/products/collateral/se/internet-of-things/at-a-glance-c45-731471.pdf> (Erişim: 15.05.2019).
- CLARK, J. W. (2017). *Trends in Social Engineering: Securing the weakest link*. Software Engineering Institute, Carnegie Mellon University <https://www.nsi.org/Impact17Presentations/J.Clark.pdf> (Erişim: 09.01.2019).
- DATA MANAGEMENT (2019) http://digital-library.theiet.org/docserver/fulltext/books/po/pbpo110e/PBPO110E_ch25.pdf?expires=1539160911&id=id&accname=378948&checksum=974BCFFC641D7546E184FDBDCA7F2DEC (Erişim: 28.03.2019).
- DOMO (2019). Data Never Sleeps 6.0. <https://www.domo.com/learn/data-never-sleeps-6> (Erişim: 08.05.2019).
- GELECEK HANE. Nesnelerin İnterneti İle Gelen 4. Endüstri Devrimi. <https://www.gelecekhane.com/nesnelerin-interneti-ile-gelen-4-endustri-devrimi/> (Erişim: 11.05.2019).
- GUENTHER, M. (2001). Social Engineering. Security Awareness Series. <http://www.iwar.org.uk/comsec/resources/security-awareness/social-engineering-generic.pdf> (Erişim: 12.02.2019).
- GULATI, R. (2003). *GIAC Security Essentials (GSEC) Certification Practical Assignment Version 1.4b – Option 1*. SANS Institute InfoSec Reading Room <https://www.sans.org/reading-room/whitepapers/engineering/threat-social-engineering-defense-1232> (Erişim: 29.01.2019).
- HACİNECİPOĞLU, A. (27 Mart 2017). Industry 4.0, Smart Factories and Autonomous Mobile Robots. Milvus Robotics. <http://milvusrobotics.com/blog/industry40-smart-factories-and-autonomous-mobile-robots> (Erişim: 30.05.2019).
- HAZAR, S. (2019). Bilimsel Araştırma Yöntemleri <https://www.slideserve.com/blue/bilimsel-arastirma-y-ntemleri> (Erişim: 12.12.2019).

- HELLER, M. (2018, Nisan 25). Social engineering attacks need real-world 2FA.
<https://searchsecurity.techtarget.com/news/252439882/Rachel-Tobac-Social-engineering-attacks-need-real-world-2FA> (Eriřim: 25.12.2018).
- HENNINGSEN, E. K. (2013). *The Defense and Popularity of Social Engineering in Norway*. Master's Thesis, Master of Science in Information Security, Department of Computer Science and Media Technology, Gjøvik University College, Norway.
<https://brage.bibsys.no/xmlui/bitstream/handle/11250/144040/EKHenningsen.pdf?sequence=1> (Eriřim: 31.01.2019).
- HOWSTUFFWORKS.com,
<https://science.howstuffworks.com/life/inside-the-mind/human-brain/brain1.htm> (Eriřim:14.06.2019).
- http://ayancikanadolu.meb.k12.tr/meb_iys_dosyalar/57/02/325814/dosyalar/2020_03/06141928_denetleyici_ve_duzenleyici_sistemler.pdf (Eriřim:13.06.2019).
- <http://farabi.sutef.gen.tr/bulanik/bulanik/bolum02.htm> (Eriřim: 20.05.2019).
- <http://firelog.com.tr/5651-sayili-kanun-nedir/> (Eriřim:19.03.2019).
- <http://toplummuhendisligi.com/toplum-muhendisligi/> (Eriřim:14.02.2019).
- <http://www.belgelendirme.com.tr/> (Eriřim: 19.03.2019).
- <http://www.isaca.org/Knowledge-Center/Documents/Glossary/glossary.pdf>
(Eriřim: 27.03.2019).
- <http://www.mevzuat.gov.tr/MevzuatMetin/1.5.6698.pdf> (Eriřim: 01.04.2019).
- <http://www.mevzuat.gov.tr/MevzuatMetin/1.5.5070.pdf> (Eriřim: 02.04.2019).
- <https://berovaklinik.com/2014/12/19/sinir-hucresi-noron/> (Eriřim:13.06.2019).
- <https://gdpr-info.eu/issues/> (Eriřim: 18.11.2019)
- <https://peerscientist.com/news/neurons-called-the-dendrites-arent-the-passive-receivers-heres-the-evidence/> (Eriřim:14.06.2019).
- <https://searchsecurity.techtarget.com/definition/social-engineering>
(Eriřim: 03.12.2018).
- <https://trendwatching.com/> Walmart unveils futuristic AI-powered store.
- <https://www.bgasecurity.com/egitim/kurumsal-some-egitimleri/>
(Eriřim: 08.04.2019).

<https://www.bilgi.edu.tr/tr/akademik/meslek-yuksekokulu/bilgisayar-teknolojileri/bilgi-guvenligi-teknolojisi/hakkinda/> (Eriřim: 18.03.2019).

<https://www.cisco.com>
<https://www.cisco.com/c/en/us/solutions/internet-of-things/overview.html>
 (Eriřim: 15.05.2019).

<https://www.cognifit.com/tr/science/didyou-know/neurons> (Eriřim: 13.09.2018)

<https://www.dunya.com/tekno-trend/siber-saldirilarin-yeni-kiskaci-sosyal-muhendislik-haberi-377630> (Eriřim: 21.02.2020).

<https://www.egitimler.info/nedir-ne-demektir/butuncu-yaklasim-nedir/> (Eriřim: 14.06.2019).

<https://www.ge.com/europe/industrial-internet> (Eriřim: 16.05.2019).

<https://www.haberturk.com/uber-in-piyasa-degeri-120-milyar-dolara-yukseldi-2181193-ekonomi> (Eriřim: 01.07.2019).

<https://www.investopedia.com/terms/s/social-engineering.asp> (Eriřim: 11.10.2018).

<https://www.iso.org/isoiec-27001-information-security.html> (Eriřim: 26.03.2019).

<https://www.knowbe4.com/what-is-social-engineering/> (Eriřim: 03.12.2018).

<https://www.mevzuat.gov.tr/MevzuatMetin/1.5.5237.pdf> (Eriřim: 08.04.2019).

<https://www.sis.se/api/document/preview/916656/> (Eriřim: 26.03.2019).

<https://www.social-engineer.org/about/> (Eriřim: 23.11.2018).

<https://www.social-engineer.org/framework/attack-vectors/how-can-you-protect-yourself-against-common-attacks/> (Eriřim: 06.12.2018).

<https://www.social-engineer.org/framework/psychological-principles/neuro-linguistic-programming-nlp/> (Eriřim: 07.12.2018).

<https://www.thefreedictionary.com/Information+systems+security>
 (Eriřim: 27.03.2019).

<https://www.tsys.com/> *Your Guide to Social Engineering: A Dangerous Security Risk.* (Eriřim: 31.01.2019).

https://www.turkcebilgi.com/bütüncül_yaklaşım (Eriřim: 14.06.2019).

<https://www.wikisitesi.com/butuncu-yaklasim-gestalt-kurami-psikolojisi.html>
 (Eriřim: 01.07.2019).

<https://www.webroot.com/us/en/resources/tips-articles/what-is-social-engineering>
(Eriřim: 27.12.2018).

HUNTER, P. (2013). Engineering & Technology September 2013,
www.EandTmagazine.com.
<http://digital-library.theiet.org/docserver/fulltext/et/8/8/20130809.pdf?expires=1539156758&id=id&accname=378948&checksum=7E6BED2BF56D78B701A9B92A65288530> (Eriřim: 25.03.2019).

HÜRRİYET GAZETESİ (2018, 18 Temmuz). Teknoloji. Hacker'lar özellikle neden yazıcılara saldırıyor? http://www.hurriyet.com.tr/teknoloji/hackerlar-ozellikle-neden-yazicilara-saldiriyor-40900405?utm_campaign=Bundle&utm_medium=referral&utm_source=Bundle (Eriřim: 19.03.2019).

HÜRRİYET GAZETESİ (2018, 21 Temmuz). Teknoloji. Dünya Kupası boyunca futbolseverler siber saldırıya maruz kaldı. http://www.hurriyet.com.tr/teknoloji/dunya-kupasi-boyunca-futbolseverler-siber-saldiriya-maruz-kaldi-40904375?utm_campaign=Bundle&utm_medium=referral&utm_source=Bundle (Eriřim: 19.03.2019).

HÜRRİYET TEKNOLOJİ (25.07.2018). Araç paylaşım uygulamalarındaki güvenlik açıklarına dikkat. http://www.hurriyet.com.tr/teknoloji/arac-paylasim-uygulamalarindaki-guvenlik-aciklarina-dikkat-40907937?utm_campaign=Bundle&utm_medium=referral&utm_source=Bundle (Eriřim: 09.05.2019).

HÜRRİYET TEKNOLOJİ (27.08.2018). IoT'ye yatırım yapan şirketler güvenliği göz ardı ediyor. http://www.hurriyet.com.tr/teknoloji/iotye-yatirim-yapan-sirketler-guvenligi-goz-ardi-ediyor-40937857?utm_campaign=Bundle&utm_medium=referral&utm_source=Bundle (Eriřim: 04.09.2018).

IEEE Board of Directors. IEEE policies.
http://www.ieee.org/documents/ieee_policies.pdf (Eriřim: 08.01.2019).

IRANI, D., BALDUZZI, M., BALZAROTTI, D., KIRDA, E. and PU, C. (2011). *Reverse Social Engineering Attacks in Online Social Networks*.
<https://seclab.ccs.neu.edu/static/publications/dimva2011osn.pdf>
(Eriřim: 31.01.2019).

ibb.gov.tr/sites/atikyonetimi/Documents/resim/mudurluk/doc/mantiksalyaklasim.ppt
(Eriřim: 21.11.2018).

- JOHNSON, S. (2018). Social engineering: You got nailed!
<https://searchsecurity.techtarget.com/feature/Social-engineering-You-got-nailed> (Eriřim: 27.12.2018).
- KULABAŐ, A. (26 Temmuz 2017). Endüstri 4.0! Dijital Zihniyet!
<https://medium.com/bili%C5%9Fim-hareketi/end%C3%BCstri-4-0-dijital-zihniyet-5fe9357ead9d> (Eriřim: 24.05.2019).
- LEWIS, N. (2018). How social engineering attacks have embraced online personas.
<https://searchsecurity.techtarget.com/tip/How-social-engineering-attacks-have-embraced-online-personas> (Eriřim: 26.12.2018).
- MARR, B. (20 Haziran 2016). What Everyone Must Know About Industry 4.0.
 Forbes.
<https://www.forbes.com/sites/bernardmarr/2016/06/20/what-everyone-must-know-about-industry-4-0/#434bace2795f> (Eriřim: 12.05.2019).
- MARR, B. (21 Mayıs 2018b). How Much Data Do We Create Every Day? The Mind-Blowing Stats Everyone Should Read. *Forbes*,
<https://www.forbes.com/sites/bernardmarr/2018/05/21/how-much-data-do-we-create-every-day-the-mind-blowing-stats-everyone-should-read/#43c08fb060ba> (Eriřim: 08.05.2019).
- MELANSON, T. (2018). What Industry 4.0 Means for Manufacturers.
<https://aethon.com/mobile-robots-and-industry4-0/> (Eriřim: 30.05.2019).
- METASPLOIT (2019). *Best Practices for Social Engineering Attacks*.
https://www.rapid7.com/docs/download/Metasploit_Best_Practices_for_Social_Engineering_Attacks.pdf (Eriřim: 09.02.2019).
- MIMIC TECHNOLOGIES (2013). *Social Engineering–Risks, Techniques and Safeguards*.
<https://www.itegria.com/wp-content/uploads/2014/03/ItegriaSocialEngineering.pdf> (Eriřim: 01.02.2019).
- MOBİLYA DEKORASYON (28 Haziran 2016). Tüm Boyutlarıyla Endüstri 4.0 Devrimi.
<http://www.mobilyadergisi.com.tr/haber/tum-boyutlariyla-endustri-40-devrimi> (Eriřim: 10.05.2019).
- NELMIA ROBOTICS INSIGHT. Robots and Industry 4.0
<http://www.automaticaeinstrumentacion.com/es/downloads2/nelmia-michael-laughlin.compressed.pdf> (Eriřim:30.05.2019).
- NETWORK SECURITY, http://digital-library.theiet.org/docserver/fulltext/books/te/sbte501e/SBTE501E_ch17.pdf?expires=1539157579&id=id&accname=378948&checksum=DE51A42DD18C136C1492DCB6D62BF708 (Eriřim: 28.03.2019).

- NIST Engineering Laboratory. Cyber-Physical Systems.
<https://www.nist.gov/el/cyber-physical-systems> (Eriřim: 29.05.2019).
- NYIRAK, A. (2018). The Attack Cycle.
<https://www.social-engineer.org/framework/attack-vectors/attack-cycle/>
 (Eriřim: 06.12.2018).
- OKENYI, P. O. ve OWENS, T. J., (2007). *On The Anatomy of Human Hacking*.
<https://bura.brunel.ac.uk/bitstream/2438/2496/4/On%20The%20Anatomy%20of%20Human%20Hacking.pdf> (Eriřim: 10.02.2019).
- OKS, S. J. (2016). Cyber-physical systems - Can technology be smart?
https://www.academia.edu/36555047/Cyber-physical_systems_-_Can_technology_be_smart (Eriřim: 28.05.2019).
- OKYAY, Z., B. (18 Ekim 2018). This is what a smart city should do for its people.
World Ecomomic Forum.
<https://www.weforum.org/agenda/2018/10/smart-city-people-canakkale-connected-iot-urban/> (Eriřim: 13.05.2019).
- ÖZOĞUL, E. M. (21 Temmuz 2017). Bu Yıl 100 Milyon Konaklamayı Gececek Olan Airbnb, Otel Endüstrisini Tehdit Ediyor.
<https://pazarlamasyon.com/yil-100-milyon-konaklamayi-gececek-olan-airbnb-otel-endustrisini-tehdit-ediyor/> (Eriřim: 01.07.2019).
- PESEN, M. M. (2015). Bilgi Güvenlięi Nedir ve Nasıl Sınıflandırılır?
<https://www.sibergah.com/genel/bilgi-guvenligi-nedir-ve-nasil-siniflandirilir/>
 (Eriřim: 18.03.2019).
- PHILPUT, J. *Tactics to Improve Organizational Security Acceptance*.
https://media.blackhat.com/bh-us-12/Briefings/Philput/BH_US_12_Philput_Hacking_The_Corporate_Mind_WP.pdf
 Hacking the Corporate Mind: Using Social Engineering
 (Eriřim: 30.01.2019).
- PTOLEMY PROJECT (2012). Heterogenous Modeling and Design.
<https://ptolemy.berkeley.edu/projects/cps/> (Eriřim: 29.05.2019).
- ROUSE, M. (2018a). Social Engineering. *Search Security*.
<https://searchsecurity.techtarget.com/definition/social-engineering>
 (Eriřim: 24.12.2018)
- ROUSE, M. (2018b). two-factor authentication (2FA).
<https://searchsecurity.techtarget.com/definition/two-factor-authentication>
 (Eriřim: 29.03.2019).

- RTÜK (11.10.2016). Medya Okuryazarlığı Nedir?
https://www.medyaokuryazarligi.gov.tr/menu_goster.php?Guid=B7AA7732-1593-4B32-BDE5-D76E64C2A5FA&MenuId=2 (Erişim: 14.02.2019).
- SAVAGE, M. (2018). Gaining awareness to prevent social engineering techniques, attacks. <https://searchsecurity.techtarget.com/magazineContent/Gaining-awareness-to-prevent-social-engineering-techniques-attacks> (Erişim: 26.12.2018).
- SEVİNÇ, A. (19 Temmuz 2018). Yapay Zekâ Yaşam Kalitesini Artıracak. Genç Nesil, Güncel İçerikler. <http://magg4.com/asrin-sevinc-yapay-zeka-yasam-kalitesini-artiracak/> (Erişim: 07.05.2019).
- SHACKLEFORD, D. (2018). Social engineering penetration testing: Four effective twchniques. <https://searchsecurity.techtarget.com/tip/Social-engineering-penetration-testing-Four-effective-techniques> (Erişim: 26.12.2018).
- SHETTY, D. (2019). Social Engineering. <https://www.exploit-db.com/docs/english/18135-social-engineering---the-human-factor.pdf> (Erişim: 17.01.2019).
- ŞENGÜN, G. (2018). NAT-Network Address Translation nedir ve nasıl çalışır? <https://medium.com/@gokhansengun/nat-network-address-translation-nedir-ve-nasil-calisir-a2c8b6291de8> (Erişim: 16.02.2019).
- TÜRK DİL KURUMU (2018). http://tdk.gov.tr/index.php?option=com_bts&view=bts&kategori=verilst&ayn1=bas&kelime1=stereotip (Erişim: 20.11.2018).
- U.S. DEPARTMENT OF HOMELAND SECURITY. Deception Detection: Identifying Hostile Intent. <https://www.dhs.gov/science-and-technology/deception-detection> (Erişim: 01.02.2019).
- WEBER, V. (16 Nisan 2019). Smart cities must pay more attention to the people who live in them. *World Ecomomic Forum*. <https://www.weforum.org/agenda/2019/04/why-smart-cities-should-listen-to-residents/> (Erişim: 13.05.2019).
- WILCOX, H., BHATTACHARYA, M. ve ISLAM, R. (2014) . *Social Engineering through Social Media: An Investigation on Enterprise Security*. <http://csusap.csu.edu.au/~mbhattac/pub/ATIS-2014-HW-MB-RI.pdf> (Erişim: 30.01.2019).
- WORLD ECONOMIC FORUM (6 Şubat 2019). Internet of Things, Robotics and Smart Cities. <https://www.weforum.org/communities/internet-of-things-robotics-and-smart-cities> (Erişim: 13.05.2019).

YILDIRIM, Ö. (2018). Sosyal Algı Nedir? Felsefe.
<http://www.felsefe.gen.tr/psikoloji/sosyal-algi-nedir-ne-demektir.asp>
 (Erişim: 14.02.2019).

Raporlar ve Dokümanlar

BİRLEŞİK DEVLETLER ULUSAL İSTİHBARAT YÖNETİM OFİSİ VE İÇ
 GÜVENLİK DEPARTMANI, 2017 Kamu-Özel Analitik Değişim Programı
 (Office of the Director of National Intelligence and the Department of
 Homeland Security, 2017 Public-Private Analytic Exchange Program, *The
 Future of Ransomware and Social Engineering*)
[https://www.dni.gov/files/PE/Documents/6---2017-AEP_The-Future-of-
 Ransomware-and-Social-Engineering.pdf](https://www.dni.gov/files/PE/Documents/6---2017-AEP_The-Future-of-Ransomware-and-Social-Engineering.pdf) (Erişim: 15.01.2019).

CAZIER ve BOTELHO (2007). *Social Engineering's Threat to Public Privacy*. The
 6th Annual Security Conference. (April 11-12, 2007). Las Vegas.
<http://www.isy.vcu.edu/~gdhillon/Old2/secconf/secconf07/PDFs/51.pdf>
 (Erişim: 16.01.2019).

DELOITTE (2017a). Guiding the IoT Safety, Deloitte University Press,
 dupress.deloitte.com
[https://www2.deloitte.com/content/dam/Deloitte/tr/Documents/technology-
 media-telecommunications/guiding-the-IoT-to-safety.pdf](https://www2.deloitte.com/content/dam/Deloitte/tr/Documents/technology-media-telecommunications/guiding-the-IoT-to-safety.pdf)
 (Erişim: 15.05.2019).

DELOITTE (2017b). Revolution: The Fourth Revolution is now: are you ready?
 Deloitte University Press, dupress.deloitte.com
[https://www2.deloitte.com/content/dam/Deloitte/tr/Documents/technology-
 media-telecommunications/gx-strategy-ops-the-fourth-revolution-now.pdf](https://www2.deloitte.com/content/dam/Deloitte/tr/Documents/technology-media-telecommunications/gx-strategy-ops-the-fourth-revolution-now.pdf)
 (Erişim: 15.05.2019).

DIMENSIONAL RESEARCH (2011). *The Risk Of Social Engineering On
 Information Security: A Survey Of It Professionals*.
[https://www.stamx.net/files/The-Risk-of-Social-Engineering-on-Information-
 Security.pdf](https://www.stamx.net/files/The-Risk-of-Social-Engineering-on-Information-Security.pdf) (Erişim: 01.02.2019).

[http://www.eventtracker.com/eventtracker/media/eventtracker/files/collateral/verizon
 -data-breach-2013.pdf](http://www.eventtracker.com/eventtracker/media/eventtracker/files/collateral/verizon-data-breach-2013.pdf) (Erişim: 21.03.2019).

https://enterprise.verizon.com/resources/reports/2009_databreach_rp.pdf (Erişim:
 21.03.2019).

https://enterprise.verizon.com/resources/reports/2017_dbir.pdf (Erişim: 21.03.2019).

[https://enterprise.verizon.com/resources/reports/data-breach-investigation-
 report_2015.pdf](https://enterprise.verizon.com/resources/reports/data-breach-investigation-report_2015.pdf) (Erişim: 21.03.2019).

https://enterprise.verizon.com/resources/reports/DBIR_2016_Report.pdf
(Eriřim: 21.03.2019).

https://enterprise.verizon.com/resources/reports/DBIR_2018_Report_execsummary.pdf (Eriřim: 21.03.2019).

<https://www.nu.nl/files/Verizon.pdf> (Eriřim: 21.03.2019).

https://www.wired.com/images_blogs/threatlevel/2010/07/2010-Verizon-Data-Breach-Investigations-Report.pdf (Eriřim: 21.03.2019).

https://www.wired.com/images_blogs/threatlevel/2011/04/Verizon-2011-DBIR_04-13-11.pdf (Eriřim: 21.03.2019).

https://www.wired.com/images_blogs/threatlevel/2012/03/Verizon-Data-Breach-Report-2012.pdf (Eriřim: 21.03.2019).

International Organisation for Standardisation. Information Technology – Security Techniques – Code of Practice for Information Security Controls. ISO/IEC 27002:2013.

ÖZMEN, C. (2018). *Lisansüstü Programlara Öğrenci Alımlarında Bulanık Mantık Yaklaşımı Kullanılarak Hazırlanmış Bir Model Önerisi*, Giresun Üniversitesi, Sosyal Bilimler Enstitüsü, Seminer Ödevi.

PROOFPOINT, INC. (2016). *The Human Factor (Research Report)*.

RAJ SAMANI, R., ve MCFARLAND, C., (2015). *Hacking The Human Operating System: the role of social engineering within cybersecurity*. Intel Security (Report).

ULUSAL SİBER GÜVENLİK STRATEJİSİ RAPORU (2012). T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı ve Bilgi Güvenliği Derneği. https://www.bilgiyguvenligi.org.tr/wp-content/uploads/2016/03/Ulusal_Siber_Guvenlik_Stratejisi.pdf (Eriřim: 14.05.2019).

Fotograflar

<https://pixabay.com> (Eriřim: 15.05.2019).

<https://pixabay.com/illustrations/home-smart-automation-house-system-4100193/>
Image by mohamed Hassan from Pixabay (Eriřim: 11.03.2020).

<https://pixabay.com/photos/3d-printing-3d-printer-technology-3800204/>
Image by ZMorph3D from Pixabay (Eriřim: 11.03.2020).

<https://pixabay.com/photos/augmented-reality-medical-3d-1957411>
(Erişim: 31.05.2019).

<https://pixabay.com/photos/industry-technology-machine-3d-3225119/>
Image by Christian Reil from Pixabay (Erişim: 11.03.2020).

<https://pixabay.com/photos/smart-city-communication-network-4168483/>
Image by Tumisu from Pixabay (Erişim: 11.03.2020).

<https://searchsecurity.techtarget.com/feature/Social-engineering-You-got-nailed>
(Erişim: 03.12.2019).

<https://unsplash.com/photos/SeTgyZSgj4Y>, Photo by DynamicWang on Unsplash
(Erişim: 11.03.2020).

<https://unsplash.com/photos/YKW0JjP7rlU>, Photo by Franck V. on Unsplash
(Erişim: 28.05.2020).

<https://www.domo.com/learn/data-never-sleeps-6> (Erişim: 08.05.2019).

<https://www.facebook.com/> (Erişim: 03.12.2019).

EKLER

- **EK-1 (TR):** Doktora Tez Çalışması Alan Araştırması İçin Katılımcı Onay Formu (Türkçe)
- **EK-1 (EN):** Doktora Tez Çalışması Alan Araştırması İçin Katılımcı Onay Formu (İngilizce)
- **EK-2 (TR):** Tanım ve Kavramlar Hakkında Kısa Bilgilendirme (Türkçe)
- **EK-2 (EN):** Tanım ve Kavramlar Hakkında Kısa Bilgilendirme (İngilizce)
- **EK-3 (TR):** Mülakat Soruları (Türkçe)
- **EK-3 (EN):** Mülakat Soruları (İngilizce)



DOKTORA TEZ ÇALIŞMASI ALAN ARAŞTIRMASI İÇİN KATILIMCI ONAY FORMU

Araştırmacı : Cevdet ÖZMEN GSM: [Redacted]
Üniversite/Enstitü : Giresun Üniversitesi, Sosyal Bilimler Enstitüsü, İşletme ABD, www.giresun.edu.tr
Tez Danışmanı : Prof. Dr. Bayram KAYA GSM: [Redacted]
Araştırma Projesinin Adı : Sosyal Mühendislik Bağlamında Bilgi Güvenliğinin Endüstri 4.0 Tabanlı Sistemlere Uyarlanması

Bu araştırmaya katılmayı düşündüğünüz için teşekkür ederim. Katılımcı Onay Formundan veya size daha önce yapılmış açıklamalardan kaynaklanan sorularınız varsa, lütfen katılıp katılmayacağınıza karar vermeden önce araştırmacıya danışınız.

Araştırmanın Amacı: Bu çalışmanın amacı; yakın gelecekte yaşam akışını daha da içine alacak bir sürecin yapı taşları olan Sosyal Mühendislik, Bilgi Güvenliği ve Endüstri 4.0 ilişkisini ortaya koymaktır.

Verilerin Kullanımı: Bulgular doktora tezimin bir parçasını oluşturmak için kullanılacaktır.

Açıklama: Lütfen bu Form sayfasının tamamını okuduktan sonra en altta bulunan ilgili yerleri doldurunuz.

- Araştırma için düzenlenen bu Onay Formunu okuduğumu ve anladığımı onaylıyorum.
- Katılımımın gönüllü olduğunu ve görüşme sırasında herhangi bir sebep göstermeksizin istediğim zaman geri çekilmekte özgür olduğumu biliyorum.
- Araştırma raporlarında ismimin gizliliğinin korunacağını ve hiçbir yayında ismimin açık olarak kullanılmasının mümkün olmadığını biliyorum.
- Görüşmenin ses kaydının yapılmasına izin veriyorum.

Not (varsa):

..... Araştırmacının İmzası Cevdet ÖZMEN Araştırmacının Adı Soyadı	 Katılımcının İmzası  Katılımcının Adı Soyadı	 Görüşme Tarihi

CONSENT FORM FOR PARTICIPANT IN DOCTORAL RESEARCH STUDY

Researcher : Cevdet ÖZMEN GSM: [REDACTED]
University/Institute : Giresun University/Turkey, Social Sciences Institute, Department of Business Administration, www.giresun.edu.tr
Adviser : Prof. Dr. Bayram KAYA GSM: [REDACTED]
Title of Research Project: The Adaptation of Information Security to Industry 4.0 Based Systems in the Context of Social Engineering

Thank you for taking part in this research. If you have any questions that may arise from the Consent Form or any previous explanations already given to you, please consult with the researcher before deciding whether or not to participate.

Purpose of the Research: The aim of this study; is to reveal the relationship of Social Engineering, Information Security and Industry 4.0, which are the building blocks of a process that will encompass more the flow of life in the near future

Use of Data: The findings will be used to form part of my doctoral thesis.

Note: Please read the entire page of this Form and fill in the relevant fields at the bottom.

- I confirm that I have read and understood the Consent Form for the Research.
- I understand that my participation is voluntary and that I am free to withdraw at any time during the interview without giving any reason.
- I understand that confidentiality and anonymity will be maintained and it will not be possible to identify me in any publications.
- I consent to my interview being audio recorded.

P.S. (if any):

..... Signature of Researcher Cevdet OZMEN Name of Researcher	 Signature of Participant  Name of Participant	 Date of Interview

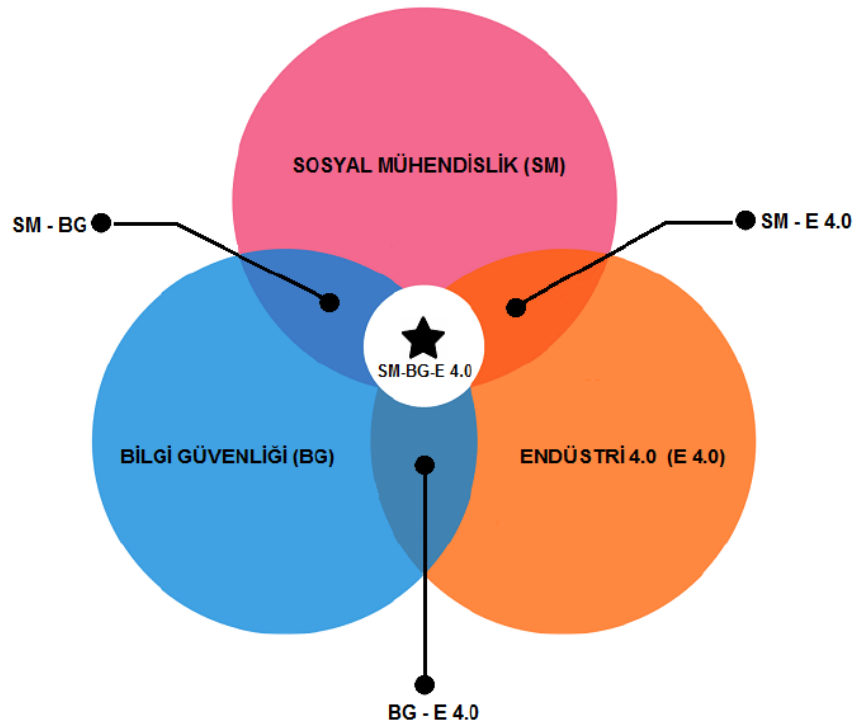
TANIM ve KAVRAMLAR HAKKINDA KISA BİLGİLENDİRME

SOSYAL MÜHENDİSLİK BAĞLAMINDA BİLGİ GÜVENLİĞİNİN ENDÜSTRİ 4.0 TABANLI SİSTEMLERE UYARLANMASI

Sosyal Mühendislik: İnsanların bilgisizliğinden, insani zayıflıklarından ve zafiyetlerinden yararlanarak; aldatma, ikna, zorlama, güvenini kazanma ve teknik/teknolojik ataklar vasıtasıyla; kişisel, kurumsal, değerli ve kritik bilgiler elde ederek; finansal kazanç elde etme, güvenli alanlara erişme ve insanların istenilen yönde aksiyon almalarını sağlamaktır.

Bilgi Güvenliği: Bilgi Güvenliği, bir varlık türü olarak bilginin izinsiz veya yetkisiz bir biçimde erişim, kullanım, değiştirilme, ifşa edilme, ortadan kaldırılma, el değiştirme ve hasar verilmesini önlemek olarak tanımlanmakta ve “gizlilik”, “bütünlük” ve “erişilebilirlik” olarak üç temel unsurdan meydana gelmektedir. Bu üç temel güvenlik ögesinden herhangi biri zarar görürse güvenlik zafiyeti oluşur (Pesen, 2015).

Endüstri 4.0: Sevinç’e (2018) göre E 4.0 en son ve ileri teknolojiyi, otomasyonu, veri alışverişini ve üretim teknolojilerini kolektif bir yapı içerisinde kullanmayı içermektedir. Böylece siber-fiziksel sistemlerin kendi kendine (self) optimizasyonun sağlanmasını öngörmektedir. Bu kapsamda E 4.0’ı, geleneksel sanayiye bilgisayarlaşma yönünde teşvik eden ve yüksek teknolojiyle donatmasını içeren proje olarak tarif etmek mümkündür. Marr (2016) E 4.0’ı, bilgisayarlar ve otomasyonun tamamen yeni bir şekilde bir araya gelerek ortaya çıkarttığı bir yapılanma olarak tanımlıyor. Makine ve robotlara insan müdahalesinin çok az olduğu, robotik öğrenmenin ön planda olduğu ve makinelerin bir birlerine uzaktan erişim sağladığı bir sistem olarak tarif ediyor.



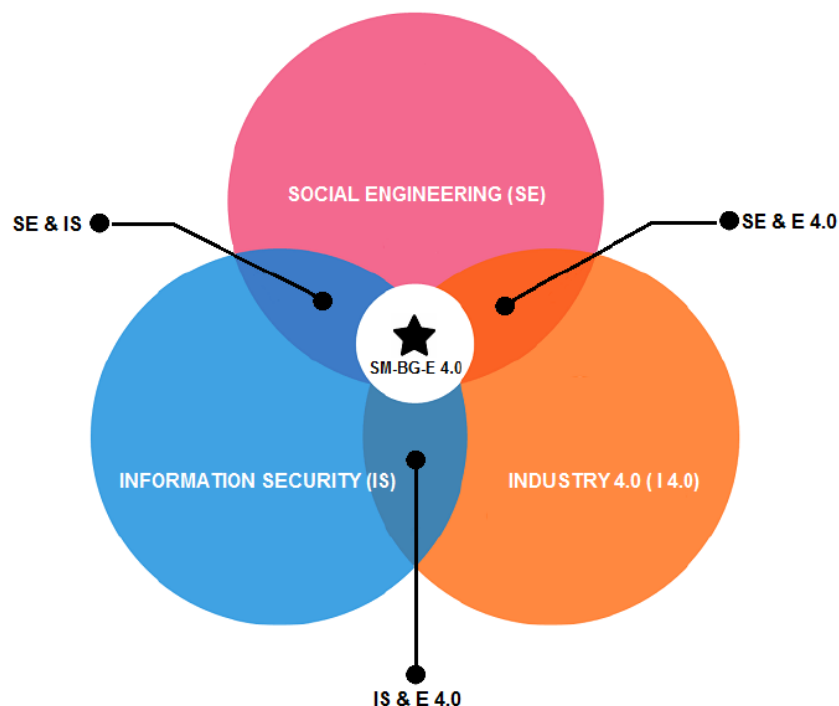
BRIEF INFORMATION ON THE DEFINITIONS AND CONCEPTS

THE ADAPTATION OF INFORMATION SECURITY TO INDUSTRY 4.0 BASED SYSTEMS IN THE CONTEXT OF SOCIAL ENGINEERING

Social Engineering: Taking advantage of people's ignorance, human weaknesses; through deception, persuasion, coercion, trust and technical/technological attacks; obtaining personal, corporate, valuable and critical information; financial gain, access to safe areas, and ensuring that people take action in the desired direction.

Information Security: Information Security is defined as preventing the unauthorized or unauthorized access, use, modification, disclosure, elimination, alteration and damage of information as an asset of three basic elements which is defined as “confidentiality”, “integrity” and “accessibility”. If any of these three basic security elements are damaged, security weakness occurs (Pesen, 2015).

Industry 4.0: According to Sevinç (2018), I 4.0 involves using the latest and advanced technology, automation, data exchange and production technologies in a collective structure. Thus, self-optimization of cyber-physical systems is provided. In this context, it is possible to describe I 4.0 as a project that encourages traditional industry to computerize and equip it with high technology. Marr (2016) describes I 4.0 as a structure that computers and automation come together in a completely new way. He describes it as a system in which human intervention in machines and robots is minimal, where robotic learning is at the forefront and machines provide remote access to each other.



Giresun Üniversitesi, Sosyal Bilimler Enstitüsü, İşletme A.B.D.
“Sosyal Mühendislik Bağlamında Bilgi Güvenliğinin Endüstri 4.0 Tabanlı
Sistemlere Uyarlanması” Başlıklı Doktora Tezi Alan Araştırması İçin
Mülakat Soruları

Araştırmacı : Cevdet ÖZMEN
 Danışman : Prof. Dr. Bayram KAYA



1) Endüstri 4.0 konusundaki yaklaşım ve görüşlerinizden bahseder misiniz?

1.1	Endüstri 4.0 ile ilgili sizce ne tür çalışmalar yapılabilir?	
1.2	Endüstri 4.0 ile ilgili yenilikleri takip etmek için neler yapılabilir?	
1.3	Endüstri 4.0 ile ilgili yeniliklerin adaptasyonu için neler yapılabilir?	
1.4	Endüstri 4.0 ile ilgili karşılaşılan ve karşılaşılabilecek riskler nelerdir ve bu risklere karşı alınabilecek önlemler nelerdir?	
1.5	Endüstri 4.0'ın uygulanmasına yönelik verebileceğiniz öneriler nelerdir?	

2) Bilgi Güvenliği konusundaki yaklaşım ve görüşlerinizden bahseder misiniz?

2.1	Bilgi Güvenliği ile ilgili sizce ne tür çalışmalar yapılabilir?	
2.2	Bilgi Güvenliği ile ilgili yenilikleri takip etmek için neler yapılabilir?	
2.3	Bilgi Güvenliği ile ilgili yeniliklerin adaptasyonu için neler yapılabilir?	
2.4	Bilgi Güvenliği ile ilgili karşılaşılan ve karşılaşılabilecek riskler nelerdir ve bu risklere karşı alınabilecek önlemler nelerdir?	
2.5	Bilgi Güvenliği'nin uygulanmasına yönelik verebileceğiniz öneriler nelerdir?	

3) Sosyal Mühendislik konusundaki yaklaşım ve görüşlerinizden bahseder misiniz?

3.1	Sosyal Mühendislik ile ilgili sizce ne tür çalışmalar yapılabilir?	
3.2	Sosyal Mühendislik ile ilgili yenilikleri takip etmek için neler yapılabilir?	
3.3	Sosyal Mühendislik ile ilgili yeniliklerin adaptasyonu için neler yapılabilir?	
3.4	Sosyal Mühendislik ile ilgili karşılaşılan ve karşılaşılabilecek riskler nelerdir ve bu risklere karşı alınabilecek önlemler nelerdir?	
3.5	Sosyal Mühendislik'in uygulanmasına yönelik verebileceğiniz öneriler nelerdir?	

EK-3 (TR)

- 4) **Endüstri 4.0 ile Bilgi Güvenliği** ilişkilendirilerek yapılan çalışmalar nelerdir?
- Birkaç örnek verebilir misiniz?
 - Endüstri 4.0 ile Bilgi Güvenliği kavramlarını birlikte düşündüğünüzde yaklaşım ve görüşleriniz nelerdir?
- 5) **Endüstri 4.0 ile Sosyal Mühendislik** ilişkilendirilerek yapılan çalışmalar nelerdir?
- Birkaç örnek verebilir misiniz?
 - Endüstri 4.0 ile Sosyal Mühendislik kavramlarını birlikte düşündüğünüzde yaklaşım ve görüşleriniz nelerdir?
- 6) **Bilgi Güvenliği ile Sosyal Mühendislik** ilişkilendirilerek yapılan çalışmalar nelerdir?
- Birkaç örnek verebilir misiniz?
 - Bilgi Güvenliği ile Sosyal Mühendislik kavramlarını birlikte düşündüğünüzde yaklaşım ve görüşleriniz nelerdir?
- 7) **Endüstri 4.0, Bilgi Güvenliği ve Sosyal Mühendislik** ilişkilendirilerek yapılan çalışmalar nelerdir?
- Birkaç örnek verebilir misiniz?
 - Endüstri 4.0, Bilgi Güvenliği ve Sosyal Mühendislik kavramlarını birlikte düşündüğünüzde yaklaşım ve görüşleriniz nelerdir?

EK-3 (TR)

Endüstri 4.0, Bilgi Güvenliği ve Sosyal Mühendislik'in kesişme alanlarına ait aşağıdaki bileşenler için önem sıralaması sizce nasıl olmalıdır? (*lütfen kutucuklara 1'den 11'e kadar rakam yazınız*)

- ☐ Teknoloji Okur-Yazarlığı
- ☐ İnsan Faktörü
- ☐ Kimlik Hırsızlığı
- ☐ Veri ve Bilgi (Güvenliği)
- ☐ Fiziksel Güvenlik
- ☐ Siber Güvenlik
- ☐ Ulusal Güvenlik
- ☐ Dağıtık (distributed) ve Merkezi Olmayan (decentralization) Yapı
- ☐ Standartların Geliştirilmesi
- ☐ Risk Yönetimi
- ☐ Bütüncü (Holistik) Yaklaşım

Yukarıdaki liste için eklemek istediğiniz başka bir bileşen varsa, lütfen aşağıya yazınız.

-
-
-
-
-

Lütfen aşağıdaki soruları cevaplar mısınız?

- Yaşınız? :
- Mesleğiniz? :
- Kaç yıldır bu kurumda çalışıyorsunuz? :
- Pozisyonunuz/göreviniz nedir? :
- Sektörde kaç yıldır çalışıyorsunuz? :
- Eğitiminiz nedir? :
.....
.....

**Giresun University/Turkey, Social Sciences Institute,
Department of Business Administration**
Questions of PhD Thesis Interview for the Field Research Entitled
“The Adaptation of Information Security to Industry 4.0 Based Systems in the
Context of Social Engineering”

Researcher : Cevdet ÖZMEN
Advisor : Prof. Dr. Bayram KAYA

1) Could you please talk about your approaches and opinions on Industry 4.0?

1.1	What kind of practice might be done about Industry 4.0 in your opinion?	
1.2	What can be done to keep abreast of Industry 4.0 innovations? (How do you get updated?)	
1.3	What can be done to adapt the innovations in Industry 4.0?	
1.4	What are the risks that can be faced and related to Industry 4.0 and what precautions can be taken against these risks?	
1.5	What are your recommendations for the implementation of Industry 4.0?	

2) Could you please talk about your approaches and opinions on Information Security?

2.1	What kind of practice might be done about Information Security in your opinion?	
2.2	What can be done to keep abreast of Information Security innovations? (How do you get updated?)	
2.3	What can be done to adapt the innovations in Information Security?	
2.4	What are the risks that can be faced and related to Information Security and what precautions can be taken against these risks?	
2.5	What are your recommendations for the implementation of Information Security?	

3) Could you please talk about your approaches and opinions on Social Engineering?

3.1	What kind of practice might be done about Social Engineering in your opinion?	
3.2	What can be done to keep abreast of Social Engineering innovations? (How do you get updated?)	
3.3	What can be done to adapt the innovations in Social Engineering?	
3.4	What are the risks that can be faced and related to Social Engineering and what precautions can be taken against these risks?	
3.5	What are your recommendations for the implementation of Social Engineering?	

4) What kind of activities and projects have been accomplished in terms of **Industry 4.0** and **Information Security** correlation?

- Could you please give some examples?
- What are your views regarding these two concepts together?

5) What kind of activities and projects have been accomplished in terms of **Industry 4.0** and **Social Engineering** correlation?

- Could you please give some examples?
- What are your views regarding these two concepts together?

6) What kind of activities and projects have been accomplished in terms of **Information Security** and **Social Engineering** correlation?

- Could you please give some examples?
- What are your views regarding these two concepts together?

7) What kind of activities and projects have been accomplished in terms of **Industry 4.0**, **Information Security** and **Social Engineering** correlation?

- Could you please give some examples?
- What are your views regarding these three concepts together?

EK-3 (EN)

Would you please propose an order for the following components according to their significance in terms of the intersection of **Industry 4.0**, **Information Security** and **Social Engineering**? *(please give the numbers from 1 to 11 in the boxes)*

- ☐ Technology Literacy
- ☐ Human Factor
- ☐ Identity Theft
- ☐ Data and Information (Security)
- ☐ Physical Security
- ☐ Cyber Security
- ☐ National Security
- ☐ Distributed and Decentralized Structure
- ☐ Developing Standards
- ☐ Risk Management
- ☐ Holistic Approach

If there is any other component you want to add for the list above, please write down below.











Could you please answer the following questions?

What is your age? :

What is your occupation? :

How long have you been working for this organization/company? :

What is your position? :

How many years have you been working in this sector? :

What is your education? :

.....

.....

ÖZGEÇMİŞ



CEVDET ÖZMEN, Anadolu Üniversitesi (AÖF) İktisat Bölümü ve Hacettepe Üniversitesi Fransız Dili ve Edebiyatı Bölümü'nden mezun olmuş, Giresun Üniversitesi Sosyal Bilimler Enstitüsü, İşletme A.B.D.'da yüksek lisansını tamamlamıştır. Özel sektörde uzun yıllar yönetici pozisyonunda çalışmıştır. Gazi Üniversitesi Teknopark'ta (Ankara), AR-GE projesi kapsamında web tasarım, grafik tasarım, yazılım geliştirme ve proje yöneticiliği yapmıştır. 2014 yılından bu yana Giresun Üniversitesi'nde öğretim elemanı olarak görev yapmaktadır. Giresun Üniversitesi "*Kariyer Yönlendirme Merkezi*", "*Dış İlişkiler Koordinatörlüğü*", "*Akademik Teşvik Komisyonu*", "*Stratejik Planlama Ekibi*", "*Araştırma ve Uygulama Merkezleri Koordinatörlüğü*" birimlerinde çeşitli pozisyonlarda görev almış, *Genel Sekreterlik Koordinatörü* olarak çalışmıştır. İngiltere'nin Cambridge ve Bournemouth şehirlerinde dil eğitimi almış, İngilizce ve Fransızca bilmektedir. Akademik çalışma alanları: Yönetim Bilişim Sistemleri, Bilgi Yönetimi, Teknoloji ve Yenilik Yönetimi, E-Ticaret, Stratejik Yönetim, Bilgi Güvenliği ve Endüstri 4.0'dır.

ORCID: 0000-0002-8820-6032