

T.C.
GENELKURMAY BAŐKANLIĐI
HARP AKADEMİLERİ KOMUTANLIĐI
STRATEJİK ARAŐTIRMALAR ENSTİTÜSÜ MÜDÜRLÜĐÜ
YENİLEVENT/İSTANBUL

ENDÜSTRİYEL CASUSLUĐUN SOĐUK SAVAŐ SONRASI
KÜRESEL REKABET ORTAMINDAKİ YERİ

ULUSLARARASI İLİŐKİLER ANA BİLİM DALI
YÜKSEK LİSANS TEZİ

Hazırlayan
Bölent SUNGUR

Tez Danıőmanı
Yrd. Doç. Dr. őamil ÜNSAL

İSTANBUL – 2012

(BU SAYFA BOŞ BIRAKILMIŞTIR.)

TEZ TANITIM FORMU

TEZİN TARİHİ: 12.06.2012

TEZİN TİPİ: Yüksek Lisans

TEZİN BAŞLIĞI: Endüstriyel Casusluğun Soğuk Savaş Sonrası Küresel Rekabet Ortamındaki Yeri

TEZİN YAPILDIĞI BİRİM: Harp Akademileri Komutanlığı Stratejik Araştırmalar Enstitüsü Müdürlüğü

DAĞITIM LİSTESİ: Harp Akademileri Komutanlığı Stratejik Araştırmalar Enstitüsü "Tez Hazırlama ve Değerlendirme Yönergesi"nde belirtilen yerlere.

TEZİN ÖZETİ: Başka devletlere ait ticari sırların çalınmasının kökeni çok eski tarihlere dayanmaktadır. Ancak Soğuk Savaş sonrası fikri mülkiyetlerin ekonomik rekabette önem kazanması, endüstriyel casusluğun da artmasına yol açmıştır. Önceleri şirketler arası yasa dışı ticari sır hırsızlığı olarak algılanan endüstriyel casusluk, artık devletlerin ve istihbarat kurumlarının da içinde yer aldığı bir süreç haline gelmiştir.

ANAHTAR KELİMELELER: Fikri Mülkiyet Hakları, Ticari Sır, Bilişim Sistemleri, Siber Saldırı, Endüstriyel Casusluk, İstihbarat, Soğuk Savaş, Küresel Rekabet.

SAYFA SAYISI: 169

GİZLİLİK DERECESESİ: Tasnif Dışı

Bu tezin ihtiva ettiği hususlar şahsî görüşlerim olup; Türk Silahlı Kuvvetlerinin resmî görüşünü yansıtmamaktadır.


Bülent SUNGUR

T.C.
GENELKURMAY BAŐKANLIĐI
HARP AKADEMİLERİ KOMUTANLIĐI
STRATEJİK ARAŐTIRMALAR ENSTİTÜSÜ MÜDÜRLÜĐÜ
YENİLEVENT/İSTANBUL

ENDÜSTRİYEL CASUSLUĐUN SOĐUK SAVAŐ SONRASI KÜRESEL
REKABET ORTAMINDAKİ YERİ

ULUSLARARASI İLİŐKİLER ANA BİLİM DALI
YÜKSEK LİSANS TEZİ

Hazırlayan
Bölent SUNGUR

Tez Danıőmanı
Yrd. Dođ. Dr. őamil ÜNSAL

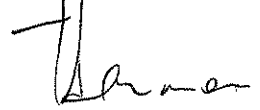
İSTANBUL – 2012

TASNİF DIŞI

HARP AKADEMİLERİ KOMUTANLIĞI

STRATEJİK ARAŞTIRMALAR ENSTİTÜSÜ MÜDÜRLÜĞÜNE

Bülent SUNGUR'un "Endüstriyel Casusluğun Soğuk Savaş Sonrası Küresel Rekabet Ortamındaki Yeri" konulu tez çalışması, jürimiz tarafından ULUSLARARASI İLİŞKİLER Ana Bilim Dalında YÜKSEK LİSANS tezi olarak kabul edilmiştir.



Başkan

Prof. Dr. Tolga YARMAN

Üye

Prof. Dr. Sıddık YARMAN

Üye

Yrd. Doç. Dr. Şamil ÜNSAL

(Danışman)

ONAY

Yukarıdaki imzaların, adı geçen öğretim üyelerine ait olduğunu onaylarım.

12/ 06/ 2012



Hasip SAYGILI

Dr. Kur. Alb.

Enstitü Müdürü

TASNİF DIŞI

ÖZET

Geçmiş çok eski tarihlere dayanan endüstriyel casusluğun Sanayi Devrimi sonrasında hız kazandığı görölmektedir. Soğuk Savaş süresince istihbarat örgütlerinin hedefinde, rakip devletlerin siyasi koşulları, liderleri, askeri ve ekonomik kapasiteleri, birliklerinin konuşlanma durumu, yeni geliřtirdikleri silahların özellikleri vb. gibi güvenlik kaynaklı başlıklar bulunmaktaydı. Berlin Duvarı'nın yıkılıőı ve Varşova Pakti'nin çöküşünün ardından askeri üstünlükten ziyade ekonomik üstünlüğün artan önemi devletler arası ilişkilerin de yeni anlamlar kazanmasını sağlamıştır. Geçmişteki askeri anlaşmalar yerini ekonomik işbirliği anlaşmalarına bırakırken, küresel ticarete büyük kazançlar elde etmek Batı'lı ölkelerin temel hedefi olmuştur. Bu yarışta kendi özel sektörlerinin ölkeler ekonomisi yararına daha fazla kazanç getirmesini gözeterek devletler istihbarat ve güvenlik kurumlarını da geçmişte kullanmadıkları bir sahada kullanmaya başlamışlardır.

Endüstriyel casusluk olaylarına bakıldığında en önemli unsurun insan olduđu görölmektedir. ARGE faaliyeti sonucu yoğun emeklerle hazırlanmış, ticari değeri yüksek olan patentli ürüne ait bilgilerin, çalışan bir personel tarafından yabancı şirkete verilmesiyle, bundan yüzyıllarca önce ipek üretimine dair sırların Çin'den çıkarılması arasında mantıksal açıdan bir farklılık yoktur. Ticari sırların elde edilmesinde insanların kişisel zaafaları, yabancı devletler ve firmalar tarafından sıklıkla kullanılmaktadır. Aynı zamanda bilgi güvenliği konusunda yeterli eğitim almamış çalışanlar da önemli kayıplara neden olabilmektedir.

Bilişim teknolojilerinde yaşanan gelişmelerle birlikte her türlü verinin elektronik ortamda işlenmesi, depolanması ve iletilmesi kolaylaşmış ancak hassas bilgilerin ve ticari sırların saklanması da bir o kadar zorlaşmıştır. Basılı haliyle bile saklanması mümkün olmayan binlerce sayfalık gizli bilgi barındıran veriler, saniyeler içinde kaydedilerek tek tuşla dünyanın herhangi bir yerine gönderilebilmektedir. Coğrafi sınır tanımayan siber uzay kendisine özgü bir suç dünyası yaratırken, bilgisayar korsanları ile istihbarat görevlileri sanayi casusluğunun yeni aktörleri olarak karşımıza çıkmaktadırlar. Dolayısıyla küresel ekonomi ile siber uzayın birleşmesi, yapılan mücadelede yeni bir cephe açmıştır. Uluslararası ortamdaki rekabetin acımasız doğası değişmemekle, birlikte kullanılan araç ve yöntemlerin teknolojik gelişime paralel olarak giderek daha da karmaşık hale geleceği ve çeşitlilik kazanacağı değerlendirilmektedir.

SUMMARY

It's observed that industrial espionage which rooted to the ancient history, gained momentum after Industrial Revolution. Security issues such as competing states' political conditions, leaders, military and economic capaticities, deployment of arms, features of new weapons were targeted by intelligence services during the Cold War. After the fall of Berlin Wall and the collapse of Warsaw Pact, economic superiority gained importance rather than military superiority, so that inter-state relations had new meaning. Achieving large profits in global trade has been targeted by Western Countries, while old style military aggreements leaving its place to economic cooperation. States that seek to espouse own private sector for advantage of national economy, started to use intelligence services in that race.

Industrial espionage cases indicate that the most important element is human factor. There is no logical difference between disclosing valuable patent information produced by intensive R&D researchs to a foreign company in that age, and running the secrets of silk production out of China hundred years ago. To obtain trade secrets, personal failings are frequently used by foreign governments and companies. At the same time, employees who didn't receive adequate training in information security can also cause major losses.

Advances in information technologies simplified processing, storage and transmission of all kinds of electronic data and sensitive information but made them difficult to hide. Data, contained thousands of pages confidential information, can be recorded with one click and sent anywhere in the world in seconds. Intelligence agents and hackers arise as new actors of industrial espionage while cyber space where has no geographical borders, composes a sui generis cime area. Therefore, the connection of cyberspace with the global economy has a new front in economic rivalry. It's evaluated that nature of ruthless competition in international environment will not change but tools and methods will become increasingly complex and diversified in parallel with technological development.

İÇİNDEKİLER

	SAYFA
ÖZET	I
SUMMARY	II
İÇİNDEKİLER	III
TABLolar LİSTESİ	VIII
ŐEKİLLER LİSTESİ	IX
RESİMLER LİSTESİ	X
KISALTMALAR LİSTESİ	XI
ÖNSÖZ	XV

BİRİNCİ BÖLÜM
ARAŐTIRMANIN PROBLEMİ

1. PROBLEMİN DURUMU	1
2. ARAŐTIRMANIN AMACI	3
3. ARAŐTIRMANIN ÖNEMİ	4
4. ARAŐTIRMANIN VARSAYIMLARI	4
5. ARAŐTIRMANIN SINIRLILIKLARI	5

İKİNCİ BÖLÜM
YÖNTEM

1. ARAŐTIRMANIN MODELİ	6
2. VERİLERİN TOPLANMASI	6
3. VERİLERİN ÇÖZÜMÜ VE YORUMLANMASI	6

ÜÇÜNCÜ BÖLÜM
KURAMSAL ÇERÇEVE

1. FİKRİ MÜLKİYET HAKLARI, TİCARİ SIR ve İLGİLİ KAVRAMLAR	7
a. Fikri Mülkiyet Kavramı ve Tarihsel Gelişimi	8
b. Fikri Mülkiyet Haklarında Temel İlkeler	9
(1) Tescil İlkesi	9

TASNİF DIŐI

(2) Ülkesellik İlkesi	10
(3) Gerçek Hak Sahipliđi İlkesi	11
(4) Rüçhan (Öncelik) İlkesi	11
(5) Ön Kullanım Hakkı	12
(6) Tükenme İlkesi	12
b. Fikri Mülkiyet Alanına Giren Konular	13
(1) Patent ve Buluşlar	15
(2) Faydalı Model	18
(3) Endüstriyel Tasarımlar	20
(4) Entegre Devre Topoğrafyaları	21
(5) Yeni Bitki Çeşitleri	22
(6) Know-How	23
c. Ticari Sırrın Unsurları ve İlgili Kavramlar	24
(1) Ticari Sırrın Unsurları	25
(a) Bilgi	25
(b) Ticari Nitelikte Olma	26
(c) Sır Olma	26
(ç) Sır Olarak Saklama İradesi	26
(2) Ticari Sırla İlgili Kavramlar	27
(a) İşletme Sırrı	27
(b) Meslek Sırrı	27
(c) Müşteri Sırrı	28
(ç) İş Sırrı	28
ç. Fikri Mülkiyet ve Ticari Sırların Korunması ile İlgili Uluslararası Kuruluşlar ve Anlaşmalar	28
(1) Paris Sözleşmesi	29
(2) Dünya Fikri Mülkiyet Hakları Organizasyonu (WIPO)	30
(3) Gümrük Tarifeleri ve Ticaret Genel Anlaşması(GATT)	30
(4) Ticaretle Bağlantılı Fikri Mülkiyet Hakları Sözleşmesi (TRIPs)	31
(5) Patent İşbirliđi Sözleşmesi (PCT)	32
(6) Avrupa Patent Sözleşmesi (EPC)	32

2. BİLİŞİM SİSTEMLERİ, SİBER SALDIRI ve BİLGİ

TEKNOLOJİLERİ GÜVENLİĞİ	33
a. Bilişim ve Bilişim Sistemleri	33
b. Siber Uzay ve Siber Saldırı	35
c. Siber Saldırıda Kullanılan Yöntemler	37
(1) Zararlı Yazılımlar	39
(a) Bilgisayar Virüsleri	39
(b) Solucanlar	40
(c) Truva Atı	40
(ç) Arka Kapılar	41
(d) Bot Ağı (Botnet)	41
(e) Klavye Kaydediciler	42
(f) Reklam Yazılımları	42
(g) Casus Yazılımlar	42
(ğ) Gelişmiş Sürekli Saldırıları	43
(2) Servis Saldırıları	44
(a) Hizmet Dışı Bırakma	44
(b) Dağıtık Hizmet Dışı Bırakma	44
(c) İstenmeyen E-posta	45
(3) Kimlik Saldırıları	46
(a) Phishing (Oltalama)	46
(b) Ortada Adam Saldırısı	47
(c) Kimlik Gizleme	47
(ç) Koklayıcı	47
(4) Gizli Dinleme	47
ç. Bilgi Teknolojileri Güvenliği	49
(1) Ortak Kriter (ISO 15408)	50
(2) Bilgi Güvenliği Yönetim Sistemi	51
(3) SCADA Güvenliği	51

DÖRDÜNCÜ BÖLÜM
BULGULAR VE YORUM

1. SOĞUK SAVAŞ SONRASI KÜRESEL REKABET ORTAMI	54
a. Yeni Dünya Düzeni ve Küreselleşme	56
b. Küresel Rekabet Ortamı	59
(1) Teknolojik Yenilik ve ARGE	62
(2) Çok Uluslu Şirketler	65
c. Ekonomik Güvenlik	68
ç. Ekonomik İstihbarat	72
2. ENDÜSTRİYEL CASUSLUK	76
a. Endüstriyel Casusluğun Tarihsel Gelişimi	78
b. Endüstriyel Casuslukta Kullanılan Yöntemler	80
(1) Ticari Bilgiler İçin Yapılan Beklenmedik İstekler	82
(2) İş Ziyaretinde Karşılaşılan Sıra Dışı Olaylar	83
(3) Şüpheli İş Teklifleri	83
(4) Uluslararası Sergi, Seminer ve Toplantıları Kullanma	84
(5) Ortak Girişim ve Araştırmaların İstismar Edilmesi	85
(6) Şirketlerin veya Teknolojinin Satın Alınması	85
(7) Eski çalışanların kullanılması	86
(8) Kültürel Benzerliklerin Kullanılması	86
(9) Çöp Karıştırma	87
(10) Sızdırma (Toplum Mühendisliği)	88
c. Bilişim Teknolojileri ve Endüstriyel Casusluk	90
ç. ECHELON ve Endüstriyel Casusluk	94
d. Rekabet İstihbaratı ve Endüstriyel Casusluk	98
e. İstihbarat Örgütlerinin Endüstriyel Casusluk Faaliyetleri	103
f. Endüstriyel Casusluğun Ekonomiye Olan Etkisi	110
g. Endüstriyel Casusluğa Karşı Alınması Gereken Tedbirler	115

TASNİF DIŐI

(1) İőletme Seviyesinde Alınması Gereken Tedbirler	116
(a) Personel Güvenliđi	119
(b) Fiziksel Güvenlik	119
(c) Siber Güvenlik	120
(ĉ) Farkındalık/Eđitim	121
(d) Rekabet İstihbaratı	122
(2) Devlet Seviyesinde Alınması Gereken Tedbirler	123
ğ. Endüstriyel Casusluđun Önlenmesinde Karőılaőılan Zorluklar	124
SONUÇ ve DEĞERLENDİRME	127
KAYNAKÇA	137
ÖZGEÇMİŐ	150

TABLolar

	SAYFA
TABLO-1: Sınai Mülkiyet Kapsamında Kanunda Yer Alan Koruma Süreleri	10
TABLO-2: Fikri Mülkiyet Haklarının Çeşitleri	14
TABLO-3: Dünya Genelinde Patent Başvurusunda Önde Gelen İlk Dokuz Ülke ve Türkiye	17
TABLO-4: Faydalı Model Başvurusunda Önde Gelen İlk Sekiz Ülke	19
TABLO-5: Endüstriyel Tasarım Başvurusunda Önde Gelen İlk Altı Ülke	21
TABLO-6: Dünya Genelinde İnternet Kullanıcı Sayısı	34
TABLO-7: Spam'ın Diğer Hasar Türleri ile Mukayesesi	45
TABLO-8: Dünya Genelinde Askeri Harcamalar	54
TABLO-9: Dünya GSYH Sıralamasında İlk Beş Ülke	55
TABLO-10: Dünyanın En Büyük İlk On Şirketi (2011)	66
TABLO-11: Güvenlik Unsurlarına Yapılan Saldırıları ve Kullanılan Yöntemler	90
TABLO-12: Yeraltı Dünyasında Saldırı Çeşitleri ve Fiyatları	91
TABLO-13: 2011 Yılında Sektörel Bazda Engellenen Günlük Ortalama Saldırı Sayısı	93
TABLO-14: ABD Casus Uyduları	96
TABLO-15: Endüstriyel Casusluk Faaliyetinde Bulunduğu Değerlendirilen İstihbarat Örgütleri ve Kurumlar	109

ŐEKİLLER

	SAYFA
ŐEKİL-1: Saldırı Geliőmiőliđi-Saldırgan Bilgi Düzeyi	36
ŐEKİL-2: Küreselleőme Sonucu Meydana Gelen Deđiőimin Boyutları ve Dinamikleri	57
ŐEKİL-3: Bilim ve Teknoloji Ekonomilerinin Kronolojik Sıralaması	63
ŐEKİL-4: Uluslararası Rekabet Gücünü Belirleyen Etkenler	70
ŐEKİL-5: Küresel Ekonomi ve Siber Uzayda Risk ve Tehditlerin Birleőimi	79
ŐEKİL-6: Toplum Mühendisliđi (Sızdırma) Döngüsü	89
ŐEKİL-7: Rekabet İstihbaratı Süreci	100
ŐEKİL-8: Yasal Durumlarına Göre Fikri Mülkiyet Hakları Koruma Yöntemleri	117
ŐEKİL-9: İőletmelerde Bilgi Güvenliđi	118

RESİMLER

	SAYFA
RESİM-1: Örnek Shadow Security Scanner Tarama Sonucu	38
RESİM-2: Menwith Hill İstasyonu (İngiltere)	97
RESİM-3: Bad Aibling İstasyonu (Almanya)	97
RESİM-4: Dassault Mirage III Savaş Uçağı	106
RESİM-5: IAI Kfir Savaş Uçağı	106

KISALTMALAR

APEC	: Asia-Pacific Economic Cooperation (Asya Pasifik Ekonomik İşbirliđi)
APT	: Advanced Persistent Threat (Gelişmiş Sürekli Saldırı)
ARPA	: Advanced Research Project Agency (İleri Araştırma Projeleri Ajansı)
ASEAN	: Association of Southeast Asian Nations (Güneydođu Asya Uluslar Birliđi)
ASIS	: American Society for Industrial Security (Amerikan Endüstriyel Güvenlik Topluluđu)
BGYS	: Bilgi Güvenliđi Yönetim Sistemi
BİLGEM	: Bilişim ve Bilgi Güvenliđi İleri Teknolojiler Araştırma Merkezi
BND	: Bundesnachrichtendienst (Almanya Federal Haber Alma Servisi)
BTE	: Bilişim Teknolojileri Enstitüsü
CIA	: Central Intelligence Agency (Amerikan Merkezi İstihbarat Teşkilatı)
CSE	: Communications Security Establishment (Kanada Haberleşme Güvenlik Kurulu)
CSIS	: Canadian Security Intelligence Service (Kanada Güvenlik İstihbarat Servisi)
ÇUŞ	: Çok Uluslu Şirket
DCI	: Défense Conseil Intenational (Uluslararası Savunma Konseyi)
DDoS	: Distributed Denial of Service (Dağıtık Hizmet Dışı Bırakma)
DGSE	: Direction Générale de la Sécurité Extérieure (Fransız Dış Güvenlik Genel Müdürlüđu)
DIS	: Defense Security Service (Amerikan Savunma Güvenlik Servisi)
DNS	: Domain Name System (Alan Adı Sistemi)
DoS	: Denial of Service (Hizmet Dışı Bırakma)
DRM	: Direction du renseignement militaire (Askeri İstihbarat Direktörlüđu)

TASNİF DIŐI

DSD	: Defence Signals Directorate (Avustralya Savunma Haber Direktörlüğü)
DTÖ	: Dünya Ticaret Örgütü
EAL	: Evaluation Assurance Level (Değerlendirme Garanti Seviyesi)
EDTK	: Entegre Devre Topografyalarının Korunması Hakkında Kanun
EEA	: Economic Espionage Act (Ekonomik Casusluk Kanunu)
EGE	: l'Ecole de Guerre Economique (Ekonomik Savaş Okulu)
End.Tas.KHK:	Endüstriyel Tasarımların Korunması Hakkında Kanun Hükmünde Kararname
EPC	: European Patent Convention (Avrupa Patent Sözleşmesi)
FSEK	: Fikir ve Sanat Eserleri Kanunu
GATT	: General Agreement on Tariffs and Trade (Gümrük Tarifeleri ve Ticaret Genel Anlaşması)
GCHQ	: Government Communications Headquarters (İngiltere Hükümet Haberleşme Merkezi)
GCSB	: Government Communications Security Bureau (Yeni Zelanda Devlet İletişim Güvenlik Bürosu)
HUMINT	: Human Intelligence (İnsan İstihbaratı)
IMF	: International Monetary Fund (Uluslararası Para Fonu)
IP	: Internet Protocol (İnternet Protokol)
ISO	: International Organization for Standardization (Uluslararası Standartlar Organizasyonu)
İKK	: İstihbarata Karşı Koyma
JETRO	: Japan External Trade Organization

TASNİF DIŐI

(Japonya Dıő Ticaret Organizasyonu)

LAKAM : ha-Lishka le-Kishrei Mada (İsrail- Bilimsel İliőkiler İtibat BÜrosu)

Mar.KHK : Markaların Korunması Hakkında Kanun HÜkmünde Kararname

MITI : Ministry of International Trade and Industry

(Uluslararası Ticaret ve Sanayi Bakanlığı)

MİT : Milli İstihbarat Teőkilatı

NAFTA : North American Free Trade Agreement

(Kuzey Amerika Ülkeleri Serbest Ticaret Anlaőması)

NCC : National Counterintelligence Center

(Amerikan Ulusal Karőı İstihbarat Merkezi)

NPA : National Planning Agency (Ulusal Planlama Ajansı)

NSA : National Security Agency (Amerikan Ulusal Güvenlik Ajansı)

OKTEM : Ortak Kriter Test Merkezi

ONCIX : Office of National Counterintelligence Executive

(Amerikan Ulusal Karőı İstihbarat İcra Dairesi)

Pat.KHK :Patent Haklarının Korunması Hakkında Kanun HÜkmünde Kararname

PCT : Patent Cooperation Treaty (Patent İőbirliőı Anlaőması)

PLC : Programmable Logic Controller

(Programlanabilir Mantıksal Denet-leyiciler)

SCADA : Supervisory Control and Data Acquisition

(Denetleme Kontrol ve Veri Toplama)

SCIP : Society of Competitive Intelligence Professionals

(Rekabet İstihbaratı Profesyonelleri Topluluőu)

SIGINT : Signal Intelligence (Sinyal İstihbaratı)

TASNİF DIŐI

TCK	:Türk Ceza Kanunu
TDK	:Türk Dil Kurumu
TPE	:Türk Patent Enstitüsü
TRIPs	: Agreement on Trade Related Aspects of Intellectual Property Rights (Ticaretle Bağlantılı Fikri Mülkiyet Hakları Sözleşmesi)
TSE	: Türk Standartları Enstitüsü
TUBİTAK	: Türkiye Bilimsel ve Teknik Araştırma Kurumu
UEKAE	: Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü
USB	: Universal Serial Bus (Evrensel Seri Veri Yolu)
WIPO	: World Intellectual Property Organisation (Dünya Fikri Mülkiyet Örgütü)

ÖNSÖZ

Ekonomik değeri olan bilginin veya ticari sırrın başka devletler tarafından elde edilmek istenmesinin tarihi oldukça eskiye dayanmaktadır. Ancak teknolojiadaki gelişmeler, Soğuk Savaş sonrası değışen güvenlik anlayışı ve fikri mülkiyetlerin küresel ticaretteki değeri önne çıkması istihbarat örgütlerinin de bu alanda yoğun bir şekilde faaliyet göstermesine neden olmaktadır. Bu konuda uluslararası hukukun ve devletlerarası anlaşmaların çok da yeterli olmadığı görölmektedir.

Mevcut çalışmanın ilk iki bölümünde araştırmanın problemi, varsayımları, sınırlılıkları ve tezde kullanılan yöntem; üçüncü bölümünde fikri mülkiyet hakları, ticari sır ve ilgili kavramlar ile bilişim sistemleri, siber saldırı ve bilgi teknolojileri güvenliği irdelenerek kuramsal çerçevenin oluşturulması hedeflenmiştir. Çalışmanın dördüncü bölümünde ise oluşturulan kuramsal çerçeveden temin edilen bulgulara istinaden, Soğuk Savaş sonrası küresel rekabet ortamı ve endüstriyel casusluk konuları incelenmiştir. Son bölümde ise temin edilen bulguların analiz edilmesi suretiyle varılan neticeler yer almıştır.

Yapılan tez çalışmayla ilgili olarak, öncelikle yüksek lisans eğitimi görmeme imkân tanıyan Jandarma Genel Komutanlığı'na; tezimin her aşamasında değeri katkı ve rehberliğiyle beni yönlendiren danışman hocam Yrd. Doç. Dr. Şamil ÜNSAL'a, İstanbul'un çeşitli üniversitelerinden gelerek bizleri aydınlatan, bugüne gelmemizde emeği olan öğretim üyelerimize ve eğitim süreci boyunca bizlere destek olan tüm SAREN personeline şükranlarımı sunuyorum.

Tezin yazımı sırasında bana gramer konusunda destek olan değeri hocam Muammer DEMİR'e; ömür boyu sürmesini temenni ettiğim dostlukları için SAREN'de birlikte eğitim aldığım sınıf arkadaşlarıma; her daim bana devamlı moral veren anneme; çalışmalarım sırasında gösterdiği fedakârlık ve ilgi için eşim Tuğba'ya ve varlığı ile yaşama sevinci veren oğlum Ata Deniz'e çok teşekkür ediyorum.

BİRİNCİ BÖLÜM

ARAŐTIRMANIN PROBLEMİ

1. PROBLEM DURUMU:

20. yüzyılda ekonomik açıdan ileri düzeyde olan ülkelere bakıldığında bunların büyük çoğunluğunun petrol yataklarına sahip olan, işleyen ve ticaretini yapan ülkeler (Japonya hariç) olduğu görülmektedir. Günümüzde ise dengenin, bilgiyi üreten, pazarlayan ve kullanan ülkelerin ve şirketlerin lehine döndüğünü söylemek mümkündür. Barutçugil'in (2002, s.13) ifadesi ile *"21. yüzyılın petrolü bilgidir."*

Ticari anlamda küresel rekabetin tırmanması, şirketlerin yeni buluşlar için ARGE faaliyetlerine yatırım yapmalarını zorunlu kılmaktadır. Bu durum çok uluslu şirketlerin ticareti adeta bir "savaş" olarak algılamalarına yol açmakta, dolayısıyla yüksek kâr elde edebilmek için bilginin üretimi ve sahiplenilmesi önem kazanmaktadır. Ulusal güvenlik açısından ekonomik gelişmişliğin daha fazla değer kazanması, ekonomik istihbarat faaliyetlerinde de artışa neden olmuştur. Endüstriyel casusluğun, artık ticari alanda yapılan mücadelenin yeni cephesi olduğunu söylemek mümkündür. Bunun yanında, devletlerin ticari sırlarını korumalarını ve rakiplerin bilgilerini ele geçirmek suretiyle ARGE faaliyetlerinde büyük paralar harcamadan teknolojik rekabeti gerçekleştirmelerini de sağlamaktadır (Güldiken, 2006, s. 178-179).

Daha önceleri askeri alanda değerlendirilen "güvenlik" anlayışının şekil değiştirmesi, durumu daha karmaşık hale getirmektedir. Bunun neticesinde "ulusal güvenlik" anlayışı artık ekonomik istihbarat ile bir arada düşünülmektedir. Soğuk Savaş süresince ortak güvenlik şemsiyesi altında bir arada hareket eden devletler, bugün ekonomik anlamda birbirlerinin rakipleri durumundadırlar (J.P. Brodeur, 2003, s.5). Örnek vermek gerekirse, 1992 yılında Fransız İstihbarat Örgütü DGSE'nin (Direction Générale de la Sécurité Extérieure-Dış Güvenlik Genel Müdürlüğü), Air France Havayollarına ait uçakların birinci sınıf kabinlerine yerleştirdiği dinleme cihazları ile seyahat eden Amerikalı iş adamlarını dinlediği ortaya çıkmıştır. İş adamlarının kaldığı otel odaları da dinlenmiştir. Fransızların uyguladığı bu tarz operasyonlara karşı CIA, 1993 yılında Paris Hava Gösterine (Paris Air Show) katılacak şirketleri, Fransızların ticari sırları çalma ihtimaline karşı uyarmıştır (Nasheri, 2005, s. 16).

Soğuk Savaş süresince istihbarat ve güvenlik anlayışının odak noktasını askeri ve siyasi hedefler oluşturmaktaydı. Ancak Soğuk Savaşın sona ermesiyle birlikte, NATO'dan Avrupa Birliği'ne, CIA'dan Dünya Ticaret Örgütü'ne kadar

TASNİF DIŐI

neredeyse bütün güvenlik kurumları ve ekonomik organizasyonlar, görevlerini yeniden tanımlama ve yeni roller üstlenme çabasına girişmişlerdir. Bu dönemde ekonomik üstünlüğün askeri üstünlüğe eşdeğer hatta daha ileri bir değer kazanması, istihbarat faaliyetlerinin ekonomik alanda yoğunlaşmasını sağlamış, ekonomik casusluğu ön plana çıkarmıştır. Bu doğrultuda rakip devletlere ait ticari sırlar, üretim süreçleri ve teknolojik yenilikler istihbarat faaliyetlerinin yeni odak noktası olarak değer kazanmışlardır (Nasheri, 2005, s. 19). Örneğin Rusya Federasyonu'nda dış istihbaratla ilgili 8 Aralık 1995 yılında kabul edilen 5 Numaralı Federal Kanunda, istihbarat toplama faaliyetlerinin hedeflerinde biri olarak, ülkenin ekonomik gelişimi ile bilimsel ve teknik alanda ilerlemesinin desteklenmesi ifadesi yer almaktadır (md.5\3). Aynı kanunun 14'üncü maddesinde ise, istihbarat bilgisinin resmi organlar haricinde işletmelere, enstitülere ve Rusya Federasyonu Başkanınca tayin edilen organizasyonlara da sağlanacağı belirtilmektedir (FAS, 2012).

Klasik istihbarat yaklaşımında ekonomik istihbarat dışında değerlendirilen endüstriyel casusluğun, ekonomik istihbaratın doğasında ortaya çıkan gelişmeler sonucu ekonomik istihbaratın bir dalı haline geldiği gözlemlenmektedir. Önceleri şirketler arası yasa dışı bilgi hırsızlığı olarak algılanan endüstriyel casusluk, artık devletlerin birbirlerine karşı kullandıkları ve istihbarat kurumlarının da yer aldığı bir süreç haline gelmiştir (Özdağ, 2009, s.124). ABD'de her yıl Kongre'ye ekonomik istihbarat ve endüstriyel casusluk hakkında rapor sunan Ulusal Karşı İstihbarat İcra Dairesi (Office of National Counterintelligence-ONCIX)'ne göre; ekonomik casusluğu önlemek maksadıyla 14 resmi kuruluş görev yapmaktadır (ONCIX, 2011, s.iv). ABD'nin karşı istihbarattan sorumlu kuruluşu olan Ulusal Karşı İstihbarat Merkezi (National Counterintelligence Center-NCC)'nin 1997 yılında yayınladığı raporda ise, ticari sırların gerek yabancılar gerek ülke içinden çalınmasının ABD endüstrisine ayda 2 milyar dolarlık kayba neden olduğu ifade edilmektedir (NCC, 1997, s. 7). Buna karşın, Geçici Komisyon¹ tarafından 2001 yılında Avrupa Parlamento'suna sunulan ECHELON Raporunda ise ABD, İngiltere, Kanada, Avustralya ve Yeni Zelanda'nın dünya genelinde bütün haberleşme sistemlerini (uydu, telefon, faks, internet vs.) izleyebilme imkânına sahip oldukları belirtilmektedir. Raporda adı geçen ülkelerin elde ettikleri bilgileri sadece askeri ve siyasi maksatlarla değil, kendi ülkelerindeki özel şirketlere küresel rekabette haksız fayda sağlamak için de kullandıkları vurgulanmaktadır. Yapılan çalışmada, 1994 yılında Suudi Arabistan ile

¹ Temporary Committee on the ECHELON Interception System, Report on the existence of a global system for the interception of private and commercial communications (ECHELON interception system) (2001/2098(INI)), 11 July 2001. http://epic.org/EU_ECHELON_Rpt.pdf Erişim Tarihi:12.09. 2011.

TASNİF DIŐI

Airbus řirketi arasında önemli bir ihalenin pazarlığı ile ilgili görüşmelerin, Ulusal Güvenlik Ajansı (National Security Agency-NSA) tarafından rakip Boeing ve McDonnell-Douglas firmasına aktarılması suretiyle Amerikalıların 6 milyar dolarlık anlaşmayı kazandıkları belirtilmektedir. Aynı belgede, 1996 yılında ABD Kongresi'ne sunulan Brown Raporu'na² atıfta bulunularak; açık olmayan kaynaklardan elde edilen istihbaratın %5'inin ekonomik istihbarat maksadıyla kullanıldığı bu sayede Amerikan endüstrisinin anlaşmalarda 7 milyar dolarlık kazanç sağladığı ifade edilmektedir.

Sonuç olarak, devletlerin geçmişte siyasi ve askeri güvenlik maksadı ile kullandıkları istihbarat faaliyetlerini, Soğuk Savaş sonrasında endüstriyel casusluk faaliyeti ile küresel rekabette kendi özel sektörlerini desteklemek için kullanmaları bu araştırmanın problemini oluşturmaktadır.

2. ARAŐTIRMANIN AMACI:

Bu çalışmadaki temel amaç, Soğuk Savaş sonrası ticaretin küresel bir nitelik kazanması sonucu çok uluslu řirketlerin kendi ülkelerinin ekonomilerine önemli ölçüde katkı sağlamaları ve bu doğrultuda devletlerin de sahip oldukları istihbarat kurumları vasıtasıyla bu řirketlere verdikleri desteğı ortaya koymaktır. Temel amaca yönelik olarak alt amaçlar:

- a. Fikri mülkiyet hakları, ticari sır ve yenilik (innovation) kavramlarını ulusal ekonomi ve küresel rekabet açısından değerlendirmek,
- b. Endüstriyel casusluk açısından biliřim sistemleri, siber saldırı ve bilgi teknolojileri güvenliğini değerlendirmek,
- c. Ekonomik istihbarat, rekabet istihbaratı, iş istihbaratı, ekonomik casusluk ve endüstriyel casusluk kavramları arasındaki farkları ve ilişkileri incelemek,
- ç. İstihbarat örgütlerinin endüstriyel casusluk konusundaki faaliyetlerini değerlendirmek,

² Commission on the Roles and Capabilities of the United States Intelligence Community: Preparing for the 21st Century: An Appraisal of U.S. Intelligence (March 1, 1996). file:///C:/Documents%20and%20Settings/Administrator/Desktop/Commission%20on%20the%20Roles%20and%20Capabilities%20of%20the%20United%20States%20Intelligence%20Community.htm Eriřim Tarihi:12.09.2011.

TASNİF DIŐI

d. Ekonomik ve endüstriyel casusluğun ülke ekonomisi ve kalkınma üzerine olan etkilerini değerlendirmek,

e. Gelişen teknoloji ile birlikte, ekonomik ve endüstriyel casuslukta kullanılan teknik ve yöntemleri incelemektir.

3. ARAŐTIRMANIN ÖNEMİ:

Soğuk Savaş süresince istihbarat örgütlerinin hedefinde, rakip devletlerin siyasi koşulları, liderleri, askeri ve ekonomik kapasiteleri, birliklerinin konuşlanma durumu, yeni geliőtirdikleri silahların özellikleri vb. gibi güvenlik kaynaklı başlıklar bulunmaktaydı. Berlin Duvarı'nın yıkılıőı ve Varőova Paktı'nın çöküşünün ardından askeri üstünlükten ziyade ekonomik üstünlüğün artan önemi devletler arası ilişkilerin de yeni anlamlar kazanmasını sağlamıőtır. Geçmiőtteki askeri anlaşmalar yerini ekonomik işbirliğı anlaşmalarına bırakırken, küresel ticarete büyük kazançlar elde etmek Batı'lı ülkelerin temel hedefi olmuőtur. Bu yarıőtta kendi özel sektörlerinin ülke ekonomisi yararına daha fazla kazanç getirmesini gözeten devletler istihbarat ve güvenlik kurumlarını da geçmişte kullanmadıkları bir sahada kullanmaya başlamıőtlardır. Bu doğırtuda yapılacak çalışmanın iki açıdan önem taşıdığı değerlendirilmektedir:

a. Fikri mülkiyet hakları bakımından ekonomik ve endüstriyel casusluğun ülke ekonomisi ve kalkınma üzerine olan etkilerinin irdelenmesi,,

b. Soğuk Savaş sonrası küresel rekabet ortamında istihbarat örgütlerinin yeni faaliyet alanı olarak endüstriyel casusluğun incelenmesi.

4. ARAŐTIRMANIN VARSAYIMLARI:

Bu tez çalışmasında;

a. Küresel ölçekte çok uluslu şirketler arasındaki rekabet sürdüğü müddetçe ekonomik ve endüstriyel casusluk faaliyetlerinin artarak devam edeceği,

b. Ekonomik ve endüstriyel casuslukla ilgili parlamento ve kongrelere sunulan raporlar ile yakalanan kişilere ait mahkeme kararlarının doğıru ya da doğıruya yakın oldukları,

c. Ekonomik ve endüstriyel casusluğun endüstrileőtmiş ülkelerin kendi aralarında olduğı kadar, endüstrileőtmekte olan, içinde Türkiye'nin de bulunduğı; Çin, Tayvan, Malezya vb ülkeleri de giderek kapsayacağı varsayılmaktadır.

5. ARAŐTIRMANIN SINIRLILIKLARI:

İstihbarat örgütlerinin ve devletlerin resmi kurumlarının özel şirketler lehine ekonomik ve endüstriyel casusluk alanındaki faaliyetlerinin hız kazandığı Soğuk Savaş sonrası dönem araştırmanın inceleme açısından zamansal sınırını oluşturmaktadır.

Devletlerin kendi şirketleri arasında meydana gelen endüstriyel casusluk olayları, genellikle bu konunun adli bir mesele olması ve iç hukuk (ceza kanunu, ticaret kanunu vs.) yolları ile çoğu zaman çözülebilir olması nedeniyle de araştırmanın kapsamı dışında bırakılmıştır.

İKİNCİ BÖLÜM

YÖNTEM

1. ARAŐTIRMANIN MODELİ:

Çalışma Soğuk Savaş sonrası ekonomik gelişmişliğın artan değeri ile birlikte, devletlerin küresel rekabette öne geçmek için kullandıkları endüstriyel casusluk faaliyetlerini kapsamaktadır. Bu doğrultuda; küresel ticarete haksız rekabet, ekonomik güvenlik, ulusal çıkar ve fikri mülkiyet hakları çerçevesinde, tekil araştırma modeli temelinde bir inceleme yapılacaktır.

2. VERİLERİN TOPLANMASI:

Araştırmada kullanılacak verilerin toplanmasında; kütüphanelerden, internetteki akademik veri tabanlarından, bilimsel yayın tarama sitelerinden, medya ve web sitelerinin arşivlerinden, resmi web sitelerinden elde edilecek birincil ve ikincil kaynaklardan istifade edilmiştir.

3. VERİLERİN ÇÖZÜMÜ VE YORUMLANMASI:

Verilerin çözümü ve yorumlanmasında, çoğunlukla basılı metinler, kullanılacağından nitel araştırma tekniklerinden doküman incelemesi ve içerik analizi yöntemleri uygulanacaktır. Yapılacak araştırma şu şekilde aşamalandırılmıştır:

- (1) Araştırma sorularının geliştirilmesi,
- (2) Verilerin toplanması, kategorilere ayrılması ve alt problemlerle ilişkilendirilmesi,
- (3) Verilerin analizi ve yorumlanması,
- (4) Durum çalışmasının rapor edilmesi

ÜÇÜNCÜ BÖLÜM

KURAMSAL ÇERÇEVE

1. FİKRİ MÜLKİYET HAKLARI, TİCARİ SIR ve İLGİLİ KAVRAMLAR

Tarihin bilinen başlangıcından günümüze kadar olan dönemde ekonomik yapının üç ayrı aşamadan geçtiği kabul edilmektedir. Birinci dönemde ekonomi, tarıma dayalı üretime dayanırken, ikinci dönemde endüstri temelli üretim ön plana çıkmıştır. Günümüz ekonomilerinde ise sanayi ağırlıklı ekonomilerin yerini artık bilgiye dayalı yapılar almıştır (Toffler, 1992, s.82-83). Bilgi ekonomisi, önemli ölçüde bilginin üretilmesi ve yaygınlaştırılmasına dayanan ekonomi anlayışıdır. Devletlerin, kurumların ve işletmelerin başarısı bilgi üretmelerine ve bu bilgiyi etkin bir şekilde kullanmalarına bağlıdır (Alper, 2011, s.154). Gayri maddi varlık olarak da nitelendirilen bilgi, teknolojik, biyolojik ya da sosyal bir sistem tarafından anlamlandırılan her türlü veriyi ifade etmektedir. Bu sistemler içindeki işlevi nedeniyle koruma altına alınan tüm sanatsal ve bilimsel çalışmalar da bilgi kavramı içerisinde yer alır (Bayamlıoğlu, 2008, s.7).

Bilgiyle ilgili faaliyetler, sosyal koşullar ve teknolojik kapasite ile yakın ilişki içindedir. Örneğin antik çağlarda yaşayan zanaatkârlarca kullanılan ve geliştirilen aletler, bir anlamda bedenin devamı niteliğinde ve insanla bütünleşmiş nesnelerdir. Ancak modernleşme ile birlikte kullanılan teknolojik araçlar insan bedeninin değil beynin uzantısı konumundadır (Bayamlıoğlu, 2008, s.41).

Sanayi toplumlarındaki maddi üretimden ziyade bilginin kitlesel üretiminin öne çıktığı, nitelikli insanın önem kazandığı, yeni teknolojilerin yoğun olarak kullanıldığı, üretildiği ve süratle yayıldığı, bilginin kontrolü ve sahipliği için kurumsallaşmanın sağlandığı ve son olarak bilgili insanın merkez konumda olduğu toplumlar bilgi toplumu olarak adlandırılmaktadır (TOBB, s.16). Giderek çoğalan bilgi birikimi uzmanlaşmayı doğurmuş ve bunun sonucunda bilgi malvarlıksal bir değer kazanmıştır (Bayamlıoğlu, 2008, s.75). Ancak bilgiyi üreterek pazarlayan ve bu sermayesini gün geçtikçe artıran devletler ile az gelişmiş devletler arasındaki mesafe giderek açılmaktadır. Bu nedenle fikri mülkiyet üretemeyen ve haklarını da koruyamayan toplumlar ekonomik, sosyal ve kültürel alanlarda önemli sorunlarla yüzleşmektedirler (Karahan, Suluk, Saraç ve Nal, 2011, s.32-33).

Ülkeler fikri mülkiyetlerini genellikle iki nedenden dolayı korumak istemektedirler. Bunlardan ilki eser ya da buluş sahibinin yarattığı ürün üzerindeki ekonomik ve ahlaki hakları ile kamunun bu eserlere ulaşma hakkını kanuni güvence

TASNİF DIŞI

altına almak. Diğerleri ise yaratıcılığı teşvik ederek ekonomik ve sosyal gelişime katkıda bulunacak uygun rekabet ortamını sağlamaktır (WIPO, 2012, s.4). Ancak fikri mülkiyet ve ticari sırların gün geçtikçe artan önemi endüstriyel casusluk yolu ile değerli bilgilerin çalınması sorununu da beraberinde getirmiştir. Bu nedenle endüstriyel casusluğun amaçları ve etkileri bakımından fikri mülkiyet ve ticari sırları incelemenin son derece önemli olduğu değerlendirilmektedir.

a. Fikri Mülkiyet Kavramı ve Tarihsel Gelişimi

En geniş tanımıyla fikri mülkiyet, “*insan düşüncesinin ürünü olan gayrimaddi mallar*” şeklinde tanımlanmaktadır (Erdem, 2002, s.2). İngilizce kaynaklarda “intellectual property” olarak ifade edilen terim; fikir ve sanat eserleri (telif hakları), patentler, faydalı modeller, tasarımlar, biyoteknolojik buluşlar, entegre devre topoğrafyaları, know-how ve ticari sırları kapsayan bir çerçeve kavramdır (Karahana, Suluk, Saraç ve Nal, 2011, s.1). Çeşitli kaynaklarda “fikri mülkiyet”, “fikri ve sınai mülkiyet”, “fikri, sınai ve ticari mülkiyet” gibi ifadeler yer alsa da esas itibariyle aralarında fark bulunmamaktadır (Tekinalp ve Tekinalp, 2000, s.681).

Batı Avrupa’da sınai mülkiyet konusundaki ilk gelişmeler 15. yüzyılda başlamıştır. Bu dönemdeki sınai haklar yasal düzenleme bulunmaksızın lonca ya da meslek örgütlerine tanınan imtiyazlarla yürütülmüştür. Dünyada fikri mülkiyet konusunda ilk yasal düzenleme, 1474 yılında Venedik’te kabul edilen “Venedik Patent Yasası”dır. Bahse konu yasada, buluş sahiplerine diğer koruma tedbirlerinin yanında buluşun koruma süresi olarak on yıllık süre tanınmıştır (Topçu, 2007, s.33-34).

Patent, marka ve tasarım gibi sınai mülkiyet haklarının modern anlamda ortaya çıkması Sanayi Devrimine denk gelmektedir. Bunun nedeni ise Sanayi Devriminde kullanılmaya başlanan yeni üretim şeklinin böyle bir korumayı zorunlu kılmasıdır. 1474’teki patent düzenlemesinden sonra ikinci düzenleme, İngiltere’de Tekel Kanunu olarak bilinen 1624 tarihli kanundur. Bunları 1790 tarihli Amerikan, 1791 tarihli Fransız ve 1799 tarihli İsveç patent kanunları izlemiştir (Karahana, Suluk, Saraç ve Nal, 2011, s.23).

Türkiye’de ise fikri mülkiyetle ilgili yasal düzenlemeler 18. yüzyılın sonlarına uzanır. Osmanlı Devleti döneminde 1872 yılında Alamet-i Farika Nizamnamesi ve 1879 yılında İhtira Beratı Kanunu yürürlüğe girmiştir. Markaların korunmasına ilişkin çıkarılan Alamet-i Farika Nizamnamesi 1857 tarihli Fransız Marka Kanunundan; İhtira Beratı Kanunu ise 1844 tarihli Fransız Patent Kanunundan tercümedir. Ancak

TASNİF DIŞI

kanunlar yürürlükte olmasına karşın Osmanlı Devleti döneminde ihtira beratı (patent) istenen buluşlar ön incelemeye tabi tutulmadığı gibi icadın sağladığı yenilik ve fayda da devlet kefaleti altına alınmamıştır (Bülbül ve Özbay, 2010, s.50-51). Buna neden olarak ise ülkenin içinde bulunduğu ekonomik ve sosyal şartlar gösterilmektedir. Fikir ve sanat eserlerinin korunması ile ilgili olarak 1952 yılında Fikir ve Sanat Eserleri Kanunu (FSEK) yürürlüğe girmiştir. 1995 yılında ise reform denilebilecek düzeyde değişiklikler yapılmıştır (Karahana, Suluk, Saraç ve Nal, 2011, s.24). 31 Aralık 1995 yılında yürürlüğe giren Türkiye ile Avrupa Birliği arasında imzalanan Gümrük Birliği Kararı ile Türkiye; fikri, sınai ve ticari mülkiyetin korunması konusunda ulusal hukukunda yeni düzenlemeler yapmayı üstlenmiştir. Bu yükümlülüğün gereğince, patent haklarının korunması amacıyla İhtira Beratı Kanunu ilga edilerek bugün hala yürürlükte bulunan 551 sayılı Patent Haklarının Korunması Hakkında Kanun Hükmünde Kararname (Pat.KHK), marka haklarının korunması için 556 sayılı Markaların Korunması Hakkında KHK (Mar.KHK), endüstriyel tasarımların korunması için 554 sayılı Endüstriyel Tasarımların Korunması Hakkında KHK (End.Tas.KHK) kabul edilmiştir. Ayrıca telif hakları bakımından uyum sağlama süreci kapsamında FSEK'te 1995 ve 2001 yıllarında önemli değişiklikler yapılmıştır (Erdem, 2003, s.1).

b. Fikri Mülkiyet Haklarında Temel İlkeler

Fikri mülkiyet haklarında yer alan temel ilkeler taşıdığı özellikler nedeniyle diğer haklardan ayrı olarak değerlendirilmektedir. Buna göre;

- Tescil ilkesi,
- Ülkesellik ilkesi,
- Gerçek hak sahipliği ilkesi,
- Rüçhan (öncelik) ilkesi,
- Ön kullanım hakkı,
- Tükenme ilkesi, fikri mülkiyet haklarının belirlenmesinde son derece önemlidir.

(1) Tescil İlkesi

Marka, patent ve tasarım gibi sınai hakların oluşabilmesi için öncelikle ilgili kurumlar nezdinde tutulan sicile tescil ettirilmeleri gerekmektedir. Türkiye'de bu konudaki yetkili kurum Türk Patent Enstitüsü (TPE)'dür. Patent, tasarım, marka ya da faydalı model belgesi sahibi, bu belge iptal edilinceye ya da süresi doluncaya kadar korumadan yararlanacaktır. Kara Avrupası hukuk sisteminde yer alan Türk hukukunda sınai haklar bakımından tescil ilkesi kabul edilmiştir. Ancak telif hakları bakımından kural olarak tescil öngörülmemiştir (Karahana, Suluk, Saraç ve Nal,

TASNİF DIŞI

2011, s.6-7). Aşağıda yer alan tabloda ise tescili yapılan sınai mülkiyete ilişkin hukukumuzda kabul edilen koruma süreleri yer almaktadır (Tablo-1).

HAK	KORUMA BAŞLANGICI	KORUMA SÜRESİ
İncelemeli Patent	Başvuru Tarihi	20 yıl
İncelemesiz Patent	Başvuru Tarihi	7 yıl
Faydalı Model	Başvuru Tarihi	10yıl
Tasarım	Başvuru Tarihi	5 yıllık dönemler halinde yenilenmek kaydıyla 25 yıl
Entegre Devre	Ticari olarak piyasaya sürme; piyasaya sürülmemişse başvuru tarihi	10 yıl
Yeni Bitki Çeşidi	Tescil	25 yıl (Ağaçlar, asmalar ve patates için 30 yıl)

Tablo-1: Sınai Mülkiyet Kapsamında Kanunda Yer Alan Koruma Süreleri.

(Kaynak:Sami Karahan, Cahit Suluk, Tahir Saraç ve Temel Nal. Fikri Mülkiyet Hukukunun Esasları.Ankara, Seçkin Yayıncılık, s.28'den alınarak düzenlenmiştir)

Tescil verilerek koruma altına alınan buluşlarla ilgili koruma sürelerinde uluslararası anlaşmaların getirdiği standartlar baz alınmaktadır. İlerleyen bölümlerde patent konusu daha detaylı açıklanmakla beraber koruma süresi bakımından incelemeli patentin süresi başvuru tarihinden itibaren 20 yıl iken incelemesiz patentte bu süre 7 yıl olarak öngörülmüştür (Pat.KHK md.72). Faydalı model ve entegre devre topoğrafyalarında 10 yıl, tasarımlarda ise beş yıllık dönemler halinde azami 25 yıl koruma süresi tanınmıştır. Yeni bitki çeşitlerinde de 25 yıllık bir koruma sağlanmakla birlikte bazı özel bitkiler (ağaçlar, asmalar ve patates) için süre 30 yıla kadar uzamaktadır.

(2) Ülkesellik İlkesi

Ülkesellik ilkesi, fikri ve sınai mülkiyet hakları ile bu hakların bulunduğu ülke arasındaki bağı ifade etmek için kullanılmaktadır. Kendisinden koruma talep edilen her devlet bir buluşun, tasarımın vb fikri ürünlerin hangi şartlar altında tescilleneceğini kendisi belirler. Ayrıca bu haklar üzerinde yapacağı tasarrufları, tecavüz teşkil eden fiillerin neler olduğunu ve bunların sonuçlarını da belirler. Ancak bir devletin kanunlarının sağlamış olduğu koruma yalnız bu devletin ülkesi ile sınırlıdır. Bu prensibin bütün devletler tarafından kabul edilmesinin gerekçesi olarak,

TASNİF DIŞI

devletlerin ekonomi politikaları üzerindeki egemenliklerini sürdürmek istemeleri gösterilmektedir (Erdem, 2003, s.46-48).

Türkiye’de fikri mülkiyet korumasından yabancılar da yararlanmaktadır. Türk vatandaşlarına kanunen veya fiilen patent veya faydalı model belgesi koruması tanıyan devletlerin uyruğundaki gerçek veya tüzel kişiler de, karşılıklılık ilkesi uyarınca Türkiye’de de korumadan yararlanabilmektedir (Pat.KHK md.2).

(3) Gerçek Hak Sahipliği İlkesi

Ülkeler, buluş ya da eser sahiplerini ve özgün tasarım geliştirenleri ödüllendirerek yeni ürünler için teşvik etmektedirler. Bu yüzden fikri ürünü ilk kez bulan kişi aksi sabit oluncaya kadar korumadan faydalanır. Fikri mülkiyet hukuku gerçek hak sahiplerini korumak için oluşturulmuştur (Karahana, Suluk, Saraç ve Nal, 2011, s.9-10).

Buluş, birden çok kişi tarafından birlikte gerçekleştirilmişse ve gerçek hak sahibi taraflar başka türlü kararlaştırmamışsa bu kişilerin tamamına ait olur. Aynı buluş birbirinden bağımsız birden çok kişi tarafından aynı zamanda gerçekleştirilmişse, patent isteme hakkı, daha önce başvuru yapana veya diğerine göre rüçhan hakkı olana aittir. Patent almak için ilk başvuran kişi, aksi sabit oluncaya kadar, patent isteme hakkının gerçek sahibidir (Pat.KHK md.11).

(4) Rüçhan (Öncelik) İlkesi

Ülkesellik ilkesi gereğince fikri mülkiyet koruması tescil edilen ülke ile sınırlıdır. Diğer ülkelerde aynı ürün üzerinde hak iddia edebilmek için bu ülkelerin her birinde başvuru ve tescil yapılması gerekmektedir. Ancak tescil işleminin aynı anda farklı ülkelerde yapılamaması koruma açısından çeşitli sorunlara yol açmaktadır. İlk ülkede yapılan tescil başvurusu ile diğer ülkelerde yapılan tesciller arasında geçen zaman, sınai hakkın başkaları tarafından kullanılması ya da tescil edilmesi riskine yol açmaktadır. Özellikle uluslararası alanda hak sahiplerinin mağdur olmamaları ve bu gibi olumsuzluklarla karşılaşmamaları için “rüçhan ilkesi” getirilmiştir (Demirci, 2009, s.29-30). Rüçhan hakkı öncelik hakkı anlamına gelmektedir. Buluş sahibine, ilk patent başvurusunun herhangi bir ülkede yapılması tarihinden itibaren 12 aylık bir süre içinde aynı buluş için başka bir ülkede başvuru yapma hakkı sağlamaktadır. İlk defa başvuru yapacaklar için rüçhan hakkı söz konusu değildir. Daha önce yapılmış başvurular için rüçhan (öncelik) hakkı söz konusudur. Yabancı ülkelerde patent verilmesi için yapılan bir başvurunun farklı ülkelerde yapılmış olmasına bakılmaksızın birden çok rüçhan hakkı talebinde bulunulabilir (TPE, 2012b).

(5) Ön Kullanım Hakkı

Ön kullanım hakkının tanınmasındaki amaç, patente konu olan buluşu tescil ettiren kişilerden bağımsız ya da habersiz olarak, söz konusu buluşla ilgili çalışmalar yapan veya buluşu kullanmaya başlayan iyi niyetli kişilerin yatırım ve emeklerinin boşa gitmesini önlemektir. Bu durumda olan kişiler buluşu kendi işletmelerinin sınırları içerisinde menfaat dengesine uygun olacak şekilde kullanabilirler. Ancak ön kullanım hakkı, patent sahibine sağlandığı gibi mutlak bir hak olmayıp sadece belirli koşullarda kullanılabilen nisbi bir haktır. Ön kullanım hakkına sahip olabilmek için “bu hakkın sahibi olduğunu iddia eden kişinin buluşa zilyet olması, buluşu ülke içinde kullanmaya başlamış olması veya kullanmak için ciddi hazırlıklar yapması, bu kullanımın iyiniyetli olması” gerekmektedir (Çağlar, 2006, s.81- 82).

(6) Tükenme İlkesi

Fikri mülkiyet üzerinde hak sahibi bulunan kişinin bu ürünleri piyasaya sürmesinin ardından bundan sonraki satışlara müdahale edememesine “tükenme ilkesi” denilmektedir. Bu ilke “ilk satış doktrini” olarak da adlandırılmaktadır. Herhangi bir ürünü satın alan toptancı firma, ürün sahibinin izni olmaksızın bu ürünü perakendecilere onlar da tüketicilere satabilir. Zira satın alma sonucu mülkiyet alıcıya geçmiştir. Ancak ilkenin uygulanabilmesi için “satışı yapılan ürün orijinal olmalı ve hak sahibi tarafından veya onun izniyle piyasaya sunulmalıdır” (Karahan, Suluk, Saraç ve Nal, 2011, s.14-15). Satış sonrası mülkiyet alıcıya ait olmakla beraber bu durum alıcıya; ürünü kopyalama, kamuya ödünç verme, değiştirme, yeniden üretme ve yayınlama gibi haklar sağlamaz (Nart, 2009, s.127). Başka bir ülkede piyasaya sürülen ürünle ilgili ülkesel, bölgesel ve uluslararası olmak üzere üç tür tükenme söz konusudur.

Ülkesel Tükenme: Hak sahibi veya onun izin verdiği kişilerce ürünün piyasaya sürülmesinin ardından aynı ülke içinde devam eden satışlara hak sahibinin müdahale edememesine ülkesel tükenme denilmektedir. Burada hak sahibinin hakkını tükettiği alanı ülke sınırları oluşturmaktadır. Bu ilke paralel ithalatı³ önlediği gibi hak sahibine değişik ülkelerde farklı fiyat ve satış politikası izleme imkânı sağlamaktadır (Süel, 2007, s.46-48).

³ “ Marka sahibi ya da onun rızası dâhilinde üçüncü bir kişi tarafından ülke dışında piyasaya sunulan orijinal nitelikteki markalı malların marka sahibinden izin alınmaksızın, ülkeye ithali”. Hamdi Yasaman; *Marka Hukuku*, İstanbul, Vedat Kitapçılık, 2004, s. 543.

Bölgesel Tükenme: Bölgesel tükenmede, birkaç ülkenin toprakları tek bir bölge kabul edilmekte ve fikri mülkiyet bu bölge içerisinde tüketilmektedir. AB’de kullanılan yöntem bölgesel tükenmedir. Buna göre AB üyesi herhangi bir devlette ürünün piyasaya sürülmesi halinde ürüne ait mülkiyet, birliğe üye devletlerde de sona ermektedir (Nart, 2009, s.128-129). Örneğin Casio firmasının Hollanda’da piyasaya sürdüğü saatleri satın alan bir kişi, firmadan izin almaksızın bunları herhangi bir AB üyesi ülkede satabilir. Türkiye, AB ile gümrük birliği oluşturmaya rağmen bu bölgeye dâhil değildir (Karahan, Suluk, Saraç ve Nal, 2011, s.16).

Uluslararası Tükenme: Uluslararası tükenme ilkesinde tüm dünya pazarları tek pazar olarak algılanmaktadır. Buna göre ilkenin kabul edilmesi halinde patentli bir mal herhangi bir ülkede piyasaya sürüldüğü takdirde fikri mülkiyet hakkı da evrensel olarak tüketilmiş olur. Üçüncü kişiler bu ürünleri dünyanın herhangi bir noktasında hak sahibinden izin almadan bahse konu ürünü pazarlayabilirler (Süel, 2007, s.50).

Günümüzde ülkeler çoğunlukla ülkesel tükenmeyi tercih etmektedir. Türkiye’de uygulanan hukuk sisteminde de ülkesel tükenme kabul etmiştir. Ancak entegre devre topografyaları bakımından uluslararası tükenme tercih edilmiştir (Karahan, Suluk, Saraç ve Nal, 2011, s.16).

b. Fikri Mülkiyet Alanına Giren Konular⁴

Fikri mülkiyet genel olarak sınai mülkiyet ve telif hakları olmak üzere iki gruba ayrılmaktadır. Patentler, endüstriyel tasarımlar, coğrafi işaretler vb. fikri ürünler sınai mülkiyet kapsamında değerlendirilirken, yazılı edebi ve sanat eserleri telif hakları kapsamında incelenmektedir. Telif hakkı, eserin başkaları tarafından izinsiz kullanımına karşı eser sahibinin haklarını koruyarak eser sahiplerine özel haklar tanımaktadır (TPE, 2012a, s.4). Sınai haklar ise “sanayi ve tarımdaki yeniliklerin, buluşların ve özgün tasarımların ilk uygulayıcıları veya malların üzerindeki işaretlerin sahipleri adına belirli bir süre ile konulan gayri maddi haktır” (Karahan, Suluk, Saraç ve Nal, 2011, s.2). “Sınai” ya da “endüstriyel” kavramının geniş bir açıklaması Paris Sözleşmesinin “Endüstriyel Mülkiyetin Korunması” md.1(3) bölümünde yer almaktadır. Buna göre, sadece sınai ve ticari açıdan uygun olan ürünler değil tarım ve maden sanayi ile bütün üretilmiş ve doğal olan ürünler (şarap, tohum, meyve,

⁴ Fikri mülkiyet haklarının endüstriyel casusluğa hedef olabilecek türlerine yer verilmiştir.

TASNİF DIŐI

mineraller, çiçekler) de sınai mülkiyet kapsamında değerlendirilmelidir (WIPO, 2012, s.5).

FİKRİ MÜLKİYET HAKLARI	
SINAI MÜLKİYET HAKLARI	FİKRİ ve SANAT ESERLERİ (TELİF HAKLARI)
Patentler	İlim ve Edebiyat Eserleri (Bilgisayar Programları Dahil)
Faydalı Modeller	Musiki Eserleri
Tasarımlar	Güzel Sanat Eserleri
Markalar	Sinema Eserleri
Coğrafi İşaretler	İşleme ve Derleme Eserler
Entegre Devre Topografyaları	
Yeni Bitki Çeşitleri	
Biyoteknolojik Buluşlar	
Ticaret Ünvanları ve İşletme Adları	
Alan Adları	
Ticari Sırlar	
Know- How'lar	

Tablo-2:Fikri Mülkiyet Haklarının Çeşitleri

(Kaynak:Sami Karahan, Cahit Suluk, Tahir Saraç ve Temel Nal. Fikri Mülkiyet Hukukunun Esasları.Ankara, Seçkin Yayıncılık, 2011 s.3'den alınarak düzenlenmiştir)

Fikri mülkiyet hakları konusunda hukuk sistemleri arasında çeşitli farklılıklar bulunmaktadır. Yukarıdaki tabloda yer alan ve ilerleyen konularda detaylı olarak anlatılacak olan “ticari sırlar” daha çok Anglo-Sakson hukuk sisteminde kullanılan bir kavram olup Türk ve AB hukuk sisteminde yer almamaktadır. Aynı şekilde know-how'lar için de özel bir yasa düzenlenmemiştir. Ancak fikri bir ürün olarak ticari değer taşımaları nedeniyle sınai mülkiyet kapsamında değerlendirilmektedir.

(1) Patent ve Buluőlar

İnsanoğlunun yaratmış olduđu medeniyet buluşlarla gelişmiş ve gelişmeye de devam etmektedir. Buluş ve yenilikler toplumsal ilerlemenin ayrılmaz bir parçası olmasına karşın, bu konuda emeđi geçenlere ait hakların korunması fikri 20. yüzyıla kadar tam olarak yaygınlaşmamıştır. Özellikle sınai haklarda yaşanan anlayış deđişimi sonucu buluşlar, idari bir belgeye bağlanarak buluş üzerindeki hakların ispat aracı olarak hukuk düzeninde yer almıştır (Topçu, 2007, s.138-139). Esasında Latince kökenli bir kelime olan patent terimi “açık olmak” anlamına gelmektedir. Önceleri yalnızca kralın tanımış olduđu imtiyazları belirtmek için kullanılan “açık mektup (letters pattern)” kavramı zamanla buluşlar üzerindeki hakkı tanıyan, kapsamını belirleyen ve ispatlayan resmi bir belge olarak algılanmıştır. Türkiye’de ise patent kavramı ilk kez 1879 tarihli İhtira Beratı Kanununda “ihtira beratı” olarak kullanılmıştır. İhtira terimi “benzeri görülmemiş şey icat etme, vücuda getirme” anlamına gelirken, berat terimi ise “imtiyaz verildiđini bildiren fermanı” ifade etmektedir. 551 sayılı Pat.KHK ile birlikte Türk hukuk sisteminde de “patent” kelimesi yer almıştır (Karahan, Suluk, Saraç ve Nal, 2011, s.199).

Patentin konusu buluştur. Buluş ise bir ürün ya da yöntemle ilgili probleme getirilen teknik çözümdür. Teknolojik, ekonomik ve sosyal alanda ilerlemeyi sağlamak için buluşlar patent belgesi ile koruma altına alınırlar. Fikri bir ürün olan buluş ile fikri mülkiyet hakları çerçevesinde deđerlendirilen patent hakkı arasında önemli bir ayrım vardır. Patent, buluş sahibi kişiye ürünü ile ilgili kullanabilme, üretebilme satabilme veya ithal edebilme gibi ayrıcalıklar sağlayan mutlak bir haktır. Bu hakkın resmi olarak gösterimi Patent Tescil Belgesi ile sağlanır (Alper, 2011, s.155). Bir buluşun patent alabilmesi için gereken şartlar kanunlarla düzenlenir. Pat.KHK’nın 5’inci maddesine göre bir buluşa patent verilerek korunabilmesi için;

- Yeni olması,
- Tekniđin bilinen durumunu aşması,
- Sanayiye uygulanabilir olması gerekmektedir.

Pat.KHK’nın 6’ncı maddesinde patent verilemeyecek buluşlar düzenlenmiştir. Buna göre;

- Keşifler, bilimsel teoriler ve matematiksel formüller,
- Zihni, ticari ve oyun faaliyetlerine ilişkin plan, usul ve kurallar,
- Edebiyat ve sanat eserleri, bilim eserleri, estetik niteliđi olan yaratmalar, bilgisayar yazılımları,

TASNİF DIŐI

- Bilginin derlenmesi, düzenlenmesi, sunulması ve iletilmesi ile ilgili teknik yönü bulunmayan usuller
- İnsan ve hayvan vücuduna uygulanacak cerrahi ve tedavi usulleri ile insan ve hayvan vücudu ile ilgili teşhis usullerine patent verilmemektedir.

Yukarıda sıralanan maddelere ek olarak, konusu kamu düzenine veya genel ahlaka aykırı olan buluşlar ile bitki veya hayvan türleri veya önemli ölçüde biyolojik esaslara dayanan bitki veya hayvan yetiştirilmesi usulleri patent korumasından faydalanamaz.

Patentler konularına göre, ürün ve usul patenti olmak üzere ikiye ayrılırlar. Ürün patentinde koruma altında olan bizzat ürünün kendisidir. Ancak patentli buluşun kullanılmasıyla elde edilen ürünler koruma kapsamında değildir. Kısaca ürün patenti, bir netice elde etmek için kullanılan buluş için alınan patenttir. Usul patentinde ise bir ürün veya sonucun elde edilmesi için kullanılan yöntem koruma altındadır (Çağlar, 2006, s.79-80).

Patentler, verilmelerinde tercih edilen sisteme göre incelemeli ve incelemesiz patentler olmak üzere iki gruba ayrılmaktadır. Başvuru sahibinin talebi doğrultusunda TPE tarafından yenilik incelemesi yapılmaksızın verilen patentlere “incelemesiz patent” denilmektedir. Ancak inceleme yapıldıktan sonra verilen patentler ise “incelemeli patent” olarak adlandırılmaktadır. Pat.KHK’nin 72’nci maddesine göre; incelenerek verilen patentin süresi başvuru tarihinden itibaren 20 yıl; incelemesiz verilen patentin süresi ise yine başvuru tarihinden itibaren 7 yıldır. İncelemesiz patent, tescil sürecinin kısalığı ve düşük maliyeti nedeniyle avantajlı gözükmeyle beraber nispeten kısıtlı bir koruma süresi sağlamaktadır. İncelemeli patent ise daha uzun bir süre ve maliyet sonunda verilmekle beraber ayrıntılı inceleme sonunda verilmesi nedeniyle daha güvenilir ve korunaklı olmaktadır (Topçu, 2007, s.144).

Milli savunma açısından taşıdığı önem nedeniyle, gizlilik kuralına uyularak verilen ve gizli patent siciline kaydedilen patentler de “gizli patent” olarak adlandırılmaktadır. Hangi buluşların milli savunma için önem taşıyacağı TPE ile Milli Savunma Bakanlığı arasında yapılacak işbirliğiyle tespit edilir. TPE, buluşun milli savunma açısından önem taşıdığı kanısına varırsa, gizlilik süresini beş aya kadar uzatabilir. Patent sahibi, buluşun içeriği hakkında yetkisi olmayan kişilerin bilgi edinmesini sağlayıcı davranışlardan kaçınmakla yükümlüdür (Pat.KHK md.125).

TASNİF DIŞI

Patent başvurusu Türkiye’de TPE’ye yapılmaktadır. Bununla beraber uluslararası patent başvuruları Patent İşbirliği Anlaşması (Patent Cooperation Treaty-PCT) veya Avrupa Patent Sözleşmesi (European Patent Convention-EPC) uyarınca da yapılabilir.

ÜLKE	2005	2006	2007	2008	2009
ABD	390.733	425.966	456.154	456.321	456.106
Japonya	427.078	408.674	396.291	391.002	348.596
Çin	173.327	210.501	245.161	289.838	314.604
Güney Kore	160.921	166.189	172.469	170.632	163.523
Almanya	60.222	60.585	60.992	62.417	59.583
Rusya	32.253	37.691	39.439	41.849	38.564
Kanada	39.888	42.038	40.131	42.089	37.477
Hindistan	24.382	28.928	35.218	36.812	34.287
Avusturalya	23.857	26.003	26.840	26.346	23.681
Türkiye ⁵	1.146	1.232	2.021	2397	2.732

Tablo-3: Dünya Geneline Patent Başvurusunda Önde Gelen İlk Dokuz Ülke ve Türkiye

(Kaynak: WIPO (2011a). IP Facts and Figures. s.12’den alınarak düzenlenmiştir.)

Patent başvuruları ülkelerin gelişmişlik durumu ve ekonomilerinin büyüklüğüne göre değişiklik göstermektedir (Tablo-3). ABD, Japonya ve Çin’de bulunan patent bürolarına yapılan patent başvuruları dünya genelinde yapılan başvuruların %60’ını oluşturmaktadır. Avrupa Patent Ofisine yapılan başvurularla birlikte sıralamada ilk dokuzda yer alan ülkeler ise tüm başvuruların %87’sini oluşturmaktadır (WIPO, 2011a, s.12). 2009 yılı için ülkeler bazında yapılan değerlendirmede 2732 patent ile Türkiye 26’ncı sıradadır (WIPO, 2011a, s.22-24). Yukarıdaki tabloda da görüldüğü üzere Türkiye’nin bu konuda kat etmesi gereken önemli bir mesafe bulunmaktadır. Sanayinin ARGE faaliyetinden uzak durması, hazır teknolojileri alarak kullanması, kaynak yetersizliği, araştırma kültürünün geliştirilmemesi ve patent konusunun taşıdığı değer toplum tarafından yeterince

⁵ Türkiye ile ilgili veriler 13 Mart 2012 tarihinde WIPO Bilgi Portalı: http://www.wipo.int/export/sites/www/ipstats/en/statistics/patents/xls/wipo_pat_appl_from_1883_table.xls adresinden alındı.

TASNİF DIŞI

algılanmaması gibi hususların patent gelişimi konusunda önemli bir engel olduğu değerlendirilmektedir (Ayhan, 2002, s.252).

2010 yılı itibariyle dünyada 7.3 milyon kadar patent bulunmaktadır ve patent lisanslarından elde edilen kazanç önemli oranda artmaktadır. Yaklaşık 2 milyon patent ile ABD bu konuda liderliği elinde bulundurmaktadır. ABD'yi 1.4 milyon patent ile Japonya takip ederken her iki ülkenin patent sayısı dünya genelinin %48'ini oluşturmaktadır (WIPO, 2011b, s.7).

Yüksek kaliteli patentler firmaların değerini arttırırken, güçlü bir patent portföyüne sahip olan şirketler de borsalarda yüksek fiyattan işlem görmektedir. Aynı zamanda işletmelerin fonlama tercihlerinin belirlenmesi aşamasında patentlerin büyük önemi vardır. Alper'e göre, *"İşletmenin sahip olduğu patentlerden gelecekte sağlanacak kazançlar karşılığında, menkulleştirme aracılığıyla yapılandırılan finansal araçlar ihraç edilerek, patentler stratejik anlamda fonlama aracı olarak kullanılabilir." Bununla birlikte gerçekçi bir yaklaşımla doğru değerlendirilen patentler de hisse senedi fiyatlarını olumlu yönde etkilemektedir (Alper, 2011, s.154).*

(2) Faydalı Model

Faydalı model tekniğin bilinen durumunu aşmayan, ancak yeni ve sanayiye uygulanabilir buluşları nitelendirmek için kullanılan bir terimdir. Genellikle karmaşık olmayan ve ticari ömrü daha kısa olan ürünler için tercih edilmektedir. Takip edilmesi gereken süreç de patente göre daha basit ve ucuzdur (WIPO, 2012, s.8-9). Patent koruması için aranan "tekniğin bilinen durumunun aşılması" ölçütünün sanayide yapılan bazı küçük buluş ve ilerlemeleri kapsamaması nedeniyle faydalı model koruması bu ihtiyacın giderilmesi için ortaya konmuştur. Örneğin, son derece basit teknik yapısı ve uzmanlık gerektirmeyen kullanımı ile "tel zimba" faydalı model olarak kabul edilebilir. Fakat daha karmaşık ve uzmanlık isteyen bilgi gerektirmesi nedeniyle "jeneratör", patente konu olacaktır. Topçu'ya göre, *"faydalı modelin topluma daha az yararlı olduğu gibi bir kriter çıkarılmamalıdır. Zira kimi zaman çok az teknik bilgi gerektiren basit düzenekler insanlık için büyük önem taşıyabilmektedir" (Topçu, 2007,s.218).*

Faydalı modellerin koruma şartları patentler ile benzerlik taşımaktadır. Ancak her iki koruma arasında da bazı temel farklılıklar bulunmaktadır. Bu farklılıklar şu şekilde sıralanabilir:

TASNİF DIŞI

- Patent hem ürün hem de usul buluşları için verilirken, faydalı model belgesi usuller ve bu usuller sonucunda elde edilen ürünler ile kimyasal maddeler hakkında verilemez.
- Tekniğin bilinen durumunun aşılması şartı faydalı modeller yönünden aranmadığından, patentler için TPE tarafından düzenlenmesi gereken araştırma raporu, kural olarak faydalı modeller için düzenlenmez.
- Patentın korunma süresi incelemeli patentte 20 yıl, incelemesiz patentte 7 yıl iken, faydalı model 10 yıl süre ile korunur (Karahan, Suluk, Saraç ve Nal, 2011, s.258).

Patent korumasının aksine faydalı model koruması ülkeler bazında görece daha az tercih edilmektedir. WIPO'nun 2011 raporuna göre patent için 135 farklı ofis bulunurken, sadece 60 ülke faydalı model koruma hakkı tanımıştır. Genel olarak patent koruması kullanılırken başka isimler altında da faydalı koruma sağlanabilmektedir. Bahse konu kavram yerine Avusturalya'da "buluş patenti (innovation patent)", İrlanda'da ise "kısa dönemli patent (short term patent)" tabiri kullanılmaktadır (WIPO, 2011b, s.34).

	ÜLKE	2004	2005	2006	2007	2008	2009
1	Çin	112.825	139.566	161.366	181.324	225.586	310.771
2	Almanya	20.286	20.418	19.766	18.083	17.067	17.306
3	Güney Kore	37.753	---	32.908	21.084	17.405	17.144
4	Rusya	8.948	9.473	9.699	10.075	10.995	11.153
5	Ukrayna	5.232	7.286	8.171	---	9.205	9.600
6	Japonya	7.986	11.387	10.965	10.315	9.452	9.507
7	Brezilya	---	3.069	2.984	---	3.218	3.122
8	Türkiye	---	---	---	3.011	2.992	2.882

Tablo-4: Faydalı Model Başvurusunda Önde Gelen İlk Sekiz Ülke

(Kaynak: WIPO (2011a). IP Facts and Figures. s.15'den alınarak düzenlenmiştir.)

Dünya genelinde yapılan faydalı model başvurularına bakıldığında %78'lik oran ile Çin'in açık ara önde olduğu görülmektedir (Tablo-4). Almanya 17.306 başvuru ile ikinci sırada yer alırken Güney Kore 17.144 başvuru ile üçüncü sırada bulunmaktadır. Sıralamada 8'inci sırada olan Türkiye'nin 2009 yılı itibariyle başvuru sayısı 2882'dir (WIPO, 2011a, s.15).

(3) Endüstriyel Tasarımlar

Endüstriyel tasarım, en geniş tanımıyla faydalı bir ürünün dekoratif ya da estetik durumunu ifade eder. Ürünün biçimi, deseni veya rengi de endüstriyel tasarıma konu olabilir. Önemli olan ürünün belirgin bir görünümünün olması ve işlevini yerine getirebilmesidir. Bunun da ötesinde yeniden üretilebilmeli ve sanayiye uygulanabilir olmalıdır. Tasarımın gerçek amacı budur ve bu nedenle endüstriyel tasarım olarak adlandırılmaktadır (WIPO, 2012, s.9). 554 sayılı End.Tas.KHK'ya göre ise; *“tasarım, bir ürünün tümü, veya bir parçası veya üzerindeki süslemenin, çizgi, şekil, biçim, renk, doku, malzeme veya esneklik gibi insan duyuları ile algılanan çeşitli unsur veya özelliklerinin oluşturduğu bütünü ifade eder.”*

Tasarım, aynı sektörde faaliyet gösteren firmalar açısından müşteri tercihlerinin kendi ürünlerinde yoğunlaşmasını sağlayan önemli unsurlardan biridir. Özellikle küçük ve orta ölçekli işletmeler tasarım yolu ile ürün yelpazesini genişleterek bir rekabet avantajı yakalamak istemektedirler. Yapılan pazar araştırmaları da, tüketici ürün tercihinde marka, kalite, fiyat gibi unsurlarla birlikte ürünlerin dış görünümünün de oldukça etkili olduğunu göstermektedir. Bu nedenle ergonomik, estetik niteliğe sahip ve yeni tasarımlar ortaya çıkarmak, fikir sahiplerine gün geçtikçe artan kazanımlar sunmaktadır. Bunun yanında bir tasarımın başarılı olması ise hayal gücüne, büyük emek ve yatırımlara dayanmaktadır (TPE, Ekim 2011, s.1).

Tasarım korumasının var olabilmesi için fikrin üründe somutlaşması gerekmektedir. Buna göre, fotoğraf, çizim hatta eskiz gibi tasarımın ürüne yansımaları gösteren her türlü çalışma da bu korumadan faydalanabilir. Burada aranan en önemli özellik bakan veya dokunan kişi tarafından algılanabilir olmasıdır. End.Tas.KHK m.3/b hükmünde ürün olarak şunlar sayılmıştır:

- Nesneler,
- Bileşik sistem veya bu sistemin parçaları
- Setler,
- Takımlar,
- Ambalajlar,
- Birden çok nesne veya sunuşun bir arada algılanabilen bileşimleri,
- Grafik semboller,
- Tipografik karakterler (Yazı karakterleri)

TASNİF DIŞI

Ancak End.Tas.KHK'da bilgisayar programları ile yarı iletkenlerin topografyaları (çipler) ürün olarak kabul edilmemiştir (Karahan, Suluk, Saraç ve Nal, 2011, s.266).

Patent ve faydalı modelde olduğu gibi tasarımların tescil işlemleri de TPE tarafından yapılmaktadır. Endüstriyel tasarımların tescil edilmesinde yeni ve ayırt edici nitelikte olması aranmaktadır. Yapılan tescil işleminin koruma süresi beş yıldır. Anılan süre beşer yıllık dönemler halinde yenilenmek üzere toplam 25 yıla kadar uzatılabilmektedir.

	ÜLKE	2005	2006	2007	2008	2009
1	Çin	163.371	201.322	267.432	312.904	351.342
2	Güney Kore	44.957	51.039	54.362	56.750	57.903
3	Almanya	52.544	54.505	57.799	50.135	54.304
4	Japonya	39.254	36.724	36.544	33.569	30.875
5	ABD	25.553	25.515	27.752	27.782	25.806
6	Türkiye	5.551	6.339	6.868	7.243	7.114

Tablo-5: Endüstriyel Tasarım Başvurusunda Önde Gelen İlk Altı Ülke

(Kaynak: WIPO (2011). IP Facts and Figures. s.20'den alınarak düzenlenmiştir.)

Çin 2009 yılında Çin'de yapılan 351.342 endüstriyel tasarım başvurusu dünya genelinde yapılan başvuruların %50'sini oluşturmaktadır. Türkiye ise altıncı olmasına rağmen yapılan başvuru sayısı 7114'tür (Tablo-5).

(4) Entegre Devre Topoğrafyaları

1947 yılında Bardeen, Brattain ve Shockley adlı üç fizikçi tarafından New Jersey'de bulunan Bell Laboratuvarında transistörün icat edilmesi, halk arasında çip olarak bilinen yarı iletken ürün endüstrisinin temelini atmıştır. 1957 yılında elektronik devrelerin silikon parçasına yerleştirilmesiyle oluşan entegre devreler mikro-elektronikte dönüm noktası olmuştur. Elektronik devrenin bulunması teknolojiyi de tetiklemiştir. 1959 ile 1962 arasında yarı iletkenlerin fiyatı %65 gerilerken üretim de 20 kat artmıştır. 1971'de üretilen bir çipte 2.300 transistör yer alırken 1993'te aynı büyüklükte bir çipte 35 milyon transistör bulunuyordu. Gün geçtikçe küçülen ve daha güçlü hale gelen çipler; bulaşık makinalarından mikro dalga fırınlara, otomobillerden

TASNİF DIŞI

bilgisayarlara uzanan geniş bir yelpazede tüm araç ve cihazların ayrılmaz parçası olmuştur (Castells, 2008, s.51-53).

Entegre Devre Topografyalarının Korunması Hakkında Kanuna (EDTK) göre entegre devre; elektronik bir işlevi veya benzeri diğer işlevleri yerine getirmek üzere tasarlanmış, en az bir aktif elemanı olan ve ara bağlantılarından bir kısmının ya da tümünün bir parça malzeme içerisinde veya üzerinde bir araya getirilmiş ara veya son formdaki üründür. Entegre devrelere çeşitli kaynaklarda çip, yonga ya da yarı iletken adı da verilmektedir. Entegre devre topoğrafyası ise entegre devreyi oluşturan tabakaların üç boyutlu dizilimini gösteren, üretim amacıyla hazırlanmış ve herhangi bir formatta sabitlenmiş görüntüler dizisi olup, her görüntü entegre devrenin üretiminin herhangi bir aşamasındaki yüzeyinin tamamının veya bir kısmının görünümüdür.

Entegre devreler uzmanlık ve mali kaynak gerektiren büyük yatırımlar ile üretilmektedirler. Daha çok işleve sahip ancak daha az yer kaplayan entegre devrelere yönelik talep gün geçtikçe artmaktadır. Entegre devreler küçüldükçe alandan tasarruf edilmekte ve üretimi için daha az malzeme kullanılmaktadır. Bilgisayar, saat, televizyon, araba vb. pek çok üründe çiplerden faydalanılmaktadır. (WIPO, 2012, s.11).

Entegre devre topoğrafyaları tüm dünyada kendine özgü (sui generis) haklarla korunmaktadır (Jain, Kaur ve Jain, 2010, s.315). Türkiye'deki tescil işlemleri TPE tarafından yapılmaktadır. Bütün olarak ele alındığında orijinallik şartını taşıyanlar korumadan yararlanmaktadır. Tasarlayıcısının kendi fikrî çabası sonucu ortaya çıkan ve diğer üreticilerce bilinmeyen entegre devre topoğrafyaları orijinal sayılmaktadır.

(5) Yeni Bitki Çeşitleri

Yeryüzündeki canlıların hayatını devam ettirebilmesinde gerekli gıda büyük oranda bitkilerden sağlanmaktadır. Aynı zamanda ilaç, yağ, boya gibi alanlarda da bitkilerden büyük oranda faydalanılmaktadır. Yaşanan hızlı nüfus artışı beslenme sorunlarına da yol açmaktadır. Bu doğrultuda daha verimli, kaliteli zararlılara karşı dayanıklı ürünler elde edilmesi amacıyla bitkiler üzerinde araştırma yapılmaya başlanmıştır. Klasik bitki ıslahı uygulamaları gıda üretiminde kullanılan pek çok besin maddesinde uzun yıllar boyunca uygulanmaktadır. Örnek vermek gerekirse, öğütülerek un haline getirilen buğday tanelerinin geçmişte fındık gibi kabuklu olduğu, ıslah çalışmalarıyla bugünkü halini aldığı bilinmektedir. Son yıllarda genetik

TASNİF DIŞI

mühendisliğinde kaydedilen ilerlemeler yeni bitki türlerinin elde edilmesinde de kullanılmaktadır (Ulukan, 2007, s.28).

5042 sayılı Yeni Bitki Çeşitlerine Ait İslahçı Haklarının Korunmasına İlişkin Kanun (BÇK)'a göre; bitkiye türünde olmayan özellikleri kazandırmak için yapılan iyileştirmelere ıslah; yeni bitki çeşidini ıslah eden veya bulan ve geliştiren kişi ıslahçı olarak adlandırılmaktadır. Kendine özgü bir fikri mülkiyet olan ıslahçı hakkı ile kişiye belirli bir süre kullanma hakkı verilmektedir (Karahan, Suluk, Saraç ve Nal, 2011, s.320).

Koruma süresi ıslahçı hakkının tescilinden itibaren yirmi beş yıldır. Bu süre ağaçlar, asmalar ve patates için otuz yıl olarak tespit edilmiştir. Türkiye’de ıslahçı hakkının tanınması amacıyla başvurunun yapılacağı yetkili makam Gıda, Tarım ve Hayvancılık Bakanlığıdır.

(6) Know-How

Know-how, patent verilemeyen faydalı ve önemli teknik bilgiler için kullanılan bir kavramdır (Shearer, 2007, s.226). İlk defa ABD’de ortaya çıkan terim, “nasıl yapıldığını bilme” anlamına gelen “know how to do it” cümlesinin kısaltmasıdır (Karahan, Suluk, Saraç ve Nal, 2011, s.395). Sonradan Kıta Avrupası hukuk sistemine de dâhil olan kavramın kapsamı konusunda farklı yaklaşımlar bulunmaktadır. Amerikan hukuk sisteminde ekonomi, spor, teknik, kültür gibi çok geniş bir yelpazede kullanılan know-how, Türkiye de dâhil olmak üzere Kıta Avrupası hukuk sisteminde sınırlı olarak teknik, ticari ve sınai alanlarda kullanılmaktadır (Erbay, 2002, s.57).

Know-how’un Türkiye’deki kullanımı Rekabet Kurumu tarafından yürürlüğe sokulan 2002/2 no.lu Dikey Anlaşmalara İlişkin Grup Muafiyeti Tebliğinde ifade edilmiştir. Buna göre know-how; *“sağlayıcının tecrübe denemeleri sonucu elde ettiği ve patentli olmayan, uygulamaya yönelik, gizli, esaslı ve belirlenmiş bilgi paketi anlamına gelir”* (m.3/f). Gizli kavramı, know-how’un bir bütün halinde veya parçaları birleştirildiğinde dahi herkes tarafından bilinmemesini ya da kolaylıkla erişilebilir olmamasını ifade etmektedir. Esaslılık ise, anlaşma konusu malların veya hizmetlerin kullanılması, satımı veya yeniden satımı bakımından alıcı için vazgeçilmez bilgilerin niteliğidir. Belirlenmiş olmada, know-how’un gizli ve esaslı olma şartlarını taşıdığını doğrulayabilmek için, geniş kapsamlı ve ayrıntılı bir şekilde tanımlanmış olması aranmaktadır.

TASNİF DIŞI

Günümüzde rekabet avantajını kaybetmek istemeyen ancak ARGE faaliyetlerine de yeteri kadar kaynak ayıramayan işletmeler bu açıklarını gidermek için sözleşme yoluyla başka işletmelerin üretim sırlarını satın alabilmektedirler. Ticari değeri olan know-how bilgileri için de işletmeler arasında “know-how sözleşmesi” yapılmaktadır. Örnek vermek gerekirse, aynı makine ve araçlarla bir malın daha seri şekilde üretilmesi veya işletmenin idaresinde maliyetleri düşüren bir çeşit bilgi de sözleşmeye konu olabilmektedir (Kırca, 1998, s.246).

c. Ticari Sırrın Unsurları ve İlgili Kavramlar

Türk hukuk sisteminde yer almayan ticari sırlar, bağımsız bir ekonomik değeri olan, ekonomik faaliyetlerde sahibine rekabet avantajı sağlayan, aleni olmayan ve sahibinin gizli kalmasını istediği her türlü bilgi olarak tanımlanmaktadır (Bilge, 2005, s.5). Yenilik veya faydalı olma gibi özellikler ticari sırlarda aranmamaktadır (Erkal, 2004, s.429). Ticari sır, Kıta Avrupa’sından ziyade Anglo-Sakson hukuk sisteminde kullanılan bir kavramdır. Planlar, prototipler, müşteri ve tedarikçi bilgileri, numuneler, üretim süreçleri, kimyasal formüller, depolama ve dağıtım yöntemleri, maliyet ve fiyatlandırma bilgileri, makine çizimleri, pazarlama teknikleri, personel kayıtları, mühendislik raporları, iş metotları, ürün test sonuçları, vb. pek çok husus ticari sırlara örnek olarak gösterilebilir (Usluel, 2009, s.27).

Türk hukuk sisteminde ticari sırları nitelendirmek üzere Borçlar Kanununda “iş sırları” (m.348), Ticaret Kanununda “imalat veya ticaret sırları” (m.57/1-7,8), İş Kanununda “meslek sırrı”, 6102 sayılı Ticaret Kanununda ise “üretim ve iş sırları” (m.55/1-b) terimleri yer almaktadır. Fakat kavramlar arasında bir uyum bulunduğunu söylemek oldukça güçtür. Türk ve AB hukuk sistematğinde ticari sırlar fikri mülkiyet hakkı olarak kabul edilmemektedir. Bu yüzden çeşitli yasalarda ticari sırlara ilişkin doğrudan ya da dolaylı nitelendirmeler bulunsa da, patent ve tasarımlara sağlanan fikri mülkiyet koruması burada söz konusu değildir (Karahana, Suluk, Saraç ve Nal, 2011, s.395).

Ticari sır koruması ile fikri mülkiyet koruması arasında seviye ve kapsam açısından önemli farklılıklar bulunmaktadır. İlk olarak bir buluşun patent korumasından yararlanabilmesi için yeni olması, tekniğin bilinen durumunu aşması ve sanayiye uygulanabilir nitelikte olması gerekmektedir. Ticari sır korumasında ise bu özellikler aranmamakla birlikte buluşun kamu tarafından bilinmemesi ve sahibine rekabet avantajı sağlaması gibi hususlar gözetilmektedir. Bu yüzden ticari sır korumasından yararlanan bilgiler çoğu zaman patent şartlarını taşımamaktadır (Erkal, 2004, s.430).

TASNİF DIŐI

İkinci fark ise buluşlarla ilgili bilgilerin kamuya açıklanmasında yatmaktadır. Fikri mülkiyet hukukundaki bilgiler tescillenerek topluma açıklanmaktadır. İncelemeli patent olarak tescillenen bir ürün 20 yıl, faydalı model ise 10 yıl sonra kamuya açık hale gelmektedir. Ancak ticari sır koruması altındaki bilgiler açıklanmadığı gibi bilgi sahibi kişi tarafından gizli olarak tutulmaya devam edilmektedir (Bilge, 2005, s.5). Örneğin Coca Cola'nın formülü 1886 yılından beri ticari sır olarak saklanmaktadır. Üreticiler sır olarak saklayabildikleri ölçüde de gizli kalmaya devam edecektir (Ramcharan, 2005,s.138). Bu yüzden tescillenerek patent verilen bir ürün koruma süresi sonunda açıklanacak olması nedeniyle ticari sır olarak değerlendirilmemektedir (The Silver Lake Editors, 2004, s.409).

Üçüncü olarak fikri mülkiyet korumasında sınırlı sayı (numerus clausus) ilkesi geçerlidir. Bu yüzden yasal düzenlemenin dışındaki bilgiler fikri mülkiyet hukuku kapsamında değerlendirilmemektedir. Daha önceki konularda da belirtildiği üzere patent, tasarım, faydalı model, entegre devre topoğrafyaları gibi tescille koruma kapsamına alınan hususlar fikri mülkiyet olarak kabul edilmektedir (Bilge, 2005, s.54).

Son olarak ticari sır ve fikri mülkiyet arasındaki diğer bir fark da korunma maliyetinden kaynaklanmaktadır. Patent başvurularının incelenmesinde başvuru sahiplerinden ücret alınmaktadır. He ne kadar patent belgesi ürünle ilgili buluş sahibine önemli ayrıcalıklar sağlasa da inceleme masrafları nedeniyle patent koruması daha maliyetli olabilmektedir (Erkal, 2004, s.430-431). Örneğin ABD'de patent maliyetleri 15.000-30.000 dolar arasında seyrederken bu rakam bazen daha yüksek miktarlara da çıkabilmektedir. Bununla birlikte buluş sahibinin ticari sır korumasından yararlanabilmesi için gizli kalmasını istediği bilginin korunmasına yönelik çeşitli tedbirler (fiziksel önlemler, gizlilik sözleşmesi vs.) alması da gerekmektedir (Ramcharan, 2005,s.138).

(1) Ticari Sırrın Unsurları

Bilgi, ticari nitelikte olma, sır olma ve sır olarak saklama iradesi ticari sırrın unsurlarını oluşturmaktadır.

(a) Bilgi

Ticari sır kavramının var olabilmesi için ilk koşul "bilgi"dir. Bilginin basit ya da karmaşık bir yapıda olması, fikri mülkiyet korumasından yararlanması, yazılı olması, anlamının kolay ya da zor olması gerekmez. Ancak bilginin doğru olması gerekir. Zira yanlış bilgi ile rekabet avantajı elde edilemez (Bilge, 2005,s.16-17).

TASNİF DIŐI

Başarısızlıkla sonuçlanan bilgiler (negative know-how) de ticari sır olarak kabul edilmektedir. Örneğin bir işletme yeni ürün üzerinde başarısızlıkla sonuçlanan 40 farklı formül denemesinde bulunsun. 41'inci denemesinde başarılı olduđu takdirde, bulduđu sonuç kadar, araştırma faaliyeti için kaynak ayırdıđı başarısız denemeleri de ticari sır konu olacaktır. Zira başarısız sonuçlardan haberdar olan rakip işletmeler, bu denemeleri yapmayacağından dolayı zaman ve maliyetten tasarruf ederek aradaki farkı kapatabilirler (Shearer, 2007, s.86).

(b) Ticari Nitelikte Olma

Herhangi bir bilginin ticari sır özelliđi kazanabilmesi için ticari nitelikte olması gerekmektedir. Bu doğrultuda bahse konu bilgi, işletmenin kendisi veya faaliyetleri ile ilgili olmalıdır. Ticari niteliđi bulunmayan kişisel sırlar, bilimsel bilgiler veya devlet sırları, ticari sır kapsamında değerlendirilmezler (Karahan, Suluk, Saraç ve Nal, 2011, s.404). İşletme ile ilgili olan; üretim süreci, hammadde kaynakları, yatırım planları, personel yönetimi, aleni olmayan finansal veriler, organizasyon biçimi stok bilgileri, müşteri listeleri, fiyat bilgileri, formüller vb. bilgiler rekabet avantajı sağlıyorsa ticari sır olabilir (Bilge, 2005, s.18).

(c) Sır Olma

Sır olma özelliđi, bir bilginin ticari nitelik kazanması için gereken en önemli unsurdur. Herkesçe bilinen, önemli zahmetlere katlanmaksızın normal yollardan elde edilen ya da kamuya açıklanan bilgiler ticari sır değildir. Açıklandığı halde kamu tarafından henüz öğrenilmeyen; resmi kurumlarca kayda alınan işletmeye ait vergi ve bilanço bilgileri, çalışan sayıları, ithalat-ihracat rakamları gibi bilgiler de ticari sır olarak kabul edilmemektedir (Karahan, Suluk, Saraç ve Nal, 2011, s.404).

Bazı durumlarda işletmeler rakiplerine ait ticari sırlara yasal yollardan ulaşılabilir. Tersine mühendislik yöntemi kullanarak, uzun ve maliyetli araştırmalar sonucu belirli bir ürünün ticari sırrına ulaşan işletmeler de bu ürüne ait ticari sırra sahip olmaktadır. Zira yapılan araştırma sonucu elde edilen bilgiler her iki işletme tarafından bilinen ticari sır olarak kabul edilir. Kamuya açıklanmış sayılmaz (Quinto ve Singer, 2009, s.15).

(ç) Sır Olarak Saklama İradesi

Ticari sır sahibinin bilginin gizli kalması konusunda makul tedbirler alması ve belli bir irade göstermesi gerekmektedir. Gizli tutma iradesi açık ya da örtülü şekilde olabilir. Çalışanlarla sır tutma sözleşmesi yapılması, işyerlerine asılan yazılı güvenlik uyarıları, kameralı güvenlik sistemleri, belirli yerlere giriş için belirli personele yetki

TASNİF DIŞI

verilmesi, bilgisayarlara şifre konulması gibi uygulamalar sır saklama iradesine örnek olarak gösterilebilir.

Sır olarak saklama iradesinde, ticari sır sahibinin, sırrın korunmasında haklı menfaatinin bulunması gerekmektedir. Örneğin hukuka aykırı hükümler içeren bir fiyat anlaşması sır olarak saklanması bu bilgiye ticari sır anlamı yüklemes (Bilge, 2005, 26-31).

(2) Ticari Sırla İlgili Kavramlar

Ekonomik değeri olan gizli bilgileri ifade etmek amacıyla çeşitli kavramlar kullanılmaktadır. Müşteri sırrı, meslek sırrı, iş sırrı, ticari sır gibi kavramlar arasında kesin çizgilerle belirlenmiş net bir ayrım bulunmamaktadır. Uşan'a göre, *“aynı durumu karşılamak üzere kimi zaman imalat sırrı, kimi zaman ticari sır kimi zaman da mesleki sırrı kavramları kullanılabilir.”* Bu kavram karmaşası diğer ülkelerde olduğu gibi Türkiye’de de yaşanmaktadır (Uşan, 2003, s.26).

(a) İşletme Sırrı

Ticari nitelik taşıyan gizli bilgileri ifade etmek için kullanılan kavramlardan biri de “işletme sırrı”dır. Daha çok Alman hukukunda kullanılan bu kavram “iş ve işletme sırları (betriebs und geschaeftsgeheimniss) şeklinde kullanılmaktadır. Kamuya açık olmayan, işletme sahibinin iradesi altında kendisine ekonomik fayda sağlayan ve gizli kalması gereken bir işletme ile ilgili tüm olaylar bu kapsamda değerlendirilmektedir. Genel iş ilişkileri ile ilgili konularda iş sırları kullanılırken, işletme sırları teknik konuları içermektedir. Teknik sırlar ve gizli usul gibi kavramlar da eş anlamlı olarak kullanılabilir. Kavramların hem teknik hem de ticari nitelik taşımaları karmaşaya yol açmaktadır. Bu yüzden Alman Rekabet Hukuku Kanununun 17’inci maddesi “iş ve işletme sırlarını” hukuken eşit olarak görmektedir. (Bilge, 2005, s.33).

(b) Meslek Sırrı

Meslek, kişilerin yaşamlarını sağlamak için bulundukları faaliyete verilen isimdir (Donay, 1978, s.7). Meslek sırrı ise mesleğin icrası sırasında meslek sahibi tarafından öğrenilen gizli bilgilerdir Bu sırlar, müşterilerle ilgili özel bilgiler olabileceği gibi meslekle ilgili tecrübe edilen ve geliştirilen gizli bilgiler de olabilir (Kaplan,1990, s.4-5).

Meslek sırrı kavramına; avukat-müvekkil ilişkilerinde avukatların, hasta doktor ilişkisinde doktorların, banka-müşteri ilişkisinde banka çalışanlarının durumları örnek olarak gösterilebilir (Usluel, 2009, s.49-50).

(c) Müşteri Sırrı

İşletmelerin, ticari faaliyet sırasında öğrendikleri müşterileri ile ilgili gizli bilgiler müşteri sırrı olarak nitelendirilmektedir. Müşterilere ait kişisel, mali, doğrudan ya da dolaylı tüm kayıt, belge ve bilgiler müşteri sırrı kapsamındadır.

Müşterilerin menfaatlerinin korunması açısından bu sırların gizli tutulması son derece önemlidir. İşletme tarafından bilgilerin ifşa edilmesi, müşteri sırrının ihlali durumunu ortaya çıkartır (Bilge, 2005, s.34-35). Türk Ceza Kanununun 239'uncu maddesine göre, *“sıfat veya görevi, meslek veya sanatı gereği vakıf olduğu ticarî sır, bankacılık sırrı veya müşteri sırrı niteliğindeki bilgi veya belgeleri yetkisiz kişilere veren veya ifşa eden kişi, ... bir yıldan üç yıla kadar hapis ve beş bin güne kadar adli para cezası ile cezalandırılır.”*

(ç) İş Sırrı

İş sırrı, iş ve işyeri ile ilgili imalat ve ticari sırlar da dâhil olmak üzere her türlü gizli bilgiyi barındıran oldukça geniş bir kavramdır. İşyerinde kullanılan bir bilginin sır olarak kabul edilebilmesi için;

- Sır olması,
- İşverenin gizli tutma iradesinin bulunması,
- İşle ilgili olması,
- İşverenin haklı menfaatinin varlığı, gibi ölçütleri taşıması gerekmektedir (Uşan, 2003, s.28-36).

İşverenin yaptığı iş nedeniyle elde ettiği ve üçüncü kişilere ait gizli kalması gereken bilgiler de iş sırrı kapsamında değerlendirilmektedir. Örnek vermek gerekirse, bir muhasebecinin yanında çalışan işçinin, müşterilere ait hesap bilgilerini saklama yükümlülüğü bulunmaktadır. Ancak işçinin mesleki bilgi ve tecrübesi iş sırrı kapsamının dışındadır. İşçinin yaptığı işte zaman içerisinde kazandığı ve kendisinin ayrılmaz bir parçası olan mesleki bilgiler iş sırrı olarak kabul edilemezler (Uşan, 2003, 32-33).

ç. Fikri Mülkiyet ve Ticari Sırların Korunması ile İlgili Uluslararası Kuruluşlar ve Anlaşmalar

Pazarların bir araya gelerek ekonominin küresel bir nitelik kazanması, sanayinin itici gücü olan ticari sırların uluslararası ortamda korunması ihtiyacını ortaya koymuştur. Bu koruma, özellikle dünya ölçeğinde ticaret yapan ve değerli bilgilere sahip şirketler ile bu şirketlerin katkılarının bulunduğu ülke ekonomileri açısından son derece önemlidir (Bilge, 2005, s.68).

TASNİF DIŞI

Daha önceden de belirtildiği gibi ülkesellik ilkesi gereği patent koruması ulusaldır ve patentler ancak alındıkları ülkelerde hak sahipliği doğurmaktadır. Bu nedenle yurt dışında hiçbir koruma ve hak sağlamazlar. Dünya patenti ya da uluslararası patent gibi bir kavram yoktur. Ancak patentin başka ülkelerde de tescil ettirilmesi mümkündür. Buna ilişkin kolaylık sağlayan Paris Sözleşmesi, Avrupa Patent Sözleşmesi, Patent İşbirliği Anlaşması, Dünya Fikri Mülkiyet Örgütü gibi uluslararası anlaşmalar ve bu konuda aktif olan kuruluşlar mevcuttur (Alper, 2011, s.158).

(1) Paris Sözleşmesi

1873 yılında Viyana’da düzenlenen Uluslararası İcatlar Sergisi (International Exhibitions of Inventions)’ne buluş sahiplerinin ürünlerinin taklit edilebileceği ve başka ülkelerde pazarlanacağı endişesiyle katılmak istememeleri sınai mülkiyet haklarının uluslararası alanda korunması gerekliliği tartışmalarını başlatmıştır. Yapılan müzakereler sonucu 1883 yılında 14 ülke (Belçika, Brezilya, Fransa, İtalya, Hollanda, Norveç, Portekiz, İspanya, İsveç, İsviçre, Tunus, İngiltere, ABD ve Dominik Cumhuriyeti) tarafından imzalanan Paris Sözleşmesi (Paris Convention for the Protection of Industrial Property), sınai mülkiyetin korunması konusunda uluslararası alanda kabul gören en temel anlaşmadır (Bülbül ve Özbay, 2011, s.50). Sınai mülkiyetin anayasası olarak kabul edilen Sözleşme, bugün sınai mülkiyet ile ilgili pek çok yasal düzenlemeye kaynaklık ederek ülkelerin iç hukuklarına da girmiştir. 2012 yılı itibarıyla 174 ülke Sözleşmeye taraftır (WIPO, 2012b). Sözleşmede yapılan değişiklikler tarihsel sıralamaya göre aşağıda yer almaktadır.

- 1890 Madrid,
- 1897 ve 1900 Brüksel,
- 1911 Washington,
- 1925 La Haye,
- 1934 Londra,
- 1958 Lizbon,
- 1967 Stockholm,
- 1979 (Stockholm metni tadil edilmiştir) değişiklikleriyle son halini almıştır.

Türkiye Stockholm metnine 1-12. Maddelerine çekince koyarak 1930’da taraf olmuş ancak bu çekinceleri de 1994’de kaldırmıştır (Topçu, 2007, s.37-38).

1967’de imzalanan sözleşmenin birinci maddesinde: “(1) *Bu Anlaşmayı uygulayan ülkeler sınai mülkiyeti koruma için bir kurum oluştururlar. (2) Sınai mülkiyeti koruma patent, faydalı modeller, endüstriyel tasarımlar, ticari markalar,*

TASNİF DIŐI

hizmet markaları, ticari unvanlar, kaynak işaretleri ve haksız rekabetin sınırlandırılması konularını içerir. (3) Sinaî mülkiyet geniş anlamda anlaşılmalıdır ve yalnızca sinaî ve ticari usullere uygulanmayacak şarap, hububat, tütün, meyve, mineraller ve maden suları, bira, çiçekler ve un gibi tüm işlemiş ve doğal ürünleri kapsayacaktır.(4) Sinaî patentler, ilgili ülkenin kurumunun belirlediği ithal patentleri, geliştirme patentleri, ilave patent ve sertifikalar gibi patent çeşitlerini içerecektir” hükümleri yer almaktaydı (Soyak, 2005, s. 5).

(2) Dünya Fikri Mülkiyet Örgütü (World Intellectual Property Organisation-WIPO)

WIPO, 1967 yılında Stockholm’de imzalanan sözleşme ile kurulmuştur. Temel amacı ise dünya genelinde fikri mülkiyet haklarını korumaktır. Aynı zamanda Birleşmiş Milletler’in bir örgütü olan WIPO’ya bağlı 184 üye devlet bulunmaktadır. Patent, marka ve endüstriyel tasarımlar için de uluslararası tescil sistemi getiren WIPO, aynı anda pek çok ülkede fikri mülkiyet koruması sağlayabilmektedir. Üye devletler için forum niteliğinde olan kuruluş fikri mülkiyet haklarının korunması konusunda ilke ve kuralları belirlemektedir. Getirdiği en önemli kolaylıklardan birisi her ülke için ayrı ayrı dillerde başvuru ve ücret ödeme zorunluluğunu ortadan kaldırmasıdır. Bu sayede başvuru sahibi ilgili ürünü tescili için tek dilde ve bir seferde ücret ödemesi yapabilmektedir (WIPO, 2012, s.16).

Günümüzde 23 anlaşmanın koordinesinden ve yürütülmesinden sorumlu olan örgüt geliştirmekte olan ülkelere de mevzuatlarını düzenlemeleri konusunda hukuki ve teknik yardım yapmakta ve uzman personelin eğitimi konusunda yardımcı olmaktadır (Karahan, Suluk, Saraç ve Nal, 2011, s.25).

Merkezi Cenevre’de bulunan WIPO’ya Türkiye 1975 yılında üye olmuştur.

(3) Gümrük Tarifeleri ve Ticaret Genel Anlaşması (General Agreement on Tariffs and Trade-GATT)

GATT, elli iki ülkenin 1947 yılında imzaladığı anlaşmanın 1948 yılında yürürlüğe girmesi ile kurulmuştur. Çok taraflı bir uluslararası anlaşma olmakla birlikte, yer alan yükümlülüklerin ortak bir tavırla yerine getirilmesi zorunluluğu nedeniyle uygulamada uluslararası bir kuruluş niteliği kazanmıştır. GATT’ın amaçları arasında, dış ticaretteki engelleri ve gümrük vergilerini kaldırarak ticaret serbestisi sağlamak yer almaktadır. Üye ülkelerin tarifelerini değiştirmelerini de esneklik sağlamakla birlikte denetim altına almaktadır (Sönmezoğlu, 2000, s.328-329).

TASNİF DIŞI

Başlangıçta mal ticaretini serbestleştirme ve liberal düzeni korumaya yönelik hükümler içeren Anlaşma daha sonra değişime uğramıştır. 1982 yılında yapılan GATT toplantısında, ABD ve diğer gelişmiş ülkeler tarafından WIPO'nun sınai mülkiyet hakları ile ilgili olarak gerek standart geliştirmede gerekse uyumsuzlukları çözmede yetersiz kaldığı ileri sürülmüştür. Sınai mülkiyet haklarının GATT kapsamında yeniden ele alınmasını isteyen gelişmiş ülkelerin teklifi üzerine konu gündeme alınmıştır. 1986 yılında Uruguay Turunda (Round) tartışılmaya başlanan görüşmelere az gelişmiş ülkeler karşı çıkmışlardır. Sonuç olarak 15 Nisan 1994'te Dünya Ticaret Örgütü'nü kuran anlaşma imzalanmıştır (Topçu, 2007, s.40-41). GATT'ın fiili etkinliği de DTÖ'ye geçmiştir (Sönmezoğlu, 2000, s.329)

(4) Ticaretle Bağlantılı Fikri Mülkiyet Hakları Sözleşmesi (Agreement on Trade Related Aspects of Intellectual Property Rights-TRIPs)

Esas itibariyle Ticaretle Bağlantılı Fikri Mülkiyet Hakları Sözleşmesi (TRIPs), 1995 yılında Uruguay Toplantıları (Round) sonucunda ortaya çıkan Dünya Ticaret Örgütü (DTÖ) Kuruluş Anlaşmasının ekidir. Ancak fikri haklar bakımından uluslararası bir standart getirme amacını taşıyan en kapsamlı düzenleme olarak kabul edilmektedir. Hâlihazırdaki sözleşmeleri ortadan kaldırmamakla birlikte bunlara ek düzenlemeler de içermektedir. Üye devletler DTÖ bünyesinde serbest ticaret sisteminin dışında kalmamak için asgari standartları yerine getirmek zorundadır. Bayamlıoğlu'na göre TRIPs Sözleşmesinin iki önemli amacı bulunmaktadır:

“TRIPs bir yandan asgari standartları belirleyerek fikri mülkiyet haklarının korunmasında etkinliği artırmayı; diğer yandan da fikri mülkiyet haklarının uygulanmasına ilişkin usul ve önlemlerin uluslararası ticaret için engel oluşturmasını önlemeyi amaçlar” (Bayamlıoğlu, 2008, s.133-134).

Sözleşme ile patent konusunda herhangi bir ayrım gözetilmeksizin koruma ilkesi benimsenirken, izinsiz kullanılan patentlerin bedelinin ödenmesi ve üye ülkelerce bu hakların koruma altına alması sağlanmıştır. Daha önce 10 yıl olan patent koruma süresi 20 yıla çıkarılmıştır (Soyak, 2005, s.10).

TRIPs'in doğmasına neden olarak Doğu Asya'daki ülkelerin hızlı kalkınmalarının yarattığı endişe gösterilmektedir. Zira bu ülkeler taklit, uyarlama ve tersine mühendislik yöntemleri ile ARGE faaliyetlerine daha az yatırım yaparak rekabet kabiliyetlerini artırmışlardır. Bu yüzden dünya genelinde sınai mülkiyet haklarının sıkılaştırılarak TRIPs anlaşması yolu ile ülkelere sorumluluklar

getirilmesinin temelinde ABD'nin baskısı olduğu ifade edilmektedir (Soyak, 2005, s.9).

(5) Patent İşbirliği Sözleşmesi (Patent Cooperation Treaty-PCT)

Patent İşbirliği Sözleşmesi, Paris Sözleşmesinin eklerinden biri olup 1970 yılında imzalanmıştır. Sözleşme gereği oluşturulan uluslararası patent sistemi ile buluş sahipleri başvurularının kabulü halinde istedikleri ülkelerde koruma imkânına sahip olmaktadır (Topçu, 2007, s.41).

PCT, bugün dünya çapında 125'i aşkın ülkede uluslararası patent başvuru sistemi sunmaktadır. Yapılan başvuruların organizasyonu WIPO tarafından gerçekleştirilmektedir. Bu sayede çoklu ulusal başvuru veya bölgesel başvurudan ziyade pek çok ülkeyi kapsayan bir koruma sağlanmaktadır. Uluslararası incelemede araştırma ile talep edildiği takdirde ön inceleme yapılmaktadır. PCT ile ülkelerin patent ofislerinin yükü azaltılmaktadır (Alper, 2011, s.159).

Türkiye bu sözleşmeye 1996'dan itibaren taraf olmuştur.

(6) Avrupa Patent Sözleşmesi (European Patent Convention-EPC)

1973 yılında Münih'te imzalanan ve 07 Ekim 1977 tarihinde yürürlüğe giren Avrupa Patent Sözleşmesi (EPC) ile üye ülkelerde patentlerin tescilinin tek bir sistemle bağlanması ve patentler için standart kuralların oluşması amaçlanmıştır. Sözleşme uyarınca Avrupa Patent Kurumu'na yapılan başvuru olumlu sonuçlandığı takdirde buluşa "Avrupa patenti" verilmektedir. Ancak Avrupa patenti ortak bir koruma hakkı sağlamamaktadır. Koruma hakkı sadece, buluş sahibinin başvurusunda belirttiği üye devletlerde geçerlidir. Sözleşmenin 2/2'inci maddesinde *"Avrupa patenti, onun verildiği üye devletlerin her birinde bu Antlaşma içinde aksi ifade edilmedikçe o devlet tarafından verilen bir patent gibi aynı etkiye sahip olacak ve aynı şartlara tabi olacaktır"* hükmü yer almaktadır.

Avrupa Topluluğu üyesi devletlerle birlikte Sözleşmenin hazırlanmasına katılmış olan ve İdari Konsey tarafından davet edilen bütün Avrupa devletleri EPC'ye katılabilmektedir. Türkiye bu sözleşmeye 2000 yılında taraf olmuştur (Erdem, 2003, s.89-90).

Fikri mülkiyetlerin korunması konusunda küresel ölçekli anlaşmalar olduğu gibi bölgesel nitelikli anlaşmalar da bulunmaktadır. Bunlara örnek olarak ABD, Kanada ve Meksika arasında imzalanan Kuzey Amerika Ülkeleri Serbest Ticaret Anlaşması (North American Free Trade Agreement-NAFTA) gösterilebilir (Ünsal, 1993, s.286). 1 Ocak 1994'te yürürlüğe giren anlaşma ticari sır korumasını doğrudan dile getiren ilk uluslararası anlaşmadır. NAFTA'nın 1711'inci maddesine göre ticari

TASNİF DIŞI

sırlar gizli kaldığı ve kamu tarafından bilinmediği müddetçe sözleşmeye taraf ülkelerce korunacaktır (Nasheri, 2005, s.127).

Fikri mülkiyet ve ticari sırların korunması konusunda imzalanan temel anlaşmalar ve oluşturulan kurumlar önemli olmakla birlikte, bu kurumların ve anlaşmaların endüstriyel casusluğu ne kadar önlediği sorusu tartışmalı bir durumdur. Özellikle 21'inci yüzyıla girerken bilişim teknolojilerinde yaşanan hızlı dönüşüm sayesinde her türlü verinin dijital ortamda saklanması, işlenmesi ve iletilmesi, endüstriyel casusluğun hedefini ve konusunu oluşturan fikri mülkiyet ve ticari sırların korunmasını daha karmaşık hâle getirmiştir.

2. BİLİŞİM SİSTEMLERİ, SİBER SALDIRI ve BİLGİ TEKNOLOJİLERİ GÜVENLİĞİ

21. yüzyılda bilgi teknolojilerinde yaşanan gelişmeler, kamu ve özel sektör alanındaki çalışma sistemlerine büyük oranda etki ederek bunların değişimlerine neden olmaktadır. Savunma, haberleşme, enerji, ulaşım, bankacılık, sanayi tesisleri, sağlık hizmetleri vb. pek çok hizmetin alt yapısını, bilgi ve iletişim sistemleri oluşturmaktadır. Bunun sonucu olarak da maliyetler düşmüş ve üretim daha verimli hale gelmiştir. Yakın gelecekte dünya genelindeki bütün altyapı sistemlerinin bilgi teknolojilerine bağımlı hale geleceği değerlendirilmektedir (Yılmaz ve Salcan, 2008, s.11). Her türlü verinin elektronik ortamda işlenmesi, depolanması ve iletilmesi kolaylaşmış ancak hassas bilgileri ve ticari sırları saklamak da bir o kadar zorlaşmıştır. Basılı haliyle saklanması mümkün olmayan binlerce sayfalık gizli bilgi barındıran veriler, saniyeler içinde kaydedilerek tek tuşla dünyanın herhangi bir yerine gönderilebilmektedir. Coğrafi sınır tanımayan siber uzay kendisine özgü bir suç dünyası yaratırken, bilgisayar korsanları da sanayi casusluğunun yeni aktörleri olarak karşımıza çıkmaktadırlar. Dolayısıyla küresel ekonomi ile siber uzayın birleşmesi, bambaşka bir mücadele alanının doğmasına yol açmıştır. Bu doğrultuda bilişim sistemlerindeki gelişmeleri takip etmek, siber uzayda meydana gelen tehdit ve riskleri öngörmek ve bilgi teknolojilerinin güvenliğini sağlamak her seviyedeki kurum ve kuruluşun başat görevi haline gelmiştir.

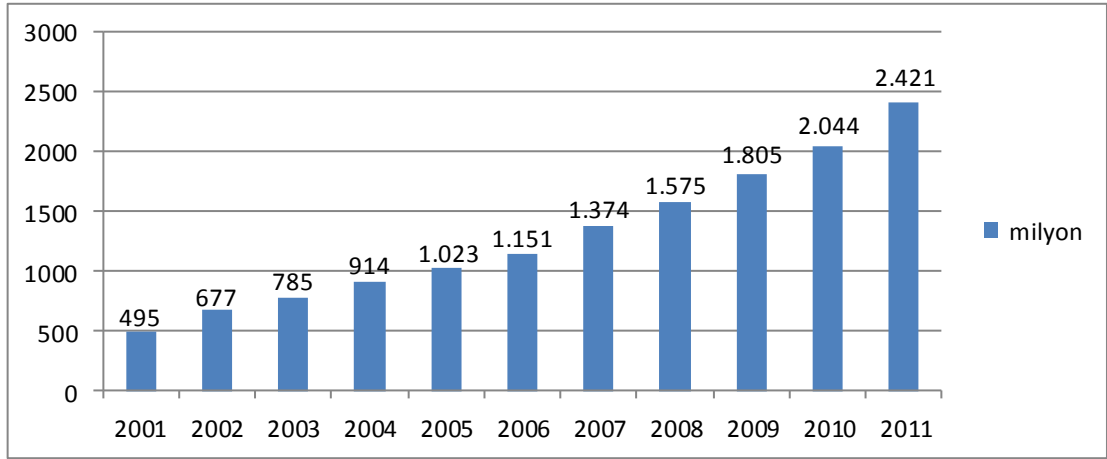
a. Bilişim ve Bilişim Sistemleri

Türk Dil Kurumu sözlüğüne göre bilişim *“insanoğlunun teknik, ekonomik ve toplumsal alanlardaki iletişiminde kullandığı ve bilimin dayanağı olan bilginin, özellikle elektronik makineler aracılığıyla düzenli ve akla uygun bir biçimde işlenmesi bilimi”* olarak tanımlanırken; bilişimde kullanılan tüm araç ve gereçlerin oluşturduğu sisteme de “bilişim teknolojisi” denilmektedir. Kısaca her türlü veriyi sayısallaştıran,

TASNİF DIŐI

iőleyen, depolayan ve ileten cihazlar biliőim teknolojileri adı altında deęerlendirilmektedir. Enerji, saęlık, ulaőım, savunma, finans, üretim vb. kritik altyapıların iőletilmeleri bilgi teknolojileri kullanılarak yapılmaktadır. őirketler ve kurumlar da; muhasebe, satış, üretim süreçleri, ARGE faaliyetleri, istatistiksel veriler vb. pek çok alanda bilgisayarları kullanmaktadır (Owens, Dam ve Lin, 2009, s.9).

Günlük hayatın vazgeçilmez bir parçası haline gelen bilgisayarlar 1940'lı yılların sonlarına doğru ortaya çıkmıőtır. Ancak bunların o dönemdeki kullanım őekilleri günümüzden oldukça farklıydı. Bilgisayarların yaygın kullanımı ise 1980'li yıllarda kişisel bilgisayarların üretilmesiyle başlamıőtır. Bununla birlikte őirketler bilgisayar teknolojisi ile otomasyona geçerken kritik ticari bilgilerin başka bir ortama kopyalanma tehlikesi de belirlemiőtir (Dlamini ve Eloff, 2009, s.191).



Tablo-6: Dünya Geneline İnternet Kullanıcı Sayısı

(Kaynak: International Telecommunication Union, <http://www.itu.int/ITU-D/ict/statistics/> adresinden alındı.)

Bilgisayarların doğuşu internetin gelişimini de tetiklemiőtir. İnternet'in temeli Amerikan Savunma Bakanlığı İleri Araőtırma Projeleri Ajansı (Advanced Research Project Agency-ARPA) tarafından yürütölen ARPANET projesiyle atılmıőtır. Projenin öncelikli amacı askeri maksatlı olarak herhangi bir saldırı durumunda dahi bilgi akışını devam ettirebilecek bir aę sistemi yaratmaktı. Ancak 1971 yılında yaklaşık 24 kadar araőtırma ve kamu sitesinin de bağlanmasıyla araőtırmacıların da kullanımına sunulmuőtur. 1989 yılında İNTERNET adını alan ARPANET artık araőtırma projesi konumundan iőletme durumuna gelmiőti (Yılmaz ve Salcan, 2008, s.35-37). 1990'larda aę sistemlerinin bağlanmasıyla geniş kitlelere ulaőım imkânı bulan internetin kullanımı 2000'li yılların ardından muazzam bir artış göstermiőtir (Tablo-6). Dünya genelinde internet kullanıcı sayısı 2001 yılında 495 milyon iken, on yıllık süre

TASNİF DIŐI

zarfında bu sayı 2,5 milyara yaklaşmıştır. Son on yılda meydana gelen bu hızlı artış bilgi güvenliği konusundaki endişeleri de beraberinde getirmiştir.

21. yüzyıla girerken bilişim teknolojilerinin neredeyse bütün endüstri dallarının altyapısını oluşturduğu ve elektronik ortama dâhil olan alanlara yeni anlamlar yüklediği görülmektedir. Elektronik ortamda mesaj gönderme için kullanılan e-postanın ardından, e-reklam, e-ticaret, e-devlet, e-oylama vb. pek çok kavram yeni teknoloji ile birlikte gittikçe gelişerek gündelik yaşamımızın birer parçası haline gelmiştir. Bunun yanında internet bağlantılı cep telefonları, diz üstü, kişisel ve tablet bilgisayarlar gibi üretilen her yeni sistem de bilgisayar tanımının sınırlarını zorlamaktadır (Dlamini ve Eloff, 2009, s.191).

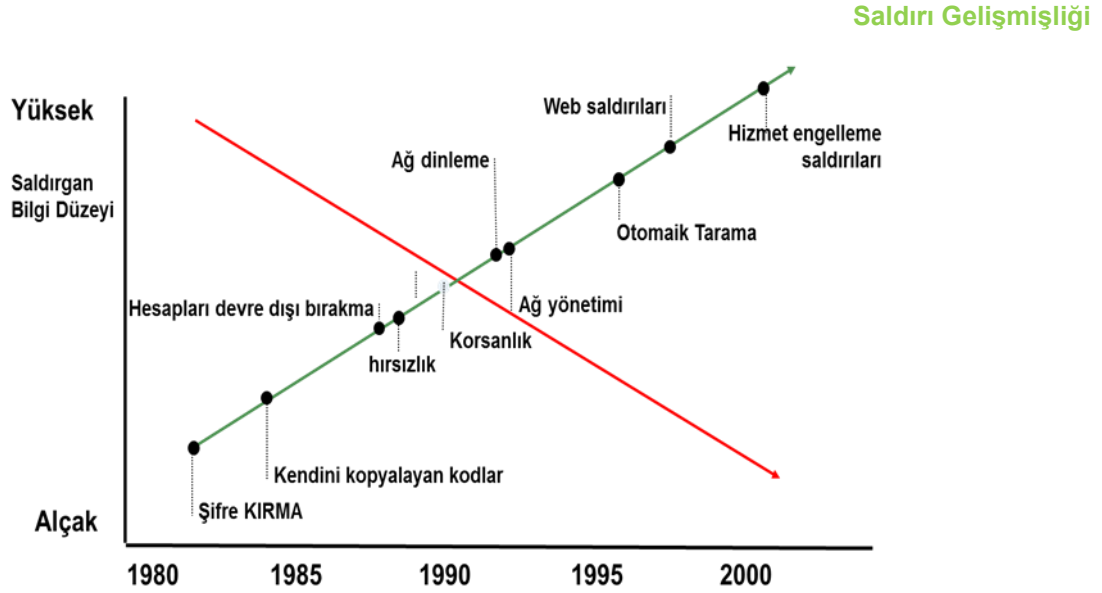
b. Siber Uzay ve Siber Saldırı

Günümüzde internet de dâhil olmak üzere tüm bilgi ve iletişim ağlarının oluşturduğu alan “siber uzay” olarak ifade edilmektedir (Whittaker, 2004, s.5). Siber uzayın fiziksel dünya ile bütünleşerek devletlerin güvenlik, ulaşım, enerji, finans vb. altyapılarına bağlanması, getirdiği faydaların yanında daha önce karşılaşılmayan risk ve tehditlerin doğmasına da neden olmuştur. Siber uzaydaki her türlü veri, program ve ağ sisteminin değiştirilmesi, bozulması, sahtesinin üretilmesi, kesintiye uğratılması ya da yok edilmesi siber saldırı olarak adlandırılmaktadır. Klasik saldırı şekilleri ile karşılaştırıldığında siber saldırı oldukça değişik bir karakter sergilemektedir. Öncelikli olarak saldırıda bulunanlar sadece kendi bilgisayarları ile değil ele geçirdikleri diğer bilgisayarları da kullanabilmeleri nedeniyle kimliklerini büyük bir oranda gizleyebilmektedirler. Bu da saldırıya uğrayanlarda, görünmeyen ya da bilinmeyen bir düşmanla savaş duygusunu yaratmaktadır. Diğer bir özellik ise saldırının yarattığı hasarın tespitinin son derece güç olmasıdır. Saldırının ne zaman başladığı, hangi sistem ve bilgilerin zarar gördüğü, bu bilgilerle saldırganların hangi kazançları sağladığı, elde ettikleri bilginin saldırganlar tarafından gelecekte de kullanılabilme ihtimalleri vb. hususlar hesaplamayı oldukça zorlaştırmaktadır. Siber saldırının diğer bir özelliği de saldırganlara zaman ve mekân açısından sunduğu fırsatlardır. Saniyenin onda biri kadar bir zaman diliminden yıllara uzanan bir saldırı dizisi, hedef sisteme çok yakın bir yerden gerçekleştirilebildiği gibi sınır ötesinde, dünyanın herhangi bir noktasından da yapılabilir (Owens, Dam ve Lin, 2009, s.1-2).

Siber uzayda saldırıda bulunanlar oldukça geniş bir yelpazede yer almaktadırlar. Devletler; düşman devletleri zayıflatmak, istihbarat toplamak ve sabotaj yapmak maksadıyla, politik örgütler ise; propaganda yapmak, ekonomik ve

TASNİF DIŐI

psikolojik çöküntü yaratarak sosyal yapının bozulması için siber saldırıyı kullanmaktadırlar. Şirketler ya da kurumlar özellikle ticarete haksız rekabet sağlamak ve endüstriyel casusluk amacıyla kullanılırken, suç örgütlerinin temel hedefinin para ve güç olduğu değerlendirilmektedir. Son grupta ise kendilerini ispatlama peşinde olan kriminaller yer almaktadır.



Şekil-1: Saldırı Gelişmişliği-Saldırgan Bilgi Düzeyi

Saldırgan Bilgi Düzeyi

(Kaynak: TUBİTAK-UEKAE Ağ Güvenliği Grubu, <ftp://ftp.dtm.gov.tr/Etik/sunular/uekae.pdf> adresinden alınarak düzenlendi.)

Siber saldırıda bulunanlar bilgisayar korsanı (hacker) veya bilişim korsanı olarak adlandırılmaktadırlar. Bilgisayar korsanlarının bilgi düzeyleri ile yaptıkları eylemin boyutları zaman içerisinde değişim göstermektedir (Şekil 1). Şifre kırma, kendini kopyalayan kodlar, hırsızlık gibi saldırılar, günümüzde yerini daha karmaşık olan ağ dinleme ve yönetimi, otomatik tarama ve hizmet engelleme gibi saldırılara bırakmıştır. Burada dikkati çeken durum saldırılarda kullanılan metotların gittikçe karmaşıklaşmasına rağmen saldırganların bilgi düzeylerinin ters orantılı olarak azalmasıdır. Sonuç olarak saldırı ve saldırgan sayısı ile meydana gelen zararlar artarken, saldırıyı önlemek için alınması gereken tedbirler giderek güçleşmektedir (Canbek ve Sağıroğlu, 2006, s.73).

Verinin taşıdığı özelliklere göre siber saldırılar üç ana noktayı hedef almaktadırlar. Bunlar:

Veri Gizliliği: Verinin sadece yetkilendirilmiş kişilere açık olduğunu ifade eder.

TASNİF DIŞI

Veri Bütünlüğü: Verinin özgün halinin bozulmaması ve değişiklik yapılmadığını gösterir.

Verinin Kullanılabilirliği: Normal durumdan olağanüstü duruma kadar verinin işlevini yerine getirme halini işaret eder (Choo, 2010, s.105).

Siber uzayda yapılan saldırılar, saldırıyı gerçekleştirenlerin kimliklerine ve maksatlarına göre çeşitli adlar almaktadır. Uluslararası ortamda devletlerin aralarındaki mücadeleyi siber ortama taşımaları siber savaş olarak adlandırılırken, çıkar amaçlı olmayan ancak kritik altyapı ve tesislere yönelik terör örgütlerince ya da kimliği bilinmeyen kişilerce yapılan eylemler ise siber terör olarak ifade edilmektedir. Ülkeler kendi özel ve tüzel kişilerinin haklarına yönelik saldırıları “siber suç” ya da “bilişim suçu” sayarak bunları çıkardıkları kanunlarla koruma altına almışlardır. Yapılan kötü maksatlı müdahaleleri “siber saldırı (cyber attack)” ve “siber sömürü (cyberexploitation)⁶” olmak üzere iki gruba ayıranlar da vardır. Siber saldırıda bulunanların adı değişmekle birlikte genellikle benzer saldırı yöntemlerini kullanmaktadırlar.

c. Siber Saldırıda Kullanılan Yöntemler

Saldırıdan önce, siber saldırıda bulunmak isteyen kimseler (bilgisayar korsanları, istihbarat örgütleri, rakipler vs.) öncelikli olarak hedefle ilgili bilgi toplamak zorundadırlar. Toplanan bu bilgiler hedef bilgisayara ait Whois⁷ veri tabanı bilgileri, İnternet Protokol⁸ (İnternet Protocol-IP) adresi, Alan Adı Sistem⁹ (Domain Name System-DNS) sunucusu vb. gibi bilgilerden oluşmaktadır. Günümüzde Netscan Tools ve Trout gibi programlarla bu bilgiler elde edildiği gibi internette bulunan çeşitli siteler vasıtasıyla bu bilgilere ait sorgulamalar da yapılabilmektedir (Elbahadır, 2011, s.41-45).

Bilgisayar korsanları için önemli olan diğer bir bilgi de hedef bilgisayarın hangi işletim sistemini (Microsoft Windows, Linux, Android vb.) kullandığının tespit edilmesidir. Elbahadır (2011, s.73)’a göre, işletim sisteminin tespit edilmesi bilgisayar korsanın işini oldukça kolaylaştırmaktadır. İşletim sistemlerinin kendilerine özgü sistem hatalarının ve açıklıklarının bulunduğu ve bu kusurları gidermek için

⁶ Siber sömürü: Özellikle istihbarat amacıyla kullanılan, hedef bilgisayardaki verilere zarar vermekten ziyade bu bilgileri uzun süreli ele geçirmeyi amaçlayan saldırı çeşidi.

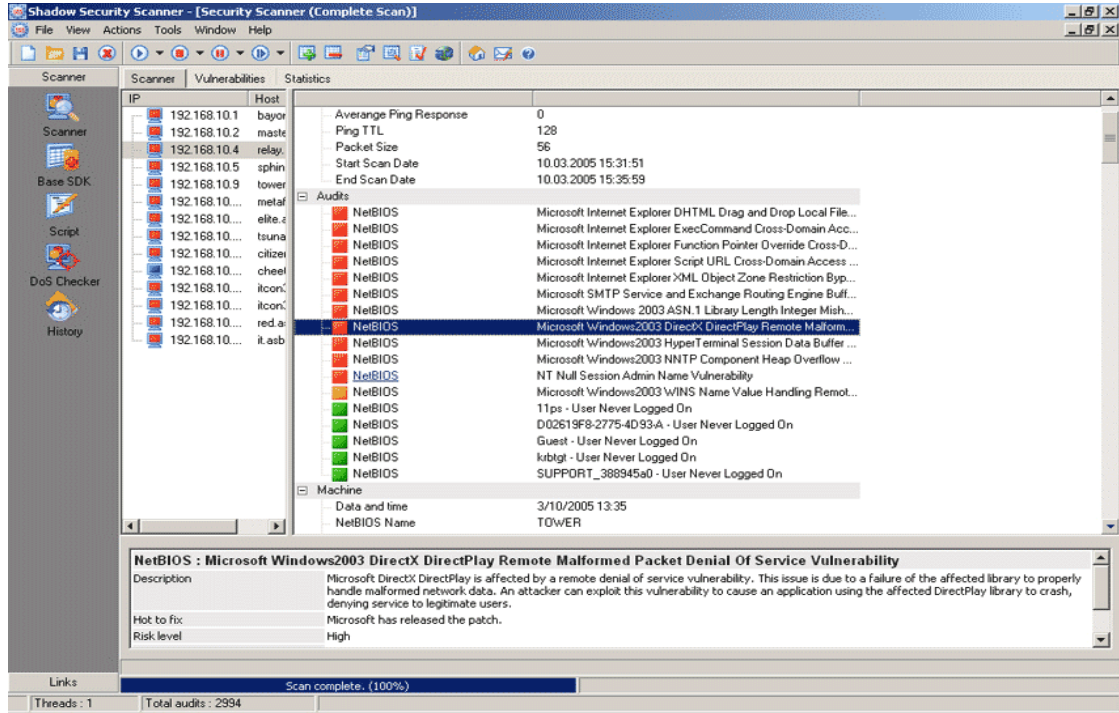
⁷ DNS adresleri, IP adresi, kullanıcının e-posta adresi, telefon numarası gibi bilgiler Whois veri tabanında bulunmaktadır.

⁸ Bilgisayarların birbirini tanıyarak iletişim kurmalarını ve veri aktarımını sağlayan, onluk sayı tabanına göre 0-255 arasında yazılan 32 bitlik rakamsal verilerdir.

⁹ Bilgisayarları ve hizmetleri daha kolay isimlerle adlandırmak için kullanılır. Örneğin Harp Akademileri Komutanlığı için DNS “harpak.edu.tr”dir.

TASNİF DIŞI

zaman zaman internet üzerinden yama ve düzeltmelerle güncelleme yapıldığı bilinen bir durumdur. Hedef bilgisayarın hangi işletim sisteminin kullanıldığının tespit edilmesi sayesinde bilgisayar korsanı sistemdeki açıklığı tespit etmek için genel bir tarama yapmaktan ziyade doğrudan o işletim sisteminin açıklıklarına yönelik denemelerde bulunacaktır. Açıklıklar, yazılım veya donanımda programlama hatasından kaynaklanan, istismar edilmeye müsait zayıflıklardır. Kötü niyetli kişilerce sistem içerisinde bulunan bilgileri silmek, çalmak, değiştirmek veya diğer sistemlere saldırı düzenlemek amacıyla kullanılmaktadır (TÜBİTAK UEKAE, 2011).



Resim-1: Örnek Shadow Security Scanner Tarama Sonucu

(Kaynak: SAFETY-LAB Bilgi Portalı, <http://www.safety-lab.com/images/SSS1.gif> adresinden 31.12.2011 tarihinde alındı)

Bilgisayar korsanları güvenlik açıklıklarını genellikle tarayıcı program kullanarak bulmaktadırlar. Bu programlar belleklerinde bulunan açık listelerini teker teker bağlandıkları sistemde denemektedirler. Örneğin, günümüzde Shadow Security Scanner (RESİM-1), GFI LANGuard Network Security Scanner ve Acutenetix Web gibi programlar sistemde bulunan açıklıkları tespit etmek için kullanılmaktadırlar. Bu programlar sayesinde güvenlik açıklıkları, olası hizmet dışı bırakma (DoS) saldırıları, açık bağlantı noktaları, zayıf şifreler vb. pek çok konuda bilgi alınabilmektedir (Elbahadır, 2011, s.75-78).

TASNİF DIŞI

Sistemde ve ağlarda açıklığı meydana getiren pek çok sebep vardır. Bunların büyük çoğunluğu hatalı kodlamalardan (uygulama hatalarından) kaynaklanmaktadır. Bu açıklıklar tespit edildiklerinde güncelleme yolu ile tüketicilere ulaştırılmaktadır. Ancak yapılan düzeltmeler sanıldığı kadar hızlı bir şekilde yapılmamaktadır. Çünkü sistem işleticileri, istenmeyen sonuçlarla karşılaşmamak için düzeltmeleri öncelikle kendi sistemleri üzerinde test etmek istemekte bu durum da zaman kaybına yol açmaktadır. Ayrıca sayıları binleri hatta milyonları bulan bilgisayarlar üzerinde yazılımların güncelleştirilmesi de büyük iş yoğunluğu ve zaman gerektirmektedir. Yazılım şirketlerinin rekabette öne geçmek amacıyla mükemmeliyetten çok hıza önem vermeleri sonucu dikkatsiz ve aceleci davranmaları da açıklıklara neden olmaktadır (Yılmaz ve Salcan, 2008, s. 64).

Siber saldırıda uygulanan yöntemlerin dört ana grupta toplandığını söylemek mümkündür. Bunlar:

- Zararlı Yazılımlar
- Servis Saldırıları
- Kimlik Saldırıları
- Gizli Dinleme

(1) Zararlı Yazılımlar

Kötü amaçlı yazılım olarak da bilinen zararlı yazılımlar arasında; virüsler, solucanlar (worms), Truva atları (trojan horses), arka kapı (backdoor) klavye kaydediciler (key logger), casus yazılımlar (spyware), reklam yazılımları (adware) yer almaktadır.

(a) Bilgisayar Virüsleri

Virüsler kullanıcının isteği dışında bilgisayara yüklenerek çalışan oldukça etkili bir programdır. Diğer bilgisayarlara bulaşma ve kendi kendine çoğalma özelliğinin biyolojik virüslere benzemeleri nedeniyle virüs olarak adlandırılmaktadırlar. Virüsler, internet sitelerinden indirilen dosyalardan, e-postalardan veya bir depolama aygıtından (CD, DVD, harici bellek vs.) bulaşabilirler. Veri kayıplarına ve hasarlara neden olabilirler (Yılmaz ve Salcan, 2008, s.56). Virüslerle diğer zararlı yazılımlar arasındaki en önemli fark, virüslerin başlatıcı unsur olarak insan etkileşimine ihtiyaç duymasıdır. Aktif hale gelebilmesi için virüslü program, dosya veya e-postanın kullanıcı tarafından çalıştırılması, okunması ya da indirilmesi gerekmektedir. Virüsler sistem bileşenlerine göre; dosya virüsleri, önyükleme (boot) virüsleri, makro virüsler ve betik (script) virüsler olarak sınıflandırılabilirler (Canbek ve Sağıroğlu, 2006,

TASNİF DIŞI

s.176-177). Symantec'in Kasım 2011 raporuna göre gönderilen her 256 e-postanın birinde virüs bulunmaktadır (Symantec, 2011, s.18).

(b) Solucanlar (Worms):

Zararlı programlardan bir diğeri de solucanlardır. Esasında virüs olmakla birlikte temel hedefleri bakımından virüslerden ayrılırlar. Virüsler, bağlantı kurulan bilgisayarın dosyalarına süratle yayılırken, solucanlar ise ağ üzerindeki diğer bilgisayarlara hızla yayılma amacını güder. Yayılmak için dosyalara bulaşma ihtiyacı yoktur. Yine virüslerden farklı olarak, aktif hale gelmesi için insan etkileşimine ihtiyaç duymaz, kendi kendini kopyalayarak diğer bilgisayarlara yayılır. Genellikle açıklıkları olan, güncelleme yapılmamış ve güvenlik duvarı bulunmayan bilgisayarlara internet üzerinden e-posta yoluyla bulaşan solucanlar, kullanıcı tarafından açılmaları halinde bilgisayarın kontrolünü ele geçirirler ve hızla çoğalarak kurbanın rehberinde bulunan adreslere kopyalarını gönderirler. Solucanları gerçekte zararlı yapan husus taşıdığı veri yüküdür (payload). Hızla yayılan solucanlara yıkıcı etkisi olan bir verinin yüklenmesi halinde vereceği zarar oldukça büyük olabilir. Veri yükü olmasa bile hızla çoğalmaları ve yayılmaları nedeniyle internet trafiğini felç edebilirler (Ghosh ve Turrini, 2010, s.52-54). 2003 yılında dünya genelinde tüm bilgisayar sistemlerinde ciddi sorunlara neden olan "Slammer" solucanı, ABD'de bulunan bir nükleer santralin güvenlik görüntüleme sistemine beş saat süreyle sızmıştır (OECD, 2008, s.43).

(c) Truva Atı (Trojan Horse)

Tarihteki bilinen özelliği ile benzer şekilde "Truva Atı", zararsız ve iyi niyetli gözükken ancak zararlı yazılım içeren programlardır. Bulaştığı bilgisayarda etkin hale gelebilmesi için kullanıcı tarafından çalıştırılması gerekmektedir. Bu yüzden Truva atı içeren oyun, resim, program vb. formdaki dosyaları indirerek açmalarını sağlamak için kullanıcılara çeşitli tuzaklar kurulmaktadır (Gozzi, 2000). Truva atları "istemci" ve "sunucu" olmak üzere iki kısımdan oluşur. Sunucu kısmı hedeflenen bilgisayarda işlem yaparken istemci kısmı da uzaktan erişim sağlayan kişinin bilgisayarında çalışır (Avşar ve Öngören, 2010, s.50). Siber saldırıda bulunanlar için en önemli husus sunucu kısmını hedef bilgisayara bulaştırarak çalışmasını sağlamaktır. Truva atları hedef bilgisayara aşağıda sıralanan zararları verebilirler;

- Şifre ve hesap bilgilerini çalma,
- Başka saldırılara kapı açma,
- Dosyaları silme, değiştirme ve yönetme,
- Sistem dosyalarına zarar verme ve sistemi yeniden başlatma,

TASNİF DIŞI

- Monitör, CD-ROM vb. donanımlar üzerinde değişiklik yapma (görüntüyü çevirme, CD-ROM açma vs.),
- Başka sistemlere yapılacak saldırılar için hedef bilgisayarın kontrolünün ele geçirme (Elbahadır, 2011, s.230-231). Örnek vermek gerekirse bilgisayar korsanları trojanları kullanarak Rusya'da Gazprom tarafından işletilen bir boru hattının kontrolünü ele geçirmişlerdir (OECD,2008,s.43).

(ç) Arka Kapılar (Backdoors)

Arka kapılar, bilgisayar korsanlarının hedef bilgisayar ya da ağ sistemlerine uzaktan yetkisiz erişim yapmalarını sağlayan zararlı yazılımlardır. Arka kapıların en önemli özelliği, sisteme ilk kez sızılırken eklenen program sayesinde aynı ortama kolaylıkla giriş imkânı sağlamasıdır. Bu tarz yazılımlarda en sık kullanılan yöntem, hedef sistemde dinleme ajanı yerleştirilmiş bir kapıyı (port) açık tutmaktır (Canbek ve Sağıroğlu, 2006, s.184). Elbahadır (2011, s.228)'a göre arka kapı bırakılan bir sistem amaca göre her türlü saldırı için kullanılabilir durumdadır. Bu yolla yapılabilecek saldırılarda saldırganlar, belirli aralıklarla hedef bilgisayardaki bilgileri sömürebilir, istenilen herhangi bir dosyayı çalıştırılabilir ya da başka zararlı yazılımları uzaktan yükleyebilir.

(d) Bot Ağı (Botnet)

Robot kelimesinden türetilen "bot"lar, bağımsız olarak çalışabilen ve işlemlerini otomatik olarak gerçekleştirebilen programlardır. Bot programı tarafından ele geçirilen bilgisayarlar "zombi" olarak da adlandırılmaktadır. "Zombi" bilgisayarların oluşturdukları zincire de "bot ağı (botnet)" denilmektedir. Botnet saldırılarının en önemli özelliği, arka planda kalan tek bir saldırgan tarafından yüzleri, binleri hatta milyonları bulan bilgisayarların, kullanıcılarının haberi dahi olmadan istenilen eylem doğrultusunda yönlendirilebilmesidir (Owens, Dam ve Lin, 2009, s.92-94). Saldırganlar ele geçirdikleri bilgisayarları kullanarak büyük miktarlardaki e-postayı hedef sitelere göndermekte ve sistemin aşırı yüklenmesine neden olmaktadır. Örneğin 2007-2009 yılları arasında faaliyet gösteren "Reactor Mailer" botneti en aktif olduğu zamanda günlük 180 milyardan fazla spam göndermiştir. Bu rakam o dönem için dünya genelinde gönderilen spamların %60'ını oluşturmaktaydı. "Reactor Mailer" saldırıları, yaklaşık 220.000 ele geçirilmiş "zombi" bilgisayar aracılığıyla yapılmıştı. Kimlik bilgilerini çalmak için klavye kaydedici yazılımı barındıran "Zeus" botnetinde 3,6 milyon bilgisayarın kullanıldığı

TASNİF DIŐI

belirtilmektedir. Botnetler, DoS saldırıları için de kullanılmaktadır (Moore, 2010, s.105).

(e) Klavye Kaydediciler (Keyloggers)

Klavye kaydediciler, klavyede basılan tuşları kaydeden ve gösteren programlardır. Genellikle kullanıcı veya sisteme ait şifreleri ele geçirmek için kullanılırlar (Sommer ve Brown, 2011, s.25). Klavye kaydediciler kendi içinde yazılım ve donanım tipi olmak üzere iki gruba ayrılır. Donanım klavye kaydedicilerde işlem ayrı bir cihazla sağlanır ve klavyeye takılır. Kullanıcı tarafından dışarıdan fark edilmesi mümkün olan bu cihazların sistemin içine takılabilenleri de vardır. (Damodaram ve Valarmathi, 2010, s.620). Yazılım klavye kaydediciler ise işletim sistemine gelen tuş basım bilgilerini depolar (Canbek ve Sağıroğlu, 2006, s.241). 2004 yılında Japon Sumitomo Mitsui Bankası'nın Londra şubesinden 423 milyon dolar çalmayı planlayan saldırganlar klavye kaydedicileri kullanmışlardır. Paranın ayrı bir hesaba aktarılması planlanan saldırıda ilk para nakli teşebbüsü (26,8 milyon dolar) Yeron Bolondi isimli bir İsrail vatandaşının aynı ülkedeki hesabına yapılmıştı (Bank Systems Technology, 2005).

(f) Reklam Yazılımları (Adware)

Bu tür yazılımlar kendi içerisinde yasal ve zararlı olmak üzere iki gruba ayrılmaktadır. Yasal bir reklam yazılımı kullanıcı tarafından aktif hale getirildiği anda ilanı veren kurum ya da kişinin bilgisayarını ile etkileşime girer. Reklam, bilgisayar ekranında anında açılan pencere (pop up) formunda açılabilceği gibi, reklam bandı şeklinde de olabilir. Arama motorlarında, tanıtımı yapılan ürünle ilgili taramaları kaydeder. Kötü amaçlı olanları ise casus yazılımlar gibi hareket eder. Kullanıcının bilgisi ve rızası olmaksızın aktif hale getirildiği sistemle ilgili bilgileri saldırgana gönderebilir. Kötücül reklam yazılımlarının en önemli özelliği sistem içindeki varlıklarının tespiti ve kaldırılmasının son derece güç olmasıdır (Ghosh ve Turrini, 2010, s.57).

(g) Casus Yazılımlar (Spyware)

Casus yazılımlar, kullanıcının bilgisi ve izni olmaksızın, kullanıcı bilgisayara ait her türlü veriyi saldırgana gönderen zararlı yazılımlardır (OECD, 2008, s. 91). Casus yazılımların topladığı verilerin oldukça geniş bir alana yayıldığını söylemek mümkündür. Kullanıcının yaptığı internet gezintisindeki alışkanlıklarından, klavyede bastığı her bir tuşa ya da e-postalarından kimlik bilgilerine kadar pek çok veri bu tarz saldırının hedefini oluşturmaktadır. Esasında casus yazılım bir çerçeve terim olup içerisinde reklam yazılımları, Truva atları, klavye kaydediciler ve bilgi toplama amaçlı

TASNİF DIŞI

diğer kötücül yazılımları da ihtiva etmektedir (Garrie, Griver ve Joller, 2010, s.4). Casus yazılımların dağılmasında kullanılan yöntemler arasında:

- İşletim sisteminde “arka kapı (backdoors)” gibi programların bulunması,
- Genellikle ücretsiz dağıtılan ekran koruyucular, oyunlar ve dosya paylaşım programlarının içinde gizlenmesi,
- Kök kullanıcı takımları (rootkit) yardımıyla kendi işlem ve dosyalarını saklayarak sistemde çalışması,
- E-postaya ekli dosyanın açılması ya da e-postada önerilen bir web adresine girilmesi,
- Bilgisayarda giderilmemiş açıklıklardan yararlanma, sayılabilir (Canbek ve Sağıroğlu, 2008, s.167).

(ğ) Gelişmiş Sürekli Saldırı (Advanced Persistent Threat-APT)

“APT”ler, belirli kişi veya organizasyonu hedef almak için özellikle tasarlanmış saldırılardır. Sistem güvenliği unsurlarınca uzun süre tespit edilememeleri için yavaş ve düşük profilli hareket etmeye programlanmışlardır. Tipik para dolandırıcılığı saldırılarından farklı olarak, casusluk veya sabotaj maksadı ile kullanılmaktadırlar. APT saldırının hedefleri arasında; askeri, politik, ekonomik maksatlı istihbarat toplama, gizli veya ticari sırları ele geçirme, bir operasyonu sekteye uğratma hatta bir materyalin imha edilmesi yer alabilir (Symantec, 2011, s.3). En tehlikeli yazılımlar arasında gösterilen APT saldırıları adını, 2010 yılında İran’ın nükleer çalışmalarını kesintiye uğratan “Stuxnet” solucanı ile duyurmuştur. Diğer solucanlardan farklı olarak “Stuxnet” endüstriyel kontrol sistemlerini etkilemek için tasarlanmıştır. Sadece “Windows” işletim sistemi bulunan bilgisayarlarda çalışan yazılım, endüstriyel kontrol sistemlerinin genellikle internet ağına bağlı olmaması nedeniyle USB¹⁰ üzerinden bulaşmaktadır. Ancak ağ üzerinden yapılan paylaşımlarla da bulaşabilir. Stuxnet, bulaştığı sistemlerde Siemens tarafından üretilen Programlanabilir Mantıksal Denetleyiciler (Programmable Logic Controller-PLC)’i hedef almaktadır. PLC’ler pek çok makine ve otomasyon sürecini bir arada kontrol edebilen işlemcilerdir ve endüstriyel tesislerin gözetim ve kontrolünü sağlayan Denetleme Kontrol ve Veri Toplama (Supervisory Control and Data Acquisition-SCADA) sistemleri ile birlikte çalışırlar. SCADA sistemlerini kontrol eden PLC’lere bulaşan “Stuxnet”, yeniden programlama yaparak sistemi istenmeyen şekilde çalıştırabilmektedir (Falliere, Murchu ve Chien, 2011, s.1-3). Çeşitli kaynaklarda yer alan haberlere göre 2010

¹⁰“ Evrensel Seri Veri Yolu” anlamına gelen “Universal Serial Bus”ın kısaltması.

TASNİF DIŞI

yılında İran'ın uranyum zenginleştirmesi için kullandığı Natanz nükleer tesisindeki 9000 IR-1 santrifüjünden 1000 kadarının Stuxnet saldırısı nedeniyle hasar gördüğü iddia edilmektedir (ISIS, 2011). İranlı yetkililer ise meydana gelen hasarın boyutlarını açıklamamakla birlikte virüsün yaklaşık 30.000 bilgisayarı etkilediğini belirtmişlerdir (NTVMSNBC, 2010). 2011'in kasım ayında Symantec tarafından hazırlanan rapora göre, aynı ay içerisinde gönderilen her iki milyon mesajın birinde APT olabilecek hedeflenmiş saldırılar bulunmaktadır (Symantec, 2011, s.5). Günlük e-posta trafiğinin 48 milyarı bulunduğu düşünüldüğünde kritik sektörler için bir uyarı niteliği taşıdığı söylenebilir.

(2) Servis Saldırıları

Servis saldırıları, daha çok hizmet aksatma amacıyla yapılmaktadırlar. Sürekli yapılan saldırılar sonucunda sistem çalışamaz ve hizmet veremez hale gelir. Bu saldırı önemli sunucuların servis vermeyi durdurması gibi büyük sorunlara yol açabilir. En çok bilinen servis saldırıları; hizmet dışı bırakma (DoS), dağıtık hizmet dışı bırakma (DDoS) ve istenmeyen e-postalardır.

(a) Hizmet Dışı Bırakma (Denial of Service-DoS)

DoS saldırılarında temel hedef web uygulamalarından ziyade sunuculardır. Amaç sunucu ve sunucuya bağlı tüm sitelerin kısmen ya da tamamen devre dışı bırakılmasıdır. Bu tarz saldırılar büyük miktarlardaki veri paketlerinin sunucuya gönderilmesiyle gerçekleşmektedir. Sunucu, kendisine iletilen veri paketlerine yoğunluktan dolayı cevap veremez hale getirildiğinde, işlemci, hafıza ve bant genişliği gibi sistem kaynakları tükenir ve işlevini yerine getiremez. Kendi içinde Smurf saldırıları, Ping Flood, Ping of Death ve SYN Flood¹¹ gibi yöntemleri de barındıran DoS saldırılarının ardından, sunucu üzerinde çalışan servisler bloke edildiği gibi, e-posta ve web hizmetleri de engellenebilir (Elbahadır, 2011, s.117-122). Önemli bir sunucunun devre dışı bırakılması yolu ile dolaylı olarak da ağın işlemez hale gelmesine yol açabilen DoS saldırılarının tespit edilmeleri, tüm ağın analizini gerektirmeleri nedeniyle oldukça zordur (Canbek ve Sağıroğlu, 2007, s.8).

(b) Dağıtık Hizmet Dışı Bırakma (Distributed Denial of Service-DDoS)

DDoS saldırıları da DoS saldırıları ile aynı yöntemle gerçekleştirilmektedir. Aradaki fark DoS saldırısı tek bilgisayar üzerinden yapılırken, DDoS saldırısında birden çok bilgisayar kullanılmaktadır. Yüzlerce hatta binlerce bilgisayar hedef

¹¹ Ayrıntılı bilgi için bkz. Hamza Elbahadır (2011). *Hacking Interface*. İstanbul:KODLAB Yayın.

TASNİF DIŞI

sistemlere eşgüdümlü saldırılarda bulunarak sistemi işlemez hale getirebilir. Bilinen ilk büyük ölçekli saldırı Şubat 2000'de gerçekleştirilmiştir. Zarar gören siteler arasında CNN, eBay, Buy.com ve Datek e-ticaret siteleri olduğu gibi FBI ve Amerikan Savunma Bakanlığı da saldırıya maruz kalmış, bu sitelere erişim belirli bir süre sağlanamamıştır. Birkaç saat süren saldırıda, hedef kurumların teknik personeli saldırının kaynağını dahi tespit edememiştir (Ghosh ve Turrini, 2010, s.40).

(c) İstenmeyen E-posta (Spam)

Gönderildiği kişiler tarafından talep edilmediği halde, büyük miktarlarda gönderilen e-postalara, istenmeyen e-posta (spam) denilmektedir. Genelde reklam amaçlı olarak gönderilen “spam”larda içerikten ziyade gönderinin çokluğu önem taşımaktadır (TUBİTAK UEKAE, 2011). Sayıları bazen milyonları bulabilen istenmeyen e-postalar yarattıkları yoğun mesaj trafiği sebebiyle ağ problemlerine neden olabilmektedirler. Örneğin, New York'ta yaşayan Anthony Greco spam mesajları gönderebilmek için Ekim-Kasım 2004 tarihinde MySpace.com'da yanıltıcı binlerce hesap yaratmıştır. Greco, bu hesapları kullanarak, mortgage kampanyaları ve yetişkin içerikli sitelerinin reklamlarını ihtiva eden 1,5 milyondan fazla spam mesajı göndermiştir. Gelen yoğun spam mesajlarını silmek ve gelecek saldırılara önlem için alınan koruyucu tedbirler MySpace şirketine 5.000 dolara mal olduğu belirtilmektedir (Yılmaz ve Salcan, 2008, s.60-61).

HASAR TÜRÜ	MALİYET (milyar dolar)
Marmara Depreminin Yapısal Hasarı ¹²	9-13
2005 Katrina Kasırgası	43
11 Eylül Saldırısının Yapısal Hasarı	83-95
Spam'ın 2008'de yarattığı Toplam Zarar	140

Tablo-7: Spam'ın Diğer Hasar Türleri ile Mukayesesi.

(Kaynak: Joe St. Sauver, <http://www.uoregon.edu/~joe/unclesam/> adresinden alınarak düzenlendi)

İnternet ve e-posta kullanımının artışı spam yolu ile saldırıları da artırmış, bu durum büyük maddi kayıpları ortaya çıkarmıştır. Spam'ın 2008 yılında dünya genelinde vermiş olduğu zararın (Tablo-7) afetlerden ve terör saldırılarından bile daha yüksek olduğu görülmektedir. Symantec'in Kasım 2011 raporuna göre, gönderilen her 100 e-postanın 70,5'ini spamlar oluşturmaktadır.

¹²Devlet Planlama Teşkilatına göre tahmini maliyet, <http://ekutup.dpt.gov.tr/deprem/>. Erişim Tarihi:31 Ocak 2012.

(3) Kimlik Saldırıları

Kimlik saldırıları genellikle dolandırıcılık ve hırsızlık gibi suçları kolaylaştırmak maksadıyla başka kişilere ait kişisel ya da finansal bilgileri çalmayı içermektedir. Saldırının başarısı, kurbanın saldırıyı fark edememesine dayanır (Loganathan ve Kirubakaran, 2011, s.389-390). Bu tür saldırılarda genel olarak; oltalama, ortada adam saldırısı, kimlik gizleme, koklayıcı ve gizli dinleme yöntemleri kullanılmaktadır.

(a) Phishing (Oltalama)

“Phishing”, saldırganlar tarafından aldatılan kullanıcıların kendilerine ait kimlik ve hesap bilgilerini açıklamalarını sağlayan bir tür internet dolandırıcılığıdır. “Phishing” kelimesi anlam olarak, “fishing” (balık tutma) kelimesindeki “f” harfinin kaldırılarak yerine eş sesli “ph” harflerinin konulmasıyla meydana gelmiştir. Oltalama adıyla da bilinmektedir (Yılmaz ve Salcan, 2008, s.60). Phishing saldırısı çeşitli basamaklardan oluşmaktadır.

- İlk olarak saldırgan, hedeflediği kurbanlara ait e-posta adreslerini çeşitli yöntemler (tahmin, açık kaynak araştırması, sızdırma vs.) kullanarak öğrenir.
- İkinci aşamada saldırgan gerçek web sitesine benzeyen sahte bir adresten müşteriye e-posta gönderir ve bazı işlemlerde bulunmasını ister. (Örneğin, müşterinin hesabının bulunduğu bankanın web sitesi görünümündeki sahte bir e-postayı müşteriye göndererek, kimlik bilgileri, şifre vb. bilgileri güncellemesini isteyebilir.)
- Gönderilen e-postanın içeriğine göre; alıcı istenen işlemi ya da güncellemeyi yapabilir, zararlı içerik bulunan dosyayı açabilir veya istenilen web sitesine bağlanabilir.
- Başarıya ulaşan saldırgan hedeflediği alıcı ya da müşteriye ait kişisel bilgileri kullanarak dolandırıcılık işlemini gerçekleştirir (McAfee, 2004, s.3).

İnternet güvenliğinde dünyanın gelen şirketlerinden olan Symantec’in Kasım 2011 raporuna göre gönderilen her 302 e-postanın birinde “phishing” saldırısı bulunmaktadır. Aynı araştırmaya göre sektörel bazda en çok saldırıya uğrayan alanı %88,3 ile finans sektörü oluşturmaktadır (Symantec, 2011, s.16). “Phishing” saldırıları doğrudan verdiği zararların yanında dolaylı olarak da şirketlere zarar vermektedir. Bunun en önemli nedeni de, internet üzerinden alışveriş yapan müşterilerin bu tür saldırılar sonucu markaya duydukları güvenin sarsılmasıdır Larson (2010, s.1-7)’a göre “phishing” saldırıları aynı zamanda haksız rekabet yaratmaları nedeniyle fikri mülkiyet hakları çerçevesinde de değerlendirilmelidir.

(b) Ortada Adam Saldırısı (Man in the Middle Attack)

“Ortada adam saldırısında”, saldırgan kendisini müşteri ile servis arasında konumlandırarak sistemler arası bütün veri akışını gözleyip kaydedebilmektedir. Saldırgan müşteriye kendisini servis olarak, servise ise müşteri olarak tanıtmaktadır. Müşteri farkında olmadan saldırganın sitesini gerçek site zannederek bağlanır ancak bağlandığı yer saldırganın kendisini yönlendirdiği tuzak sitedir. Dikkat çekmemek için aynı anda saldırgan kendisini müşteri gibi göstererek gerçek siteye de bağlanır (Loganathan ve Kirubakaran, 2011, s.389).

(c) Kimlik Gizleme (IP Spoofing)

Kimlik gizleme, saldırıda bulunan bilgisayar korsanlarınca geride iz bırakmamak için kullanılan bir yöntemdir. Yapılan saldırı hedefin güvendiği bir bilgisayardan geliyormuş gibi gözükmeştir. Kimlik gizleme saldırılarında internet protokol (IP) numaraları kullanılır. Her IP bir bilgisayar adresini (sistem kimliğini) göstermektedir. Bilgisayarlar erişimde bulundukları sisteme güvendiklerinde veri akışı sağlamaktadırlar. Kimlik gizleme yöntemi ile kendi bilgisayarını güvenilir gösteren saldırganlar, çeşitli programlar kullanarak bu bilgisayarın kontrolünü ele geçirebilmektedir (Yılmaz ve Salcan, 2008, s.58).

(ç) Koklayıcı (Sniffers)

Koklayıcılar, ağ üzerinde bulunan IP paketlerini taramak maksadıyla kullanılan donanım ve yazılımlardır. Tüm ağ trafiğini dinleyerek kaydedebilirler. En önemli özellikleri veri paketlerinde bulunan, kimlik, şifre vb. hassas bilgileri, paket içeriğini tarayarak bulabilmeleridir. Veri paketlerinin aktif ağ cihazları kullanılarak sadece istenilen adrese gönderilmeleri, koklayıcıların bu paketleri incelemesini engelleyebilir (Canbek ve Sağıroğlu, 2006, s.207). Ancak “Sniffer” saldırılarının tespit edilebilmeleri oldukça zordur. Çünkü bunlar ağ trafiğine müdahale etmekten ziyade veri paketlerini tarayıp analiz etmektedir (Trabelsi, 2005, s.53).

(4) Gizli Dinleme (Eavesdropping)

Gizli dinleme, ağ sistemi veya herhangi bir iletişim kanalı üzerinden yapılan veri alışverişinin üçüncü kişiler tarafından takip edilmesidir. İngilizce “eavesdropping” (saçak damlası) olarak adlandırılan bu saldırıda elde edilen verinin değiştirilerek alıcıya ulaştırılması da mümkündür. Bunun yanında herhangi bir sistem ya da ağa bağlı olmayan bilgisayarlar; mikroişlemci, ekran, yazıcı, klavye vb. donanımların elektromanyetik enerji yayılımları gizlice dinlenebilir. Elektronik cihazların bu tür

TASNİF DIŞI

dinlemelere olanak vermemesi için, Amerikan hükümeti TEMPEST¹³ adında bir standart geliştirmiştir (Canberk, ve Sağıroğlu, 2007, s.8). 1943 yılında Bell laboratuvarında kriptu cihazları üzerinde yapılan bir çalışmada elektromanyetik kaçağın fark edilmesi, TEMPEST tedbirlerinin doğmasına sebep olmuştur (Saraç, 2010, s.31). 1984 yılında Hollandalı bilim adamı Win Van Eck'in, TV alıcısı üzerindeki görüntüyü yönlendirilmiş anten ve anten yükselticisi kullanarak yüzlerce metre uzaktaki bilgisayar ekranında izlenebileceğini ortaya koyması da bu alandaki araştırmaları hızlandırmıştır (Yılmaz ve Salcan, 2008, s.97).

TEMPEST, her türlü elektriksel ve elektronik cihazdan yayılan, istenmeyen elektromanyetik enerji yayılımları ve bu yayılımların kontrol altına alınması olarak tanımlanırken, meydana gelen kaçaklar da TEMPEST kaçakları olarak adlandırılmaktadır. TEMPEST kaçaklarının özellikleri ise şunlardır:

- İstem dışı meydana gelirler
- Belli bir frekanstan işaretler halinde veri taşırlar
- Kablo üzerinden veya havadan yayılma imkânları vardır.
- Elde edilen veriler çözümlenmeye ihtiyaç gösterir (Saraç, 2010, s.30).

TEMPEST önlemlerinin alınmasında öncelikli olarak hassas bilgilerin istenmeyen bölgelere hangi yollarla ulaşabileceği araştırılmaktadır. Kaçaklar genel olarak iki şekilde meydana gelmektedir.

- Uzaysal Işıma: Yayılımlar havadan enerji yoluyla dağılırlar.
- Elektriksel İletkenlik: Yayılımlar cihazdan (işaret ve güç kabloları) veya cihazın yakınındaki herhangi bir metalden (kalorifer-su boruları, telefon kabloları vs.) iletilirler.

Elektriksel iletkenlikten kaynaklanan kaçaklar akım sondası ile uzaysal ışıma yoluyla meydana gelen yayılımlar ise antenler vasıtasıyla incelenebilmektedir.

Gelişen teknoloji ile birlikte gizli dinleme çeşitleri artış gösterse de TEMPEST kaçaklarına karşı şu tedbirler alınmalıdır.

- Cihazların önceden test edilerek uygun yerlere yerleştirilmesi.
- Binaların kaçaklara karşı koruma durumunun tespit edilmesi.
- Gizlilik dereceli bilgilerin işlendiği bölgelerin izolasyonu.
- Doğru topraklama yapılması.
- Kabloların güvenli şekilde döşenmesi (Kumbasar, 2010, s.24-25).

¹³TEMPEST kelimesinin açılımıyla ilgili bir görüş birliği bulunmamaktadır. Çeşitli kaynaklarda "TEMPorary Emanations and Spurious Transmission", "Transient ElectroMagnetic Pulse Emanation Standard" veya "Test for ElectroMagnetic Propagation Emission and Secure Transmission" olarak yer almaktadır.

TASNİF DIŞI

Elektronik sistem veya cihazların uğrayacağı saldırılara karşı alınacak TEMPEST karşı tedbirlerinin incelenmesi Yılmaz ve Salcan (2008, s.98)'a göre zedelenebilirlik, tehdit ve risk konularında yapılmalıdır. Zedelenebilirlik değerlendirmesinde; bilginin bulunduğu cihazın konumu, işlenen işaretin karmaşıklığı, yetkisiz kişi veya kuruluşun kaçacağı tespit ve analiz yeteneği aranır. Tehdit değerlendirmesinde; tehdidin derecesine, saldırının kaynağına ve hedefe verilen önceliğe bakılırken, Risk değerlendirmesinde ise, saldırganların olası imkân ve kabiliyetleri ile bilginin zedelenebilirliği değerlendirilir (Yılmaz ve Salcan, 2008, s.97-98).

ç. Bilgi Teknolojileri Güvenliği

Kurumlara ait bilgi varlıklarının gizlilik, bütünlük ve kullanılabilirlik özellikleri bakımından korunması bilgi güvenliği olarak tanımlanmaktadır (Öztürk, 2008, s.7). Bilgi varlıkları olmadan kurumlar üretim yapamaz ve süreklilik sağlayamazlar. Sadece devletler değil, şirketler, holdingler, KOBİ'ler ve hemen her seviyedeki kurum ve organizasyonlar değişik oranda bilgi güvenliği sorunlarıyla karşılaşmaktadır. Bilgi değişik formlarda bulunabilir. Kâğıt üzerinde yazılı olabilir, elektronik ortamda saklanabilir veya kişiler arasında sözlü olarak da ifade edilebilir. Bilgi teknolojilerinde yaşanan gelişmeler sonucu her türlü bilgi, bilgi sistemleri üzerinde depolanmaya ve saklanmaya başlanmıştır. Hangi formda olursa olsun, mutlaka uygun bir şekilde korunmalıdır. Örneğin yazılımlar için kaynak kodların gizliliği, ağlara istenmeyen erişimlerin engellenmesi ya da zararlı yazılımlardan korunma gibi önlemler, elektronik ortamda yer alan verilerin güvenli şekilde depolanması ve iletimi açısından son derece önemlidir (Elbahadır, 2011, s.3-4).

Bilgi teknolojilerindeki veri akışına yönelik saldırılar; yarıda kesme, gizli dinleme, değiştirme ve yeniden üretme olmak üzere dört ayrı özellik sergilemektedir.

- Yarıda kesmede, kaynak ile hedef arasındaki iletişim koparılarak istenilen bilgi yok edilir veya erişilemez hale getirilir.
- Gizli dinlemede, iletişime müdahale edilmeden hassas bilgiler elde edilmeye çalışılır.
- Değiştirmede, kaynak tarafından gönderilen bilgi ele geçirilir, değiştirilir ve kaynaktan geliyormuş gibi tekrar hedefe gönderilir.
- Yeniden üretmede ise saldırgan tarafından oluşturulan bilgiler kaynaktan geliyormuş gibi hedefe gönderilir.

TASNİF DIŐI

Depolanan ve iletilen bilgilerin güvenliğine (gizlilik, bütünlük, kullanılabilirlik) yönelik, dünya genelinde belirli standartlar oluşturulmuştur. Standartların oluşturulmasındaki amaç, bilgi sistemlerine bağlanması düşünülen herhangi bir ürünün genel kabul gören bir güvenlik anlayışıyla değerlendirilmesiyle, zaman ve mali kayıpların önüne geçilmesidir.

(1) Ortak Kriter (ISO 15408)

Bilgi güvenliği konusunda, ortak bir kriter yaratılması ve bunun benimsenmesi maksadıyla ilk çalışmalara 1996 yılında başlanmıştır. ABD, Almanya, Avustralya, Fransa, İngiltere, Kanada ve Yeni Zelanda'nın öncülük ettiği bu çalışmadaki standartlara Ortak Kriter (Common Criteria-CC) adı verilmiştir. Bilgi güvenliği ihtiyacını karşılamak maksadıyla oluşturulan Ortak Kriterler, Uluslararası Standartlar Organizasyonu'nun (International Organization for Standardization-ISO) 1999 yılında Uluslararası Bilgi Teknolojileri Değerlendirme Standardı olarak kabul ettiği "ISO 15408" güvenlik standardıdır (Yılmaz ve Salcan, 2008, s.101). Gizlilik, güvenilirlik ve bütünlük açısından fonksiyonel ve sızma testleri uygulanarak ürünün veya sistemin güvenlik seviyesi tespit edilir. Değerlendirme Garanti Seviyeleri (Evaluation Assurance Level-EAL) 1'den 7'ye kadar derecelendirilir. En düşük garanti seviyesi EAL 1, en yüksek garanti seviyesi EAL 7 olarak derecelendirilmektedir. Ortak Kriterler kapsamında test edilebilecek bazı bilgi teknolojisi ürün sınıfları aşağıdadır:

- Erişim Kontrol (Access Control)
- Biyometrik (Biometric)
- Veri Koruma (Data Protection)
- Veritabanı (Database)
- Akıllı kart (Smart Card)
- Anahtar Yönetimi (Key Management)
- Ağ Cihazları (Network Devices)
- İşletim Sistemi (Operating System)
- Elektronik İmza (Digital Signature)
- Güvenlik Duvarı (Firewall, IDS vb.) (Beydağlı, 2010).

TASNİF DIŞI

Ortak Kriterler hizmeti, ülkelerde bulunan bir sertifikasyon makamı ve ona bağlı lisanlı laboratuvarlar tarafından verilmektedir. Türkiye’de, Türk Standartları Enstitüsü (TSE) sertifikasyon makamı, TÜBİTAK’a bağlı Ortak Kriter Test Merkezi (OKTEM) ise lisanslı laboratuvar olarak hizmet etmektedir (TÜBİTAK, 2012). TSE tarafından 2012 yılına kadar dokuz bilgi teknolojisi ürün Ortak Kriterler kapsamında belgelendirilmiştir (TSE, 2012).

(2) Bilgi Güvenliği Yönetim Sistemi

Bilgi Güvenliği Yönetim Sistemi (BGYS), kurumlara ait değerli bilgileri korumak ve yönetmek amacıyla oluşturulan sistematik bir yaklaşımdır. BGYS’ye ait standartlar ISO tarafından “ISO/IEC 27001:2005” olarak yayınlanmıştır. Bu konuda yapılacak bilgi güvenliği kontrol standartları da “ISO/IEC 27002:2005 Bilgi Güvenliği Yönetimi İçin Uygulama Prensipleri”nde toplanmıştır. Önel ve Dinçkan’a göre, bilgi güvenliği yönetimi konusunda en yaygın kullanılan standart, ISO/IEC 27002:2005’dir (Önel ve Dinçkan, 2007, s.5-7).

ISO 27001 standardı, sürekli gelişim gösteren tehdit ve saldırılara karşı BGYS’de yer alması gereken unsurları tanımlamaktadır. Bilgi Güvenliği Yönetim Sistemi, kısaca PUKÖ (Planla-Uygula-Kontrol Et-Önlem Al) olarak adlandırılan dört aşamalı bir döngüden oluşmaktadır. ISO 27001 standardında yer alan bu döngü, ISO 27002 standardında bulunan önlemler için kullanılmakta ve alınan tedbirler sürekli güncellenmektedir. ISO 27002 standardında 11 gruba ayrılmış 133 güvenlik önlemi yer almaktadır. Örneğin, fikri mülkiyet hakları, kurumsal kayıtların korunması, verinin korunması ve kişisel bilgilerin gizliliğiyle ilgili önlemler ilk üç grupta yer almaktadır. Onuncu grupta yer alan “bilgi güvenliği olaylarının yönetilmesi”nde; bilgi sistemi arızası, virüs saldırısı, servis dışı bırakma saldırısı, eksik veya hatalı veri girişi, gizlilik ve bütünlüğü bozan ihlaller, bilgi sisteminin kötüye kullanılması vb. durumlarda hangi işlemlerin takip edilmesi gerektiği bulunmaktadır (Ottekin, 2008).

(3) SCADA Güvenliği

Bilgisayar temelli kontrol sistemleri, kurumlarda ve dağıtık hizmetlerde yer alan kritik altyapıların (enerji nakil hatları, barajlar, nükleer santraller, boru hatları, ulaşım vs.) işletilmesinde çok önemli bir yer tutmaktadır. SCADA sistemleri geniş coğrafi alanlara yayılan fiziksel süreçleri gözlem ve kontrol etmeye yararlar. Örneğin, boru hatlarının işletilmesinde; gaz akışını ve basıncını, elektrik dağıtımında; hatlarda bulunan akım ve voltaj durumunu, su dağıtımında; su seviyesi, basıncı ve

TASNİF DIŐI

saflařtırma için katılan kimyasalların miktarını gözlemler ve kontrol eder (Ciprian, 2011, s.159).

Günümüzde tesislerin ve alt yapı hizmetlerinin büyük bölümü bilgisayar sistemleri ile kontrol edilmektedir. Bilgisayar sistemlerinde TCP/IP protokolleri kullanılması nedeniyle, bu altyapı ve tesisler internete baęlı olmasalar bile siber uzayda yaşanan güvenlik riskleri ile karşı karşıyadırlar (Kara, 2012). Bunların haricinde SCADA sistemleri řirketlerin kendi aę sistemlerine de baęlı olabilmektedir. Kapalı aę sistemine herhangi bir noktadan sızılması ya da erişilmesi halinde saldırganlar ařaęıdaki saldırıları gerçekleřtirebilirler:

- DoS saldırısı ile SCADA sunucusunu kapatmak.
- SCADA sunucusunda bulunan dosyaların silinmesi.
- Truva atı virüsü yerleřtirerek sistemin kontrolünün ele geçirilmesi.
- Kullanıcıların klavye vuruřlarının kaydedilmesi ile řifre ve kullanıcı adı gibi sisteme giriř saęlayan kritik bilgilerin ele geçirilmesi.
- Kuruma ait ticari deęeri olan işlemsel verilerin kaydedilmesi.
- Var olan verilerin deęiřtirilmesi ya da uzaktaki veri tabanına kaydedilmesi (Ciprian, 2011, s.162).

Avustralya'nın Queensland bölgesinde 2000 yılının Ocak ayında yapılan bir saldırıda, kanalizasyon řebekesine ait SCADA sistemi devre dıřı bırakılarak 264.000 galon atık su çevreye yayılmıştır. 2005 yılının Ağustos ayında ise ABD'de üretim yapan Daimler Chrysler'e ait 13 fabrika, sistemlerine sızan "Zotob" virüsü nedeniyle bir saat süre ile üretim yapamamıştır. Dięer bir olay da ABD'de bulunan Hatch Nükleer santralinde yaşanmıştır. řirketin iç aę sistemine baęlı santralde, sistemde bulunan yazılımın kendisini sürekli güncellemesi nedeniyle "acil kapanma" durumuna geçilmiştir. Yapılan arařtırmada, tesise ait SCADA aęı ile řirketin aę sistemi arasında çift yönlü bir haberleřme sistemi olduęu, iç aę sisteminin kendisi ile birlikte SCADA sistemini de güncelledięi ortaya çıkmıştır. Güncelleme sonrası veri kaybı olduęunu tespit eden SCADA güvenlik sistemi, reaktörde soęumayı saęlayan su seviyesini düşük göstermekte bu da kendilięinden kapanmaya yol açmaktaydı. Mühendisler aęda bulunan çift yönlü etkileřimi bilmekle beraber, yapılan güncellemelerin aęlar arasında senkronize olacaęını bilmiyorlardı. Kamu saęlığına bir zarar gelmemekle birlikte yaşanan zarar sonucu mühendisler řirketin kapalı aę

TASNİF DIŐI

sistemi ile tesisin SCADA sistemi arasındaki fiziksel bağlantıyı kesmişlerdir (Tsang, 2009, s.5-8).

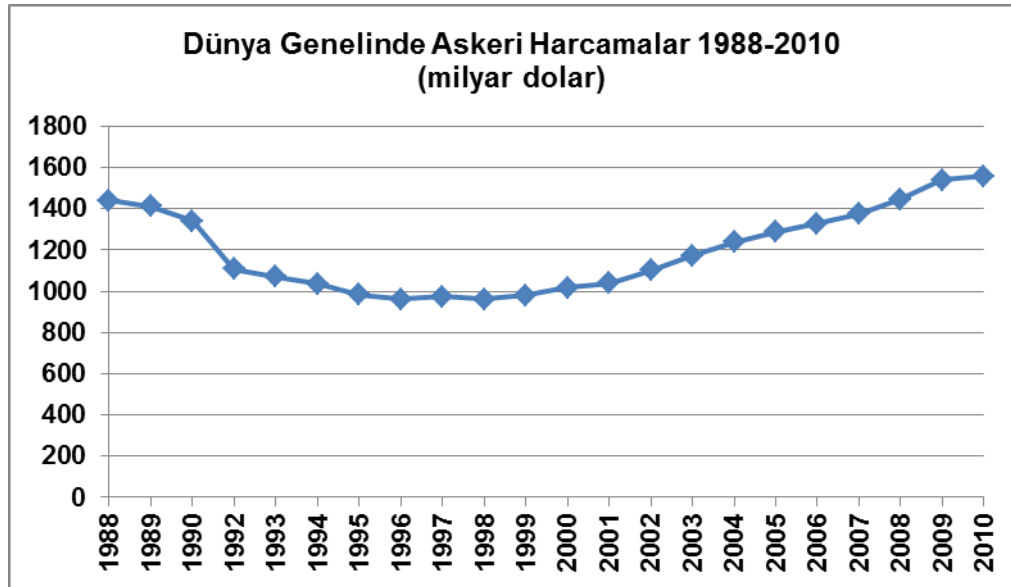
Bilişim sistemlerinde yaşanan gelişmeler güngeçtikçe üretim sistemlerine ait alt yapıların ayrılmaz bir parçası haline gelmektedir. Dolayısıyla ülkeler arasındaki küresel ticari rekabetin hedefinde fikri mülkiyet ve ticari sırlar yer alırken rekabetin zemininde ise bilişim sistemleri bulunmaktadır. Kendisine ait bir suç dünyası yaratan siber uzay her alanda olduğu gibi istihbarat örgütlerinin faaliyetlerinde de yeni ufuklar açmıştır. Soğuk Savaş sonrası değişen güvenlik algısı ve küresel rekabet ortamı istihbarat örgütlerinin ekonomik alanda faaliyet göstermesi konusunda katalizör etkisi yapmıştır. Bu nedenle Soğuk Savaş sonrası gelişen küresel rekabet ortamı ile istihbarat örgütlerinin ekonomik alanda artan faaliyetleri bu dönemi incelemeyi zorunlu kılmaktadır.

DÖRDÜNCÜ BÖLÜM

BULGULAR VE YORUM

1. SOĞUK SAVAŞ SONRASI KÜRESEL REKABET ORTAMI

II. Dünya Savaşı'nın ardından ABD ve SSCB'nin başını çektiği Batı ve Doğu Blokları arasında yaşanan, sürekli gerginlik ve kısmi çatışma biçiminde sürdürülen mücadele Soğuk Savaş olarak adlandırılmaktadır (Sönmezoğlu, 2000, s.624). Bu dönemde iki süper güç aralarında açık bir savaş çıkmasından dikkatle kaçınmakla birlikte, askeri, ekonomik, ideolojik, diplomatik vb. uluslararası ilişkilerin her alanında mücadelelerini devam ettirmişlerdir (Köni, 1999, s.77). Özellikle konvansiyonel ve nükleer silahlanma yarışı 1950,1960 ve 1970'lerde uluslararası ilişkilerin merkezinde yer alarak yüksek politikanın önemli bir parçasını oluşturmuştur. Bu yüzden ticaret, dış yardım, ekonomik kalkınma, borçlanma ve uluslararası kuruluşlar gibi konular biraz da geri planda kalmıştır. Ancak 1980'lerin başından itibaren Soğuk Savaş döneminde fazla önem verilmeyen ekonomik ve teknolojik gelişmişliğin temel bir güç olarak ortaya çıkması akabinde, Rusya'nın ve Varşova Paktı ülkelerinin ekonomik örgütler ve ekonomik bloklarla örtülmesi Köni (1999, s.79)'nin de ifadesiyle "SSCB'nin tek kurşun atılmadan çökmesine neden olmuştur".



Tablo-8: Dünya genelinde Askeri Harcamalar (Kaynak: SIPRI, 2012)

Soğuk Savaş'ın sona ermesinin uluslararası ilişkilerde iki temel etkisi olmuştur. İlk olarak Sovyet askeri gücünün Doğu Avrupa ve Üçüncü Dünya ülkelerinden çekilmesiyle demokratikleşme artarak bu ülkelerde yaşanan çatışmalar kısmen sona ermiştir. Diğer yandan süper güçler arasındaki mücadelenin uluslararası ilişkilerdeki önemini yitirmesi sonucu savunma harcamalarında da önemli düşüşler (Tablo-8)

TASNİF DIŞI

yaşanmıştır (Yılmaz, 2008, s.44). Bu azalmada savaşların düzleminin değişmiş olması da dikkate alınmalıdır. Ülkelerin daha az harcama gerektiren siber, bilgi ve ekonomik mücadelelere yöneldiği söylenebilir. Ancak 11 Eylül saldırılarının ardından ABD'nin Afganistan ve Irak'a yönelik harekâtı, askeri harcamaları tekrar yükseltmiştir. 2011 yılı dünya genelindeki askeri harcamalardaki payın %43'ünü tek başına ABD oluşturmaktadır. Askeri harcamalarda liderliği elinde bulunduran ABD'nin kaynaklarını bu alana yöneltmesi, dünya ortalamasının da göreceli olarak artmasına neden olmuştur (Global Issues, 2012).

Soğuk Savaşın ardından iki kutuplu dünya düzeni yerini ABD'nin başa geçtiği tek kutuplu dünya düzenine bırakmıştır. Ancak küresel ve bölgesel güç dengelerini belirleyen ölçütler de değişmek üzeredir. Dünyadaki güç dengelerinin oluşumunda askeri ve stratejik etmenler önemlerini korumakla beraber, ekonomik güç ve teknolojik gelişme gibi unsurlar giderek öne çıkmaya başlamıştır. Bu yüzden geçmiş ile mukayese edildiğinde ülkeler arasındaki güç dengeleri ekonomik gelişmişlik düzeyleri ile paralel olarak hızlı bir değişim süreci göstermektedir (Dindar, 2004, s.55-56). Ekonomik açıdan değerlendirildiğinde ise uluslararası sistemin tek kutupludan ziyade çok kutuplu bir yapıya sahip olduğu söylenebilir. ABD büyük bir ekonomik güç olmakla beraber yalnız da değildir (Tablo-9).

	ÜLKE	GSYH (trilyon \$)
1	ABD	14,587
2	Çin	5,927
3	Japonya	5,459
4	Almanya	3,281
5	Fransa	2,560

Tablo-9: Dünya GSYH Sıralamasında İlk Beş Ülke¹⁴ (2010)

Kaynak:(The World Bank, 2012)

2010 yılı itibarıyla Avrupa Birliği'nin toplam GSYH miktarının 12,268 trilyon avro olduğu belirtilmektedir (Eurostat, 2012). AB'nin yanında ASEAN ve APEC gibi çeşitli güç merkezleri de ortaya çıkmaktadır. Bununla birlikte ABD, Afganistan ve Irak'a yönelik operasyonların maliyetini de diğer gelişmiş veya ilgili ülkelerle paylaşmaktadır. Bu nedenle Soğuk Savaş sonrasında, tek kutuplu düzen ile

¹⁴ Sayılar yuvarlanarak verilmiştir.

TASNİF DIŞI

aralarında AB, Çin, Japonya ve Rusya'nın da bulunduğu çok kutuplu bir düzenin ortaya çıktığı söylenebilir (Yılmaz, 2008, s.46).

Soğuk Savaş sonrasında kuzeyde yer alan gelişmiş devletler ile güneyde yer alan gelişmekte olan ve az gelişmiş ülkelere arasındaki rekabet de gün yüzüne çıkmıştır. İdeolojik çatışmaların sona ermesiyle birlikte Kuzey-Güney çatışması da uluslararası ilişkilerde yer almıştır (Yılmaz, 2008, s.52). Buradan hareketle, gelişmemiş bölgelerden kitlesel göçler, terör, uyuşturucu ve insan kaçakçılığı ile etnik milliyetçilik olguları güvenliğin yeni boyutları olarak karşımıza çıkmaktadır.

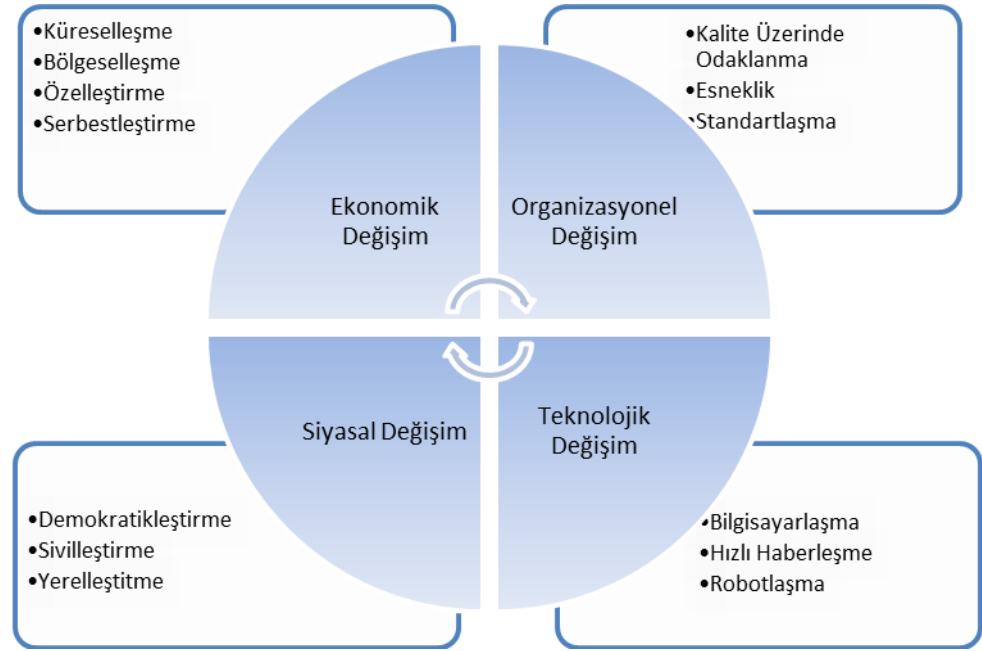
a. Yeni Dünya Düzeni ve Küreselleşme

Büyük sosyal dönüşümler; askeri, sosyo-kültürel ve ekonomik alanlara yansarak dünyadaki dengelerin değişmelerine neden olurlar. Bozulan dengeler güçlü ya da galip ülkeler tarafında yeniden tesis edilirken, yaratılan bu ortama da “Yeni Dünya Düzeni” adı verilmektedir. Ancak her yeni düzen, kuralları belirleyen hâkim güçlerin menfaatine uygun olacak biçimde şekillenir (Dindar, 2004, s.62). Yeni Dünya Düzeni Soğuk Savaş'ın ardından kapitalizmin tüm dünyada egemen hale gelmesiyle birlikte ekonomik, sosyal, siyasal ve kültürel yapıdaki dönüşümü ifade eden bir süreçtir. Bir anlamda kapitalizmin yeniden yapılanarak uluslararasılaşması da denilebilir (Sapancalı, 2001, s.116). 1991 Körfez Savaşı sırasında ABD Başkanı George Bush tarafından Kongre’de kullanılan kavramın temelinde insan hakları ve piyasa/pazar ekonomisinin korunması yatmaktaydı (Oran, 2002, s.210). Ancak terörle mücadele bahanesiyle ABD’nin Irak ve Afganistan harekâtı sırasında uluslararası hukuka aykırı uygulamaları “ Yeni Dünya Düzeninin” ne kadar düzen içerdiğini de sorgulanır hale getirmiştir.

Soğuk Savaş sonrası dengelerin değişmesiyle kurulan Yeni Dünya Düzeni’nin geldiği aşamaya “küreselleşme” adı verilmektedir. Küreselleşmenin karar ve kontrol merkezinde ABD başta olmak üzere gelişmiş devletler yer almaktadır (Dindar, 2004, s. 62-63).

TDK’ya göre küreselleşme “dünya milletlerini ekonomi, siyaset ve iletişim bakımlarından birbirine yaklaştırmaya ve bir bütün olmaya götürme” biçiminde ifade edilmektedir. Küreselleşmenin; uluslararasılaşma, teknolojik devrim, sınırların kalkması ve liberalizasyon olmak üzere dört yönü bulunmaktadır. Finans, ticaret ve yatırımların ülkeler arasında serbestçe dolaşımı uluslararasılaşma olarak kabul edilmektedir. Teknolojide yaşanan devrim sonucu bilgi ve iletişim alanındaki ilerlemeler iletişimi hızlandırmış mesafe ve yer kavramı önemsiz hale gelmiştir.

TASNİF DIŞI



Şekil-2: Küreselleşme Sonucu Meydana Gelen Değişimin Boyutları ve Dinamikleri (**Kaynak:** Çoşkun Can Aktan (1999). *Türkiye Dünya'nın Neresinde*. s.19'dan alınarak düzenlendi.)

Bilgi teknolojilerinde yaşanan gelişmelerle beraber küreselleşmenin pek çok alanda değişime yol açtığı gözlenmektedir (Şekil-2). Ekonomik sınırlar ortadan kalkmakla birlikte ülkeler bölgesel bütünleşme ile ekonomilerini korumaya çalışmaktadırlar. 1990-2004 yılları arasında 82 adet serbest bölge ve gümrük birliği anlaşması imzalanmıştır. Bunlardan bazılarını örnek vermek gerekirse;

- 1992 yılında sekiz Asya ülkesi tarafından ASEAN Serbest Ticaret Bölgesi kuruldu.
- Asya ve Pasifikte ekonomik işbirliğine yönelik 21 ülkenin katılımıyla APEC (Asya Pasifik Ekonomik İşbirliği) kurulmuştur.
- 1994 yılında ABD, Kanada ve Meksika tarafından Kuzey Amerika Serbest Ticaret Anlaşması (NAFTA) imzalandı.
- Avrupa Topluluğu 1 Kasım 1993'te yürürlüğe giren Maastricht Anlaşması ile Avrupa Birliği'ne dönüşmüş, 2002 yılında tek para rejimine geçmiştir (Çiftçi, 2004, s.67-68).
- BRIC ülkeleri olarak adlandırılan Brezilya, Rusya, Hindistan ve Çin küresel rekabette birbirlerini desteklemek amacıyla ekonomik birlik yolunda ilerlemektedir.

IMF, DTÖ, Dünya Bankası gibi örgütler küreselleşme bağlamında değerlendirilirken; NAFTA, AB, ASEAN, APEC bölgesel işbirliklerini temsil etmektedir (İyiboçkurt, 1995, s.215).

TASNİF DIŞI

Serbestlik kazanan sermaye sınır kavramının değişmesine de yol açmaktadır. Bunun yanında liberalleşme adı altında devletlerin kendi ekonomi politikaları üzerindeki etkileri özelleştirme, gümrük tarife anlaşmaları, finans sektörünün yabancı yatırımcılara açılması gibi uygulamalarla giderek zayıflamaktadır (Yılmaz, 2007, s.34). Genel olarak küreselleşme; finansal, ekonomik, teknolojik, kültürel, politik, ekolojik, coğrafi ve sosyolojik olmak üzere sekiz boyutta ele alınmaktadır.

- Ekonomik küreselleşme; özellikle çok uluslu şirketlerin ve bunların çoklu (konsorsiyum) birleşimlerinin dünyanın her yerinden sağladığı mal, işgücü ve hizmetin serbestçe dolaştığı,
- Siyasal küreselleşme; özelleştirme, serbest piyasa ekonomisi ve neo-liberal politikaların hızla yayıldığı,
- Sosyal küreselleşme, hükümet dışı organizasyonlar yoluyla dünya toplumu düşüncesinin yaygınlaştığı,
- Teknolojik küreselleşme, bilgi iletişim teknolojileri ve internet kullanımının hızla arttığı,
- Finansal küreselleşme, özellikle bankalar ve borsalar yolu ile dünya sermaye piyasasının karşılıklı olarak birbirine bağlandığı,
- Coğrafi küreselleşme, iletişim ve ulaşımın kazandığı hız nedeniyle sınırların kalktığı,
- Kültürel küreselleşme, Batı'lı kültürel değerlerin egemen olduğu ve tek tip tüketime doğru gidildiği,
- Ekolojik küreselleşme, dünya genelinde sınır tanımayan ekolojik sorunların (küresel ısınma, tsunami vb.) ortaya çıktığı, durumu ifade etmektedir (Adıgüzel, 2011, s.68-69).

Küresel ticaret 1980'li yıllarda ekonomik faaliyetlerin %17'sini oluştururken bu oran 2000'e gelindiğinde %26'ya ulaşmıştı. Ancak küresel ticaretle birlikte devletlerin ekonomik döngüleri de birbirine daha sıkı bağlanmıştı. Zira 2001 yılında ekonomik krizle birlikte ABD, Asya ve Avrupa ülkelerinin aynı anda düşüşe geçmesiyle ulusal ekonomilerdeki gerilemenin birbirine bağlı olduğu görüldü (Betz, 2010, s.63). Küreselleşmeyle birlikte sınır ötesi nitelik kazanan şirketler, maliyet açısından faydalı bölgelere üretimin çeşitli aşamalarını taşımakta, esnek üretim, esnek zamanlı çalışma, tam zamanında teslim, gibi yöntemler kullanarak üretim, dağıtım ve pazarlama faaliyetlerini yeniden organize edebilmektedirler (Acar, 2004, s.2-3).

Her ne kadar küreselleşme ile birlikte ulus devletin öneminin azaldığı iddia edilse de, sanayileşmiş ülkelerdeki devlet harcamaları gün geçtikçe artmaktadır. GSMH'ye göre 1913'te %12 olan bu harcamalar, 1995'te %45'e yükselmiştir. Çiftçi

TASNİF DIŞI

(2004, s.54)'ye göre, “bu genişlemenin altında, devletin istikrar, bölüşüm ve büyüme kaygılarına dayalı olarak ekonomide daha büyük bir kaynağa hükmetme kaygısı yatmaktadır.” ABD, Avrupa ve Japonya şu an ki durumlarını küreselleşmeden ziyade, genç sanayilerini koruyarak ilerletmelerine ve birbirlerinin teknolojilerini kopyalamalarına borçludurlar. Günümüzün ekonomik arenası iddia edildiği kadar serbest değildir. Az gelişmiş ülkeler için önemli olan çalışanların ve teknolojinin küresel dolaşımına izin verilmemektedir. Bu ülkeler sıkı göçmenlik düzenlemeleri ve fikri mülkiyet koruma kanunları ile karşılaşmaktadır (Rivero, 2003, s.5-6). DTÖ, Dünya Bankası ve IMF’de ABD’nin üstünlüğü bulunmaktadır. Oy kullanma gücü bakımından en yüksek oy oranı ABD’ye aittir. Önemli kararlarda oyların %85’inin gerektiği IMF’de %17,11’lik oranla ABD etkili ve veto edici bir güce sahiptir. (Yılmaz,2007,s.53).

Küreselleşme taraftarlarınca serbest piyasada yürütülen rekabet sayesinde tüm ülkelerin refah ve zenginliğe ulaşacakları iddia edilmekle birlikte sonucun son derece farklı olduğu görülmektedir. Gerek ülkeler gerekse bireyler bakımından refah seviyeleri arasındaki mesafe giderek uçuruma dönüşmektedir. Sahra-altı Afrika ülkelerinin toplam GSMH’ları AB’de tarım teşviklerine ayrılan fonlardan daha azdır (Karadeli, 2003, s.21). 2007 verilerine göre dünya nüfusunun %20’sini oluşturan gelişmiş devletler dünya gelirinin %81’ine sahipken, en fakir %20’lik nüfus ise toplam gelirden %1 pay almaktadır. Toplam nüfusun %60’ına düşen miktar ise gelirin %18’idir (UNICEF, 2011, s.13). Gelir dağılımındaki eşitsizliğin en somut göstergesi ise dünya nüfusunun %22’sini oluşturan 1.2 milyar insanın günde sadece 1.25 dolardan az bir ücretle çalışmasıdır (UNICEF, 2011, s.20).

Sonuç olarak küreselleşme nedeniyle ülkeler arası ekonomik anlamda artan bağımlılık uluslararası ilişkileri daha karmaşık bir yapıya büründürmüştür. Klasik devletler arası ilişkilerde, devletler ve firmalar arasındaki ilişkiler yükselen değer olarak karşımıza çıkmaktadır. Ancak küreselleşmenin getirdiği değişim ekonomik tartışmaları ön plana çıkararak yeni bir rekabet ortamı yaratmıştır (Ünsal, 2003, s.43-44).

b. Küresel Rekabet Ortamı

Küreselleşme ile birlikte devletlerin, bölgesel örgütlenmelerin ve şirketlerin kıyasıya yarıştığı bir rekabet ortamı doğmuştur. TDK’ya göre rekabet; “aynı amacı güden kimseler arasındaki çekişme, yarışma” olarak ifade edilmektedir. Rekabetin Korunması Hakkındaki Kanunda ise, “mal ve hizmet piyasasındaki teşebbüsler arasında özgürce ekonomik kararlar verilebilmesini sağlayan yarış” olarak

TASNİF DIŐI

tanımlanmaktadır. Ticari faaliyetlerine devam eden ve varlığını sürdüren her işletmenin rekabet gücü olduđu söylenebilir. Bu güç piyasadan pay alabilme kapasitesini ifade etmektedir (Adıgüzel, 2011, s.5).

Rekabet, rakiplere karşı üstünlük, kazanç veya başarı sağlama mücadelesidir. Kaynak temininden, mal ve hizmetin üretimine, pazarlanmasına ve tüketiciye ulaştırılmasına kadar geniş bir alana yayılmıştır. Firmaların piyasadaki fiyatı etkileme gücü anlamına da gelmektedir (Çiftçi, 2004, s.34).

20'nci yüzyılda yaşanan mücadelede uygun rekabetin (niche competition) yerini 21'inci yüzyılda kafa-kafaya (head to head competition) rekabet almıştır. Herkesin öne geçme şansının olduđu, “kazan-kazan” anlayışı ile hiç kimsenin dışlanmadığı rekabet “uygun rekabet olarak adlandırılmaktadır. Ancak kafa-kafaya rekabet ise kimilerinin kazanıp kimilerinin kaybedeceği “kazan-kaybet” anlayışının hâkim olduđu bir ortamda yürütölmektedir. Özellikle mikro elektronik, biyo-teknoloji, telekomünikasyon, havacılık, yazılım, mekanik gibi anahtar sanayilerde herkesin ele geçiremeyeceğı alanlarda rekabet tüm hızıyla sürmektedir (Çiftçi, 2004, s.35). Yeni ürünlerin pazardaki başarısında tasarım ve geliştirme zamanı da son derece önemlidir. Piyasaya rakiplerinden sonra giren firmalar yüksek kalite veya düşük fiyat sunmadıkları takdirde rekabet avantajlarını yitirmektedirler. Bununla birlikte başarı için tasarım da tek başına yeterli olmamaktadır. Ürün geliştirme süreciyle birlikte pazarlama sürecinin iyi yönlendirilmesi gerekmektedir. Bu durum da ancak ürün ve üretkenlikte yeniliğı sağlayarak, pazar değışimlerine kısa sürede yanıt vererek ve rekabet avantajları yakalanarak sağlanabilir (Betz, 2010, s.127-129).

Uluslararası ortamdaki işletmelerin rekabet gücü çok boyutlu olmakla birlikte, ülkenin rekabet gücü işletmelerin ortalama rekabet gücünden daha fazlasını kapsamaktadır. Ülkenin kurumsallaşma durumu, üretim yapısı, kapasitesi, teknolojik alt yapısı, nitelikli insan sermayesi, iç hukuk düzeni, üyesi olduđu ekonomik organizasyonlar ile yakından ilişkilidir. Bununla birlikte uzmanlaşma, marka tanınmışlığı, ürün kalitesi, teknolojik liderlik, hizmet, fiyat politikası, kendi devleti ve ev sahibi ülke ile ilişkiler gibi stratejik boyutları da bulunmaktadır (Porter, 2000, s.161). Burada yer alan stratejik boyutlar da bir devletin ürettiğı malların kalite ve fiyat bakımından rakip devletler ile yarışabileceğini gösterir (Çiftçi, 2004, s.40).

İlerleyen zaman içerisinde gelişen rekabet anlayışına bakıldığında 1960'lı yıllarda üretim üstünlüğü, 1970'lerde maliyet ve ürün özellikleri, 1980-1990'lı yıllarda kalite, yenilik, farklılık, hız ve esneklik, 2000'li yıllarda ise bunlara ek olarak mükemmeliyetçiliğin ön plana çıktığı görölmektedir (Çiftçi, 2004, s.41). Betz (2010,

TASNİF DIŞI

s.188)'e göre, "rekabetçi avantajlar, becerikli bir yönetim ile baskın bir pazar payını elde tutmayı sağlayan yüksek kaliteli bir ürünü geliştirmenin ve düşük maliyetle üretmenin baskın kombinasyonundan doğar". Bir ürünü ilk üreten diğer rakipleri tesis kurmakla uğraştığı sırada düşük maliyet imkânından yararlanır. Marka tanınırlığı ve pazar payı kazanarak dağıtım sistemini güçlendirir. Rakipler yeni eleman olarak organizasyon kurmaya başladığında onun çalışanları ve yöneticileri deneyim kazanır (Betz, 2010, s.188).

Küresel rekabet ortamının tanımlanmasında "sürekli yenilik" ve "hiper rekabet" önemli yer tutmaktadır. İşletmelerin rekabeti devam ettirebilmeleri için çok farklı ve esnek teknolojik yetenekler geliştirmesi gerekmektedir (Adıgüzel, 2011, s.1). Bu yeteneklere de ancak bilgi toplumu olabilmeyi başaran ülkeler sahip olabilmektedir. Bilgi toplumunu sanayi toplumu ile mukayese edecek olursak;

- Sanayi toplumundaki maddi sermayenin yerini fikri sermaye almıştır
- Sanayi toplumunda mal üretiminde insan ve makinenin uyumlaştırılması hedeflenirken, bilgi toplumunda insanlar bilgi etrafında örgütlenmektedir.
- Sanayi toplumunun gelişmesinde buhar makineleri ve içten yanmalı motor büyük rol oynarken, bilgi toplumunda bunların yerini veri tabanları, bilişim teknolojileri ve bilgi ağları almıştır
- Sanayi toplumunda maddi değerler ön planda olduğu halde bilgi toplumunda en önemli unsur zamandır (Barutçu, 2006, s.148).

Adıgüzel (2011, s.121)'e göre, "bugünkü küresel rekabet ortamını oluşturan iki ana vektör: 'küreselleşme ile bilgi toplumu' ve onun ekonomisi olan 'yeni ekonomi'dir." Yeni ekonomiyi farklı kılan küresel, enformasyonel ve ağ örgütlenmesine dayalı olmasıdır. Enformasyoneldir, çünkü organizasyonların üretkenliği bilgiye dayalı üretme ve işleme kapasitelerine bağlıdır. Küreseldir, çünkü emek, sermaye, hammadde gibi üretim ve tüketimin bileşenleri kurumlar ya da organizasyonlar arasındaki ağ üzerinden küresel bir ölçekte örgütlenmişlerdir. Son olarak ağ örgütlenmesine dayalıdır, çünkü üretim küresel bir girişim ağları üzerindeki etkileşim ağı üzerinden gerçekleşir. Rekabetin yaşandığı yer burasıdır (Castells, 2008, s.99). Yeni ekonomi özellikle bilgi teknolojileri ve finans sektöründe şekillenmiştir. ABD'nin 1995-1998 yılları arasındaki GSYH'daki payı %8 olan bilgi teknolojileri sektörünün yükselişteki katkısı %35'tir. Bu yüzden 1990'larda ABD'de yaşanan büyümede bilgi teknolojilerinin katkısı oldukça büyüktür (Castells, 2008,

TASNİF DIŞI

s.186-187). Yirminci yüzyılın sonlarına gelindiğinde işletmeler bilgi teknolojilerini çeşitli alanlarda ekonomik açıdan doğrudan kullanmaya başlamışlardır.

- Doğrudan bilgi teknolojilerinde mal ve hizmet üretimi yapanlar (Apple, Dell)
- Bilgi teknolojilerini mal ve hizmet teslimi için kullananlar (ebay, Amazon)
- Bilgi teknolojilerini ürün ve hizmet tasarımında destekleyici bir teknoloji olarak kullananlar (neredeyse tüm sektörler)
- Pazarlama ve reklam aracı olarak bilgi teknolojilerini kullananlar (web sayfaları) (Betz, 2010, s.307).

Ekonomik refahın göstergesi olan ekonomik büyüme hızı ve rekabet gücü arasında yakın bir ilişki bulunmaktadır. Zira rekabet gücü yüksek ülkelerin refah düzeyleri de yüksektir (Çiftçi, 2004, s.99). Üretim ve ihracatın artması kârı artırmakta, yapılan yeni yatırımlarla istihdam da genişlemektedir.

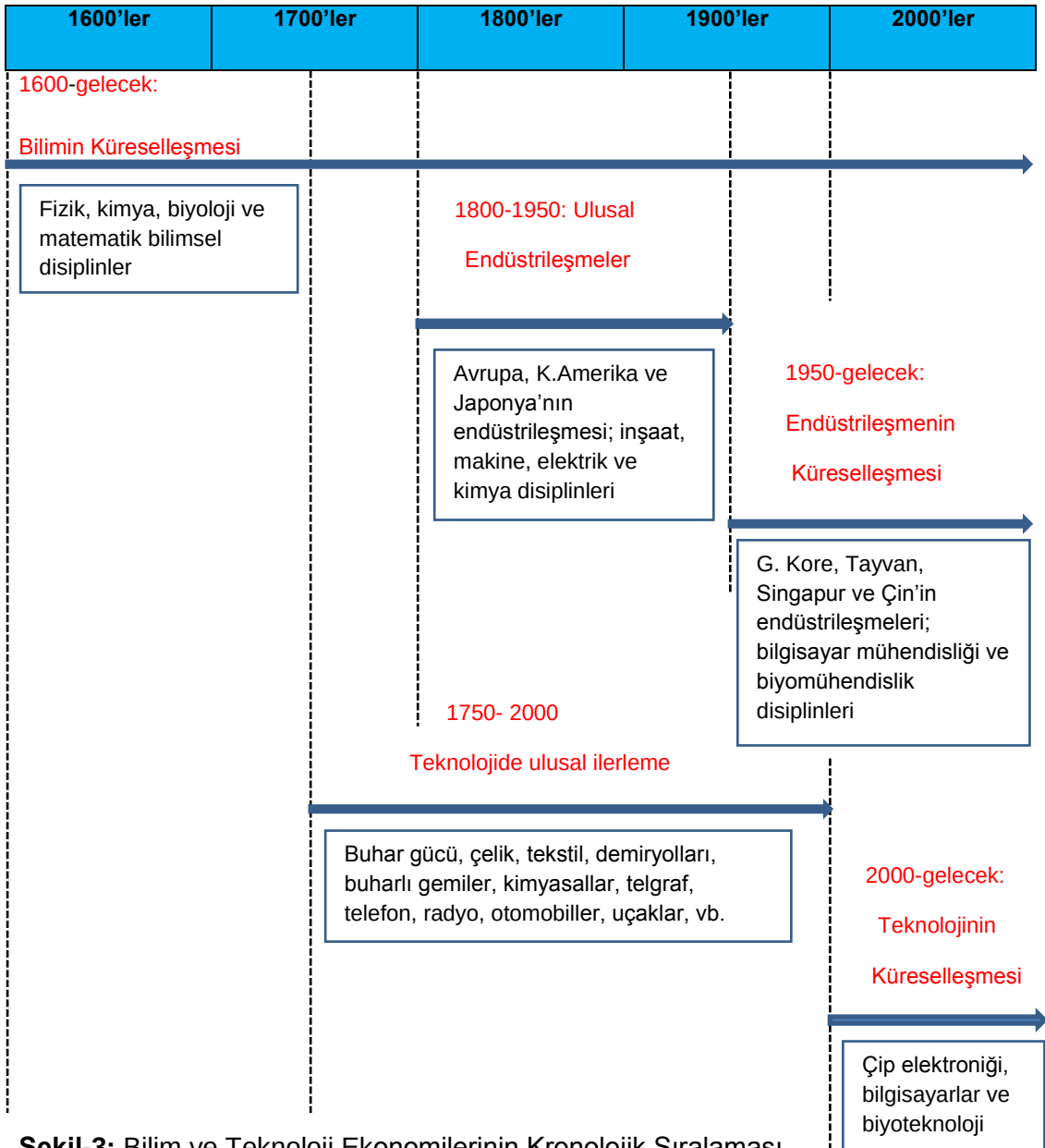
(1) Teknolojik Yenilik ve ARGE

Endüstride teknolojik yenilik yapmak için yapılan araştırma faaliyetleri kısaca ARGE (araştırma ve geliştirme) olarak adlandırılmaktadır (Betz, 2010, s.141). Küresel rekabet ortamında avantaj elde etme konusunda ARGE çalışmalarının tartışmasız üstünlüğü bulunmaktadır. Örnek vermek gerekirse elektronik bir ürünü piyasaya süren ilk iki üretici pazarın %80'ini ele geçirebilmektedir. Microsoft şirketi ARGE'ye ayırdığı yılda yaklaşık 1 milyar doları mevcut ürünlerini piyasada tutmaktan ziyade kendi teknolojisini iskartaya çıkarıp yerine yenisini ikame etmek için harcamaktadır. Bunu yapmadığı takdirde dünyadaki herhangi bir şirketin hatta bir üniversite öğrencisinin kendisinin yerine bu yeniliği yapabileceğini bilmektedir. Bu nedenle yenilik için yapılan yatırımlar bugünün tekeli korumak için değil onun yerini alacak tekele oluşturmak için yapılmaktadır (Adıgüzel, 2011, s.140).

Hızla büyüyen Apple, Dell, Hewlett-Packard vb. şirketlerin en belirgin özellikleri hepsinin de teknoloji-temelli firmalar olmalarıdır. Ülkeler de teknolojik gelişmeyi desteklemekte bu tarz üretim yapan firmaların aynı bölgelerde çalışmalarını teşvik etmektedirler. Örneğin ABD'de bulunan Silikon Vadisi, İngiltere'de Cambridge bölgesi, Japonya'daki Tokyo Yüksek Teknoloji Enstitüsü ekonomik değeri olan teknolojik yeniliklerin yoğun olarak üretildikleri bölgelerdir. İleri teknoloji kullanımı gerektiren endüstri dallarına (havacılık, elektronik, bilgisayar, ilaç vb.) bakıldığında pazar koşullarının oldukça belirsiz, ürün niteliklerinin farklı ve yoğun ARGE yatırımlarının bulunduğu gözlenmektedir (Adıgüzel, 2011, s.127). Her üretim açısından yenilik, rekabette düşük ürün maliyetleri ve üretimdeki gelişmeler açısından kritik önem taşımaktadır. Çünkü ilk üretim, diğerlerine göre daha maliyetli, daha düşük kaliteli ve daha güvensiz olacaktır (Betz, 2010, s.331).

TASNİF DIŞI

Teknolojik yenilik ve ARGE çalışmalarının temelinde bilimsel çalışmalar yer almaktadır (Şekil-3). Betz (2010, s.67-68)'e göre bilim Newton'un yeni fikirleri matematikteki gelişmelerle birleştirip matematiksel uzay, zaman ve kuvvet teorilerini bulmasıyla başladı 18. yüzyılda bu düşünceler fizik, kimya, matematik disiplinlerine dönüşürken Sanayi Devrimine de öncülük etti. Sanayi Devrimi'nin başlatıcı unsuru olan İngiltere'yi 19. yüzyılda Fransa, Almanya ile diğer Avrupa ve Kuzey Amerika ülkeleri takip ederken ulusal sanayileşme modelini Japonya ve Asya ülkeleri de model olarak aldılar. Ancak 20. yüzyılın sonu ile birlikte şirketlerin küresel ticarete ortaya çıkmalarıyla endüstrinin ve dolayısıyla teknolojinin küreselleşmesinin önü açıldı.



Şekil-3: Bilim ve Teknoloji Ekonomilerinin Kronolojik Sıralaması

(Kaynak: Frederick Betz, Teknolojik Yenilik Yönetimi: Değişimle Gelen Rekabet Avantajı, 2010, s.672'den alındı.)

TASNİF DIŞI

Yeni teknolojiler ekonomik açıdan gelişmeyi getirmekle birlikte zaman içerisinde ekonomik daralmaya da yol açmıştır. Bu duruma örnek olarak İngiltere’de arka arkaya yaşanan ekonomik daralma gösterilebilir. Sorunla ilgili olarak Konradieff, yeni teknoloji ile artan üretim kapasitesinin pazar talebinin önüne geçebileceğini bu durumun da aşırı kapasite daralmalarına neden olabileceğini öne sürmüştür. Konradieff uzun ekonomik daralması adı verilen bu süreç aşağıdaki aşamalardan oluşuyordu:

- Bilim teknolojik buluşla birlikte yeni doğa manipülasyonu sağlayan fenomen keşfeder.
- Bulunan yeni teknoloji yeni endüstriler için fırsatlar yaratır.
- Endüstrideki yenilikle birlikte hızlı pazar büyümesi ve ekonomik büyüme sağlanır.
- Yeni endüstri alanında çalışmaya devam ettikçe ürünler gelişir, fiyatlar düşer ve pazar hacmi büyür.
- Pazara giren rakip sayısı artarak daha fazla üretim gerçekleşir.
- Üretim miktarı pazar talebini geçer bu durum da fiyat indirimine neden olur.
- Düşük fiyatlar marjı düşürür ve işlerin bozularak işsizliğin artmasına neden olur.
- Piyasalarda yaşanan karmaşa durgunluğu bunalıma çevirebilir.
- Yeni teknolojik gelişmeler yeni bir ekonomik genişleme için tetikleyici olabilir (Betz, 2010, s.54-55).

1980’li yıllarla birlikte hızlı pazar değişiklikleri, ürün ve üretim teknolojisi değişiklikleri ve yeni rekabet koşulları endüstriyel şirketleri daha fazla etkilemeye başlamıştır. Bunun yanında artan rekabet ve teknolojik değişimlerle ters orantılı olarak ürünlerin pazar içerisindeki ömür süreleri de kısalmıştır. Dolayısıyla şirketler düşük maliyetli ve yüksek kalitede üretim yapan, değişik taleplere cevap verebilen esnek üretim ve üretim yönetimi teknolojilerini kullanmak ve geliştirmek durumunda kalmıştır (Çiftçi, 2004, s.24). Burada teknolojik yenilik üç seviyede ele alınmaktadır.

- Radikal Yenilik: Buhar motoru ya da buharlı gemi gibi daha önce var olmayan temel teknolojik yenilik.
- Artımsal Yenilik: Buhar motorunda regülatörün kullanılmasında olduğu gibi daha önce bulunan teknolojide performans, kalite, güvenlik, maliyet vb. konularda değişim sağlayan ancak fonksiyonu değiştirmeyen yenilik.
- Yeni Nesil Teknoloji Yeniliği: Artımsal yenilik ile aynı özellikleri taşımakla beraber yeni uygulamaları da beraberinde getiren yenilik (uçaklarda pervanenin yerini jet motorlarınının alması) (Betz, 2010, s.82).

TASNİF DIŞI

Teknolojide yaşanan gelişmeler sadece üretime değil, hizmet ve faaliyetlere de uygulanmaktadır. Bu gelişmelerin bir kısmı jenerik (herkesin bildiği) ya da müseccel (ticari sır- sadece şirket tarafından bilinen) teknolojiler olabilir. Mühendisliğin aleni standartları olan jenerik teknolojiler gerekli olmakla birlikte yeterli değildir. Belirli bir üretim alanında hizmet veren firmalar genellikle benzer teknoloji seviyesinde hizmet vermektedirler. Bunlar arasında en ileri jenerik teknolojiyi kullananlar küresel olarak rekabet şansına sahiptir. Müseccel teknoloji ise jenerik teknolojide fark yaratan ve sadece ilgili firma tarafından bilinen detaylardır. Tüm rakipler arasında rekabette öne geçmeyi sağlar (Betz, 2010, s.357). Tüm endüstrilerin temelinde karakteristik olarak yer alan dört temel teknoloji bulunmaktadır.

- Çekirdek Teknoloji: Gerekli ve tek.
- Destekleyici Teknoloji: Gerekli ama tek değil.
- Stratejik Teknoloji: Hızlı değişen teknoloji.
- İlerleyen teknoloji: Rekabeti belirleyen ve hızlı gelişen teknoloji.

Çekirdek teknolojiler temel fonksiyonel dönüşümleri sağlarlar. Örneğin otomobiller için çekirdek teknolojiler, motor ve montaj hattı teknolojileridir. Çekirdek teknolojilerde önde olan firmalar büyük bir avantaj yakaladıkları gibi rakiplerinin kendilerine zarar verme ihtimallerini de ortadan kaldırırlar. Destekleyici teknolojiler gerekli olmakla birlikte çekirdek teknolojiler kadar vazgeçilmez değildirler. Her iki teknoloji türü için de diğerlerine göre daha hızlı gelişen alanlar “stratejik teknoloji” olarak adlandırılırken, endüstriyel rekabetin doğrultusunu belirleyenler “ilerleyen teknoloji” olarak ifade edilmektedir (Betz, 2010, s.182-183).

Sonuç olarak küresel rekabet ortamında rekabet gücü yeni teknolojiler üreterek bu teknolojileri hızla yeni ürünlere ve üretim süreçlerine dönüştürme yeteneğine bağlıdır. Teknoloji transferi ile teknoloji yeteneği belirli bir noktaya kadar idame edilse bile üretimi gerçekleştirenler her zaman bir adım önde olacaklardır (Akin, 2001, s.246-247).

(2) Çok Uluslu Şirketler (ÇUŞ)

Küreselleşme ile birlikte sermayenin serbest dolaşımı özel işletmelerin de sınır ötesinde daha kolay ticaret yapmasına imkân sağlamıştır. Birden fazla ülkede yatırım yaparak üretim, dağıtım ve ticaret yapan, personel çalıştıran bu işletmeler Çok Uluslu Şirket (ÇUŞ) olarak tanımlanmaktadır. Çok uluslu şirketler, önde gelen pek çok kritik sektörde (kimya, ilaç, otomobil, elektronik eşya, enerji vb) uluslararası üretime hâkimdirler. BM yıllık Dünya Yatırım Raporuna göre bu sektörlerde yapılan

TASNİF DIŞI

ticaret ve yatırımın %60'ından fazlası şirketlerin kendi içlerinde gerçekleşmektedir. Bununla birlikte dünyadaki tüm doğrudan yabancı yatırımların %80'inden fazlası ve ticaretinin yarısı büyük çok uluslu şirketler tarafından gerçekleştirilmektedir (Yılmaz, 2007, s.367).

Dünya genelinde ticaret ve rekabet gün geçtikçe çok uluslu şirketlerin faaliyetleri ile ilintili hale gelmektedir. ÇUŞ'lar dünya ticaretinin önemli bir bölümünü gerçekleştirmektedirler ve teknolojik olarak gelişmiş ve farklılaşmış ürünlerdeki payları daha büyüktür. Örneğin ABD'de ÇUŞ'ların çoğunluk hisselerine sahip oldukları yabancı bağlı şirketlerine ihracatları 1977 yılında %41 iken bu rakam 1996 yılında %46'ya çıkmıştır (Lall, 2003, s.42).

1999 yılına gelindiğinde dünyadaki en büyük 100 ekonominin 51'ini şirketler, 49'unu ise ülkeler oluşturmaktaydı. Mukayese yapmak gerekirse General Motors Danimarka'dan, DaimlerChrysler Polonya'dan, Royal Dutch Shell Venezüella'dan, IBM Singapur'dan ve Sony şirketi de Pakistan'dan daha zengin durumdaydı. ABD'de ilk beş sırada yer alan General Motors, Wal-Mart, Exxon Mobil, Ford Motor ve DaimlerChrysler'ın 1999 yılı satış rakamları 182 ülkenin GSYİH toplamlarından daha fazladır (Anderson ve Cavanagh, 2000).

	Şirket Adı	Gelir Miktarı (milyar \$)	Kâr Miktarı (milyar \$)
1	Wal-Mart Stores (ABD)	421,849	16,389
2	Royal Dutch Shell (Hollanda)	378,152	20,127
3	Exxon Mobil (ABD)	354,674	30,460
4	BP (İngiltere)	308,928	-3,719
5	Sinopec Group (Çin)	273,422	7,629
6	China National Petroleum (Çin)	240,192	14,367
7	State Grid (Çin)	226,294	4,556
8	Toyota Motor (Japonya)	221,760	4,766
9	Japan Post Holdings (Japonya)	203,958	4,891
10	Chevron (ABD)	196,337	19,024

Tablo-10: Dünyanın En Büyük İlk On Şirketi (2011)

Kaynak: (CNNMoney, 2011)

TASNİF DIŐI

Fortune Dergisinin 2011 yılında dünyanın önde gelen şirketlerini belirlemek için yaptığı ilk 500 sıralamasında (Tablo-10) 133 Amerikan, 68 Japon ve 61 Çin firması yer almaktadır. Çin'in ekonomik kalkınmadaki hızı şirketler bazında açıkça hissedilmektedir. 2005 yılında ilk 500'de Çin'e ait 16 şirket bulunmaktaydı. Çin'li petrol şirketi Sinopec 2005 yılında aynı sıralamada 31'inci sırada yer alırken 2011'de 5'inci sıraya yükselmiştir (CNNMoney, 2005).

Az sayıda şirketin belli sektörlerde egemen olması oligopolistik bir rekabet ortamını da beraberinde getirmiştir. Örneğin ABD otomotiv endüstrisinde 1909 yılında 69 yerli otomobil şirketi varken bu sayı 1960 yılına gelindiğinde dörde (General Motors, Ford, Chrysler ve American Motors) düşmüştür (Betz, 2010, s.189). Küreselleşme sonucu oligopol bir yapıya bürünen piyasalara örnek verecek olursak;

- Yazılım sektörünün %90'ı Microsoft tarafından kontrol edilmektedir.
- Ticari uçak üretiminde dünya çapında rekabet edebilen iki firma kalmıştır. Bunlardan ilki Amerikan Boeing firması, diğeri Avrupa konsorsiyumu olan Airbus'tur.
- Exxon/Mobil, Shell, Eni, BP Amaco, Elf gibi dev petrol şirketleri, petrolün çıkarılması, işlenmesi ve dağılmasında toplam pazarın %80'lik kısmını ellerinde tutmaktadırlar (Gallino, 2007, s.91-92).

ÇUŞ'lar dünya GSYH'nın beşte birini oluştururken, iç ticaretleri de dünya ticaretinin üçte birine yakındır. Aşağıda sıralanan faktörler bunun nedeni olarak gösterilebilir:

- Liberalleşen ticaret ve yatırım politikaları,
- Ulaştırma ve haberleşme hizmetlerindeki gelişmeler,
- Üretim ve dağıtımda uzmanlığın artan önemi,
- Şirketlerin kendi ülkelerindeki olumsuz koşullar,
- Bölgesel iktisadi entegrasyon eğilimleri,
- Şirket birleşmelerinin yarattığı avantajdan faydalanma,
- Ölçek ekonomilerinin avantajlarından faydalanma,
- Vergileri, ticari engelleri, ulusal düzenlemeleri aşmak ve döviz kuru riskini azaltmak,
- Yatırımları çeşitlendirerek piyasalardaki boşluğu doldurma,
- Ticari sınırların şirketler bazında etkin korunması,
- Hammadde kaynaklarına daha rahat erişebilme (Adıgüzel, 2011, s.83-85).

TASNİF DIŞI

ÇUŞ'lar ile bağlı bulundukları ülkeler sürekli etkileşim halindedirler. Kendi ülkelerine bağlı şirketlerin küresel pazarda hâkim olmasını isteyen devletlerin de bu şirketlerde belli oranda pay sahibi oldukları gözlemlenmektedir. Devletlerin kontrolü altında bulunan şirketler genellikle bir bakanlığa ya da devlet kontrolünde bulunan bir holding şirkete teslim edilmektedir. Uzun zamana yayılan bu mülkiyet ilişkisinin şirketin, bakanlık veya holding şirketinin etkisinde kalmasına neden olabileceği ifade edilmektedir (Ararat ve Yurtoğlu, 2006, s.16).

Devletler çok uluslu şirketleri etkilemekle birlikte tam tersi bir etkileşim de dikkati çekmektedir. Örneğin dünya sıralamasında ilk 200'de yer alan 82 Amerikan şirketinin 2000 yılı seçimlerinde yapmış oldukları destek miktarı 33 milyon dolar civarındadır. Yapılan araştırmaya göre bu şirketlerin desteklerini alan adayların %94'ü ABD Temsilciler Meclisinde rakiplerini geride bırakmışlardır (Anderson ve Cavanagh, 2000)

c. Ekonomik Güvenlik

Soğuk Savaş döneminin çift kutuplu dünyasında liderliği elinde bulunduran ABD ve SSCB'nin yenilmez olduklarının düşünülmesine rağmen, ABD'nin Vietnam, SSCB'nin de Macaristan ve Çekoslovakya'da ve Afganistan'da büyük dirençle karşılaşması esasında her iki süper gücün askeri güç ile şartları çok da iyi yönlendiremediklerini göstermiştir (Karadeli, 2003, s.18). Aynı zamanda politik ve ekonomik hedeflere ulaşmada savaşın hangi ölçüde maliyet-etkin bir yöntem olduğu da Batı'da sorgulanmaya başlamıştır.

Ulusal Güvenlik kavramının Soğuk Savaş sonrası geçirdiği değişim ulusal güvenliğe yönelik tehditlerle mücadele yöntemlerini de değiştirmiştir. Askeri alandaki tehditlerle birlikte, ekonomik, siyasal, ekolojik ve sosyal hassasiyetlerde tehdit kapsamında değerlendirilmeye başlanmıştır (Dindar, 2004, s.56). Bazı yazarlar bu değişimin dünya politikasında da temel bir dönüşüme neden olduğunu ifade etmektedir. Buna göre; gelişmiş devletler artık jeopolitik dönemden jeoekonomik döneme geçmişlerdir. Geçmişte toprak kazanmak için savaşan devletler günümüzde küresel pazara sahip olabilmek adına teknolojik liderlik için mücadele etmektedirler (Denk, 2000, s.9-22). Buzan (1997, s.6-7)'a göre uluslararası ilişkilerde önde gelen güçler arasında savaş ihtimali kaybolduğu takdirde askeri güvenliğe öncelik veren realist anlayışa da şüpheyle bakılmaktadır. Bu yüzden ekonomik ve sosyal alanda gelişmiş devletlerin birbirleri ile doğrudan savaşma eğiliminde olmadıkları gözlenmektedir. Zira 1945 ve 2000 yılları arasında en zengin 44 ülke arasında hiç savaş yaşanmamıştır (Naisbitt ve Aburdene, 2000, s.29).

TASNİF DIŐI

Devlet tarafından korunan deęerler arasında; barıő, özgürlük, haklar, güvenlik; yaőam kalitesi, ulusal birlik, saęlıklı çevre, enerji istikrarı, ekonomik ve sosyal zenginlik; bilgi kaynakları; yasal düzen ve hukukun egemenlięi; bütünlük; siyasi baęımsızlık ile ülkenin bekası gelmektedir. Ulusal çıkarlarla ilgili referans noktaları bu deęerlerin taşıdığı işlevlerin içinde bulunmaktadır (Mijalkovic ve Milosevic, 2011, s.438). Ulusal güvenlik kısaca “bir devletin ulusal çıkarlarının iç ve dış tehditlere karşı korunması ve kollanması” şeklinde ifade edilmektedir. Ulusal çıkarlar, tehdit ve tehdiye karşı önlem alma da ulusal güvenlięin unsurları olarak kabul edilmektedir. (Yılmaz, 2007, s.214).

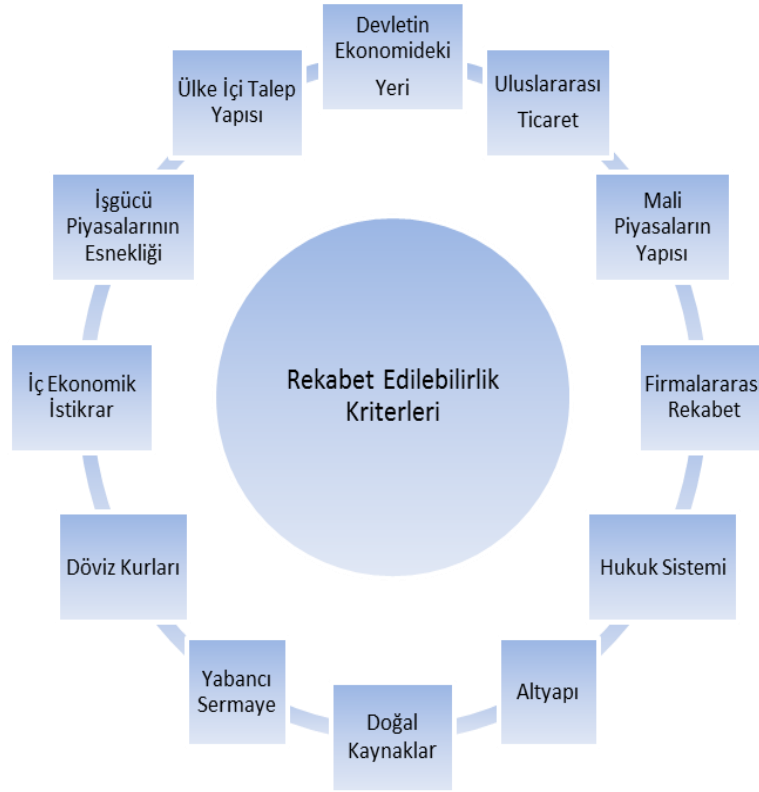
Ulusal çıkar, kısaca ulusu oluşturan bireylerin ortak menfaati olarak tanımlanabilir. Ancak bireysel çıkarların toplamından daha fazlasını ifade eder. Ulusal çıkarları mikro ve makro seviye olmak üzere iki grupta incelemek mümkündür. Mikro seviyedeki ulusal çıkarlarda vatandaşların çalışma yeteneklerini, yaratıcılıklarını, ekonomik ve teknolojik kabiliyetlerini geliőtirmek; ihtiyaç ve isteklerini genişletmek; refah düzeylerini artırarak ihtiyaç ve isteklerini karşılamak yer almaktadır. Makro seviyede ulusal çıkarlar ise devlet açısından deęerlendirilmektedir. Ülkenin ve fiziksel idamesinin korunması, baęımsızlıęı, coęrafi bütünlüęü, vatandaşlarının refahı ve kolektif güvenleri makro seviyede ele alınmaktadır. Bu kavramlar bir arada deęerlendirilecek olursa ulusal çıkarlar açısından sadece baęımsız ve ulusal bir devlet kendi vatandaşlarının üretkenlięini ve yaratıcılıęını geliőtirebilir, yeni ihtiyaçlar oluşturarak bunları tatmin edebilir (Stiblar, 2005, s. 9-10).

Günümüzde ekonomik göstergeler toplumun ortak dili haline gelirken para da nesnel iletişimin temel enstrümanı haline gelmiştir (Demir, 2003, s.7). Yaőanan tecrübeler ekonomik anlamda karşılaşılan problemlerin ulusların ekonomik çıkarlarını sekteye uğrattıęını göstermiştir. Örneęin 1973 yılında OPEC ülkelerinin uygulamıő olduęu ambargo ekonomisi zayıf ülkelerde kaosa neden olmuştur (Ekonomik Güvenlik, 2003, s.34). Bu nedenle ülkeler ekonomik çıkarlarının korunmasına son derece önem vermektedirler.

Ekonomik güvenlik, ekonomik potansiyelin fiziksel tehditlerden korunduęu ve ekonomik istikrar ve baęımsızlıęa yönelik tehditlerin bulunmadıęı bir ortamı ifade eder (Mijalkovic ve Milosevic, 2011, s.441). Ülkenin bekası ve vatandaşlarının refahını tehlikeye düşürmeden ekonomik faaliyetlerin devam ettięi, kriz ve tehditlerin bulunmadıęı ya da etkisiz kaldıęı, saęlam temellere dayanan iktisadi senteze de ekonomik güvenlik denilmektedir (Ekonomik Güvenlik, 2003, s.5).

TASNİF DIŞI

Ekonomik güvenliğe tesir eden hususların başında; endüstriyel üretim miktarı, teknolojik alt yapısı, enflasyon oranı, dış ticaret hacmi, reel döviz kuru, döviz rezervlerinin seviyesi, doğrudan yabancı yatırımların miktarı ve dış borç göstergeleri gelmektedir (Ekonomik Güvenlik, 2003, s.186-188). Bunlar aynı zamanda ülkenin uluslararası ortamda ekonomik açıdan rekabet gücünü belirleyen etkenlerdir (Şekil-4).



Şekil-4: Uluslararası Rekabet Gücünü Belirleyen Etkenler

(Kaynak: Pfeffer, J.(1995). *Rekabette Üstünlüğün Sırrı: İnsan*. İstanbul: Sabah Yayıncılık. s. 3'den alınarak düzenlendi)

Ekonomik güvenliğin değer kazanması sadece klasik merkantilizme bir dönüş değildir. Aynı zamanda küresel liberalizasyonun getirdiği pek çok tehlikeye karşı da bir tepkidir. Bu tehlikeler arasında; kaybetme riski, mali istikrarsızlık, kaynak israfı, uyuşturucu ve silah kaçakçılığı gibi hususlar yer almaktadır. Küresel ekonominin, çevre konularına, bağımsızlığa, istikrara ve askeri açıdan yeterliliğe olan etkisi de ekonomik güvenliği öne çıkaran nedenler arasındadır (Buzan, 1997, s.25).

Topyekûn bir savaş ihtimalinin ortadan kalkmasıyla birlikte küreselleşmenin yarattığı değişim de ekonomik güvenliğe olan ilginin artmasına neden olmuştur. Küreselleşmeyle birlikte ulus devletlerin ekonomileri üzerindeki hâkimiyetin azalması

TASNİF DIŞI

sonucu devletler; hammadde, sermaye, ürün, teknik bilgi vb. giriş çıkışları tam anlamıyla kontrol altına alamamaktadır. Örnek vermek gerekirse hiçbir devletin tek başına, G-7 ülkelerinin merkez bankalarının toplam rezervlerinin neredeyse altı yedi katına yakın miktardaki elektronik para alışverişlerini denetleme imkânı bulunmamaktadır. 1999 yılında 300-350 milyar dolarlık rezerv bulunmasına rağmen günlük ticari işlem 2 trilyon doları bulmaktaydı (Gallino, 2007, s.28).

Ekonomik her faaliyeti etkileyen; insan kaynakları, doğal kaynaklar ve enerji, teknoloji, endüstri, ekonomik karar yapısı, dış ticaret, tarım vb. bütün unsurların maddi ve manevi çıktıları ekonomik güç olarak tanımlanmaktadır (Ekonomik Güvenlik, 2003, s.40-41). Askeri gücün yanında ekonomik güç de ulusal güvenliğin önemli bir parçasıdır ve uluslararası ortamda ülkenin rolüne göre ekonomik güç rahatlıkla askeri güce dönüştürülebilir. Zira silahlar için mali kaynaklar gerekirken, sivil imalat sektörü savunma sanayiye desteklemek için dönüştürülebilir. Bununla birlikte ekonomik güç tek başına askeri güç yerine savunma ya da saldırı maksadıyla da kullanılabilir. Ekonomik savaşlar, abluka, yaptırımlar doğrudan rakip devletin ekonomisini dolaylı olarak da askeri gücünü çökertmek için kullanılabilir. Ekonomik güç ulusal güvenliğin sağlanmasında büyük katkıda bulunur. Bu yüzden ulusal güvenliğin sağlanmasında “yüksek güvenlik meselesi” olarak kabul edilmektedir (Mijalkovic ve Milosevic, 2011, s.439).

Sanayinin dünya ticareti içerisindeki payı 1973 yılında %60,5 iken bu oran 1999 yılında %76,5'e yükselmiştir (Nebioğlu, 2001, s.3). Teknolojik yenilik ve ARGE faaliyetleri sadece şirketlerin değil ülkelerin kalkınmasında da önemli rol oynamaktadır. Küresel rekabet ortamında bilgi;

- Laboratuvarlar ve endüstri tarafından yürütülen ARGE çalışmaları,
- Lisans anlaşmaları,
- Teknik eleman transferi,
- Başka bir firmanın satın alınması ve ortaklıklar kurulması,
- Endüstriyel casusluk, gibi yasal veya yasal olmayan yollarla da elde edilebilmektedir (Ekonomik Güvenlik, 2003, s.174).

Küresel rekabetin tırmanması devletlere ait istihbarat kuruluşlarının da ekonomik ve teknolojik istihbarata daha çok önem vermelerine neden olmuştur. Görüntü alma, izleme, iletişimin dinlenmesi amacıyla kullanılan uydular sadece askeri maksatlarla değil ekonomik mücadele açısından da önemli hale gelmiştir (A. Toffler ve H. Toffler, 1994, s.98). Günümüzde yeni güvenlik ortamının gereği olarak askeri yöntemlerin dışında ulusal çıkarları elde etme ihtiyacı, çeşitli istihbarat

TASNİF DIŐI

fonksiyonları ile desteklenen yeni ulusal güvenlik politika anlayışlarının doğmasına yol açmıştır (Yılmaz, 2007, s.216). Ulusal güvenliğin her boyutta sağlanmasında istihbarat kritik rol oynamaktadır. Ünlü Çin düşünürü Sun Tzu;

“Büyük bir askeri harekât ulusun omuzunda ağır bir yükür. Bir günlük zafer için yıllarca savaşılr. Bu yüzden casuslara (muhabirlere) ödöl vermekten kaçınmanın sonucunda düşman saflarından haberdar olmamak gerçek bir komutana devlet adamına yakışmaz. Akıllı bir liderin rakiplerini yenip başarı kazanmasında neden istihbarattır (ön bilgidir) ”, demektedir (Sun Tzu, 1996, s.196)

Soğuk Savaş boyunca istihbarat ve karşı istihbarat faaliyetleri askeri ve politik alana yönelmişti. Örneğin 1985 yılında CIA bilgi kaynaklarının isimlerini 4,6 milyon dolar karşılığında KGB'ye satan ve idam edilen CIA görevlisi Aldrich Ames bu dönemin istihbarat anlayışına örnek gösterilebilir. Ancak Soğuk Savaş'ın sona ermesiyle birlikte ekonomik güvenlik ve ekonomik çıkar yaklaşımının ön plana çıkması istihbarat faaliyetlerinin de bu alana yoğunlaşmasına neden olmuştur. Ekonomik üstünlük askeri üstünlük kadar önemli olmuş bu durum da istihbarat örgütlerinin kendilerini yeniden şekillendirmelerine yol açmıştır (Nasheri, 2005, s.19).

Gelişmiş ülkeler ekonomik güvenliklerini devletin önemli ilgi sahalarından biri olarak görmektedir. Amerikan Ulusal Güvenlik Konseyi tarafından yayınlanan strateji belgelerinde ekonomik güvenlik istihbarat örgütlerinin ilgi sahalarında yer almaktadır. Yine İngiliz istihbarat servislerinin ilgi alanlarında da ekonomik çıkarlar yer almaktadır (Aydın, 2009, s.39).

ç. Ekonomik İstihbarat

CIA'nın 1995 yılında çıkardığı Tüketicinin İstihbarat Kılavuzuna göre ekonomik istihbarat; yabancı ekonomik kaynakları, aktiviteleri ile mal ve hizmetlerin üretim, dağıtım, tüketim politikalarına ve finans, vergilendirme, ticaret gibi uluslararası ekonomik sistemin diğer unsurlarına yönelik yapılan istihbarattır. (Greory, 1997).

Aydın (2009, s.40)'a göre ekonomik istihbarat; *“politik veya ticaretle ilgili teknolojik veri, finansal, ticari ve hükümet bilgilerini içeren, yabancı meraklar tarafından toplanan, ülkeye direkt veya endirekt olarak verimli veya rekabetçi destek sağlayabilecek ekonomi bilgisinin edinilmesidir.”*

İstihbarat örgütlerinin ve teknolojik yeniliklerin ekonomik istihbarat alanında kullanılması yeni olmakla birlikte hedef ülkenin ekonomik yapısı hakkında bilgi toplamak ve buna göre ticaret ve savaş yapmak oldukça eskidir. Tarım çağında

TASNİF DIŞI

askeri hedefleri verimli topraklar oluştururken sanayi çağının hedeflerini zengin hammaddelerin ve yer altı kaynaklarının bulunduğu bölgeler olmuştur. Örneğin 1916 yılında Fransa'da oluşturulan Duplex Komitesinde savaşın nedeni ve bölgenin zenginlikleri şu şekilde sıralanmıştı:

“ Kilikya, Suriye, Filistin, Kürt Bölgesi ve Musul bize hemen şunları sağlayacaktır.

Buğday: Yılda 115 milyon kental¹⁵.

Petrol: Başka hiçbir yerde bulamadığımız ve yarın onsuz büyük bir millet olunamayacak olan petrol... Petrolsüz ne ordu ne deniz kuvveti mümkündür.

Pamuk ve yün: İşletmelerimiz bu maddeleri büyük güçlük ve korkunç fiyatlarla İngiltere ve Amerika'dan alabiliyor.” (Avar, 2012, s.75).

İstihbaratın bilgi çağındaki hedefinde ise ekonomik değeri yüksek olan fikri mülkiyet ve ticari sırlar yer almaktadır. Örneğin, Fransa 1995 yılının Şubat ayında beş CIA görevlisinin ekonomik ve politik sırları çalması nedeniyle ülkeyi terk etmelerini istedi. ABD Büyükelçisini çağıran Fransız Dışişleri Bakanı, Fransız yetkililerini hedef alan gizli operasyonlarda görev alan bazı CIA görevlilerin de yeniden çağrılmalarını istedi. CIA tarafından hedef alınan görevliler Fransa'nın müzakere stratejilerinin de bulunduğu haberleşme sistemine erişim yetkisine sahip kişilerdi. Fransa, ticari ve teknolojik sırları ele geçirmek için CIA görevlilerinin iki hükümet görevlisine rüşvet vermeye çalışmakla suçlamıştır. Bir başka olayda da Fransa Başbakanı Edouard Balladur'un danışmanlarından Henry Plagnol'a CIA tarafından, Fransa'nın GATT görüşmelerinde takınacağı tutumu bildirmesi karşılığında görüşme başına 500 franklık ödeme yapıldığı iddia edilmektedir (Nasheri, 2005, s.21).

Ekonomik istihbarat hem saldırı hem de savunma maksatlı kullanılabilir. Makro seviyede ekonomik istihbaratı uygulayan bir devlet gizli yollardan elde ettiği ekonomik istihbarat ile faiz oranlarını ne zaman artırıp azaltması gerektiğine ve çekişmeli ticari görüşmelerde nasıl pozisyon alması gerektiği bilgisini karar vericilerine sunabilir. Gizli ve açık kaynaklardan elde edilen ekonomik veriler ile gelişmekte olan pazarlar önceden tespit edilebilir. Diğer yandan ülke içinde üretilen ticari sırların korunmasına yönelik karşı istihbarat tedbirleri için de ekonomik istihbarattan faydalanılabilir (Gregory, 1997). Örneğin 1980'lerin başında ABD istihbarat örgütlerinin Dünya Bankası ve çeşitli finans kuruluşlarına yerleştirdiği “böcek” yazılımlar ile bazı Latin Amerika bankalarının batacağı bilgisini karar

¹⁵ 100 kg.lık ağırlık ölçü birimi.

TASNİF DIŐI

alıcılarına önceden ilettiđi ifade edilmektedir. O dönemde bu bankaların temerrüde düşme potansiyeli ABD ekonomi politikaları açısından büyük önem taşıyordu (Porteous, 1995).

Ulusal ekonomik istihbarat sisteminde edilen bilgiler o ülkenin çeşitli kurumları ve organizasyonları arasında geliştirilmekte ve paylaşılmaktadır. Devlet kurumlarından, yerel yetkililere, işletmelere, eğitim kurumlarına, uzman kuruluşlardan ticari birliklere kadar pek çok organizasyon değişik seviyelerde o ülkenin ekonomik istihbarat yapılanmasında yer almaktadır. Ulusal ekonomik istihbarat sisteminin üç hedefi bulunmaktadır:

- Ülkede bulunan farklı ekonomik kurumların yorum ve kavrayış yeteneklerini geliştirmek,
- Küreselleşmenin yarattığı tehditlere karşı, paylaşılan bilgi temelli eşgüdümlü eylemler üretmek,
- Uluslararası pazarda ülkenin ekonomik ve sosyal gelişimini etkileyecek etkili stratejiler uygulamak (Clerc, 1997, s.309-310).

Hedef ülkenin genel ekonomik durumu, tarım, sanayi, ticaret, finans yapısı, yer altı zenginlikleri, para politikaları, stok durumu vb. hususlar ekonomik istihbaratın hedefini oluşturmaktadır. Tarımsal konularda bir ulusun zirai ve hayvansal üretimlerinin çeşitliliđi ve yeterliđi konusunda bilgi toplanırken, sanayi alanında ekonomik istihbaratın yöneltildiđi faaliyet alanları arasında sanayi kapasitesi, teknolojik gelişmişlik gibi bilgilerin elde edilmesine çalışılmaktadır. Ticari alanda ise ticaretin hacmi, niteliđi dünya pazarlarındaki işlem durumu gibi kriterler göz önüne alınmaktadır. Stratejik maddeler ve stok durumuna yönelik olarak barış ve seferberlik stokları, miktarları, nerelerde depolandığı gibi bilgiler yine ekonomik istihbaratın yöneltildiđi konular arasındadır (Özdağ, 2009, s.93).

Ekonomik istihbarat örtülü ve gizli faaliyetlerle elde edileceđi gibi açık kaynaklardan da sağlanabilmektedir. Örneđin II. Dünya Savaşı sırasında Japonya'nın en büyük gübre tedarikçisi Cezayir ve Fas'ın işgal edilmesine rağmen Japonya'nın tarımsal üretimde sıkıntı yaşamadığını gözlemleyen ABD'li yetkililer aradıkları sorunun cevabını bir ansiklopediden bulmuşlardır. Ansiklopedide, Pasifik'te bulunan Nturu adasında fosfat bulunduğu bilgisinden yola çıkan uzmanlar bu adanın bombalanmasını önermiş sonuç olarak Japon tarım üretimi büyük darbe almıştır (Yakın, 1969, s.25).

TASNİF DIŞI

Özdağ'a göre ekonomik istihbarat, "bir ülkenin açık olarak ortaya koyduğu veya gizli bir şekilde izlediği politikayı analiz etmede kullanılacak en etkili araştırma mekanizmalarından biridir." (Özdağ, 2009, s.93). ABD Başkanı Bill Clinton döneminde ulusal güvenlik stratejisi ile ilgili yayınlanan bir belgede:

"Amerikan çıkarlarına ve ekonomik güvenliğine yönelik tehlikeleri öngörebilmek için istihbarat örgütleri; çıkarların bulunduğu ve açık kaynak istihbaratının yetersiz kaldığı politik, ekonomik, sosyal ve askeri gelişmeleri takip etmelidir. Ekonomik istihbarat, karar alıcıların ekonomideki yönelimleri anlamaları konusunda önemli rol oynayacaktır. Ekonomik istihbarat, Amerikan ticari müzakerecilerini destekleyebilir ve Amerikan şirketlerinin yabancı istihbarat örgütlerince maruz kalabileceği tehditleri ve haksız ticari uygulamaları açığa çıkarmada yardımcı olabilir" denilmektedir (The White House, 1994, s.14).

Ekonomik istihbarat konusunda sadece gizli servislerin değil çeşitli kurumların da hizmet verdiği görülmektedir. Örneğin ABD Ticaret Bakanlığı bünyesinde kurulan "Advocacy Centre" adlı birimin çalıştırdığı uzmanları vasıtasıyla, Amerikan şirketlerinin dünya genelinde almaya çalıştığı binlerce dev projeyi dakika dakika izlediği ifade edilmektedir. Anılan birim aynı zamanda diğer rakiplerin ilerlemelerini de takip etmektedir. 1995 yılında Fransa da, "Ekonomik Rekabet ve Güvenlik Komisyonu" adı altında benzer bir örgüt kurduğunu açıklamıştır. Fransa Başbakanı'nın başkanlığında toplanacak komisyon, ekonomik sırları korumak, Fransız şirketleri ve hükümetine ticari strateji konusunda tavsiyelerde bulunmak maksadıyla, gerekli bilgilerin araştırılmasını, analizini, işlenmesini ve dağıtımını yapacaktır (Porteous, 1995). Aydın (2009, s. 49)'a göre Türkiye'de ekonomik istihbarata yönelik *"karşı koyma faaliyetlerinde görevli bir kurum olmadığı gibi karşı faaliyetlerin nasıl yapılacağı da belirlenmemiştir. Genelde anlaşılan ülke aleyhine faaliyet gösterenlerin bertaraf edilmesi ya da cezalandırılmasından ibarettir."*

Ekonomik istihbaratın elde edilmesinde üç ana kaynaktan faydalanılmaktadır. İlk kaynak, resmi istatistiklerden, gazetelere, radyo yayınlarına hatta IMF ülke raporlarına uzanan herkesin kolaylıkla elde edebileceği açık kaynaklardır. İkinci sırada ise elçilik, konsolosluk ve ataşeliklerin gönderdiği, ekonomi, hazine ve dış ticaret uzmanlarınca değerlendirilen raporlar ve mesajlar yer almaktadır. Üçüncü tip kaynaklar ise hedef ülkenin bilgisi ve rızası olmaksızın uydu teknolojileri gibi sistemler ya da casus kullanarak gizli yollardan elde edilen bilgiler yer almaktadır (Manning, 2012). Daha önceki konularda da belirtildiği gibi bilgi çağındaki ekonomik istihbarat faaliyetlerinin hedeflerini fikri mülkiyet ve ticari sırlar oluşturmaktadır. Bu doğrultuda devletler ve şirketler ekonomik değeri olan bu bilgileri elde edebilmek maksadıyla ekonomik/endüstriyel casusluk yöntemlerine sıklıkla başvurumaktadırlar.

2. ENDÜSTRİYEL CASUSLUK

Endüstriyel/ekonomik casusluk, siber suçları da içeren beyaz yakalıların işlediği yeni bir suç dalı olarak tanımlanmaktadır. “Beyaz yakalı suç” terimi ilk defa 1939 yılında Edwin Sutherland tarafından American Sociological Society’de yaptığı konuşmada dile getirilmiştir. Sutherland, terimi “üzerinde çalıştığı konuda yüksek statü ve saygınlık sahibi kişiler tarafından işlenen suç” şeklinde tanımlamıştır. Çoğu beyaz yakalı suçları soruşturmak son derece güçtür. Çünkü failer karmaşık yöntemlerle işledikleri suçları gizleyebilecek yeterli donanımına sahiptirler (Nasheri, 2005, ss. xii-3).

Ticari sır hırsızlığı, beyaz yakalı suçu, endüstriyel casusluk, ekonomik casusluk gibi kavramlarda kullanım açısından ülkeler arasında farklılıklar bulunmaktadır. Saraç (Karahana, Suluk, Saraç ve Nal, 2011, s.403)’a göre “ticari sır” terimi Anglo-Sakson sisteminde kullanılan bir ifadedir. Kapsam olarak da, müşteri bilgileri, üretim yöntemleri, plan ve projeler, sözleşmeler, kimyasal formüller, iş stratejileri, test verileri, hammadde kaynakları, vb. gibi oldukça geniş bir alanı ifade etmektedir. Ana Britannica Ansiklopedisi (Encyclopaedia Britannica, 2012)’ne göre ticari sırların rakiplerden ele geçirilmesi olarak tanımlanan endüstriyel casusluk terimi, ABD hukuk sisteminde “endüstriyel casusluk” ve “ekonomik casusluk” olmak üzere iki başlık altında incelenmektedir. ABD’nin 1996 yılında çıkarmış olduğu Ekonomik Casusluk Kanunu (Economic Espionage Act-EEA)’na göre, yabancı devlet, yabancı ajan (agent) ya da yabancı unsur (instrumentality) yararına ticari sırrı bilerek çalan, ele geçiren, kopyalayanlar para ve hapis cezası ile cezalandırılmaktadırlar. Bu eylemler de “ekonomik casusluk¹⁶” olarak adlandırılmaktadır. Bahse konu “yabancı ajan” kavramı yabancı bir devlet adına çalışanlar (görevli, memur, temsilci vs.) için kullanılmaktadır. Yabancı unsur ise aslında yabancı bir devletin kontrolünde veya yönetiminde bulunan; ajans, büro, kurum, yasal veya ticari organizasyon, firma ve tüzel kişilikleri ifade etmektedir (Reilly, 2009, s.24-25). Aynı kanunda endüstriyel casusluk¹⁷; sahibinden ziyade başka kişinin ekonomik yararına olacak şekilde ticari sırrın ele geçirilmesi ve ticari sır sahibinin bu eylemden zarar görmesi olarak tanımlanmaktadır (Krotoski, 2009, s.5). Ekonomik casusluk ile endüstriyel casusluk arasındaki temel fark, ticari sırrın elde edilmesinde yabancı bir devletin doğrudan ya da dolaylı olarak katkıda bulunmasıdır.

¹⁶Economic Espionage Act, 18 U.S.C § 1831 (1996).

¹⁷Economic Espionage Act, 18 U.S.C § 1832 (1996).

TASNİF DIŞI

ABD ile benzer şekilde Kanada'da yürürlüğe konulan Bilgi Güvenliği Kanunu¹⁸ ile ekonomik casusluk, ticari sırların yabancı bir ekonomik varlık yararına kullanılması olarak nitelendirilmektedir. Buna göre, Kanada'nın ekonomik çıkarlarını zarara uğratan, ticari sırrı yabancı kişi, grup veya organizasyona ileten veya ticari sırrı yok edenler on yıldan fazla olmayacak şekilde hapis cezası ile cezalandırılmaktadırlar (Department of Justice Canada, 2011).

Fransa, Almanya ve diğer sanayileşmiş devletler endüstriyel casusluğu ceza hukukunun meselesi olarak kabul etmektedirler (Nasheri, 2005, s.178). Saraç (2011, s.406)'a göre, Türk ve AB hukuk yapısında Amerikan hukuk sisteminden farklı olarak ticari sırlar, özel bir hukuksal düzenleme bulunmaması sebebiyle fikri mülkiyet olarak kabul görmemektedirler.

(...) ülkemizde çeşitli yasalarda ticari sırlara ilişkin doğrudan ya da dolaylı nitelendirmeler bulunsa da patent veya tasarımlara sağlanan şekilde herkese karşı ileri sürülebilecek bir fikri mülkiyet korumasından bahsedilemez. (...) taraflar arasında herhangi bir sözleşme ilişkisi bulunmaması halinde hukukumuzda ticari sırların korunmasında, haksız rekabete ilişkin hükümlerden yararlanılabilir (Karahan, Suluk, Saraç ve Nal, 2011, s.406).

ABD ve Kanada hukuk sisteminde ticari sırların yabancı devlet yararına kullanılması ekonomik casusluk olarak nitelendirilirken hukukumuzda böyle bir düzenleme bulunmamaktadır. Casuslukla ilgili olarak Türk Ceza Kanunu (TCK)'nın 326-339'uncu maddeleri arasında "Devlet Sırlarına Karşı Suçlar ve Casusluk" suçları sıralanmıştır. Aynı Kanun'un 331'inci maddesinde de "uluslararası casusluk" suçu belirtilmiştir. Buna göre; "*Yabancı bir devletin güvenliği veya iç veya dış siyasal yararları bakımından niteliği itibarıyla gizli kalması gereken bilgileri, diğer bir yabancı devlet lehine siyasal veya askerî casusluk maksadıyla temin eden vatandaşa veya bunu Türkiye'de temin etmiş bulunan yabancıya bir yıldan dört yıla kadar hapis cezası verilir.*" denilmektedir. Yapılan faaliyet ancak "*yabancı devlet lehine siyasal veya askerî casusluk maksadıyla*" yapılırsa uluslararası casusluk olarak işlem görecektir. Ekonomik ya da ticari maksat suçun unsurları arasında sayılmamıştır. Casuslukla ilgili bir diğer suç da "*yasaklanan bilgilerin casusluk maksadıyla temini*" başlığı altında düzenlenmiştir. TCK'nın 335'inci maddesine göre; "*Yetkili makamların kanun ve düzenleyici işlemlere göre açıklanmasını yasakladığı ve niteliği bakımından gizli kalması gereken bilgileri siyasal veya askerî casusluk maksadıyla temin eden kimseye sekiz yıldan oniki yıla kadar hapis cezası verilir*". Burada da (331)'inci madde de olduğu gibi sadece güvenlik odaklı olarak "siyasal ve askeri casusluk maksadı" yer almıştır.

¹⁸Security of Information Act (R.S.C., 1985, c. O-5).

TASNİF DIŞI

Gerek ülkelerin hukuk sistemleri arasında farklılıklar bulunması, gerekse farklı ülkelerdeki olayları tek bir tanım adı altında karmaşıklığa yol açmadan değerlendirebilme açısından ticari sırların yabancı ülke lehine çalınması eylemi bu çalışma içerisinde “endüstriyel casusluk” olarak ifade edilecektir. ABD ve Kanada’nın kullanmış olduğu “ekonomik casusluk” terimi ile çalışma içerisinde kullanmış olduğumuz “endüstriyel casusluk” terimi aynı anlamda kullanılmıştır.

a. Endüstriyel Casusluğun Tarihsel Gelişimi

Endüstriyel/ekonomik casusluğun geçmişi çok eski tarihlere dayanmaktadır. Nasheri (2005, s.18)’ye göre bilinen ilk olay yaklaşık 1500 yıl önce Çinli prensesin yaptığı gezide şapkasının içine sakladığı ipek böceklerini Hintli bir adama vermesiyle gerçekleşmiştir. Bu sayede ipeğin elde edilmesiyle ilgili sır ülke dışına çıkmış oluyordu. Çin de gerçekleşen diğer bir olay da yüksek kaliteli porselenle ilgili sırların yine ülke dışına çıkması ile ilgilidir. 18. yüzyılda porselen fabrikasını ziyarete gelen Fransız Jesuit d’Entrecolles üretim süreci ile ilgili öğrendiği bilgileri kaydederek Fransa’ya göndermiştir.

Amerikalı Francis Cabot Lowell 1811 yılında İskoçya’ya yaptığı gezide, su gücü ile çalışan ve yüksek üretim kapasitesine sahip Cartwright dokuma tezgâhlarına ait gizli planları ülkesine getirmiştir. İngiltere’de Sanayi Devrimi’nin başlamasında çok önemli etkisi olan bu makinaların ülke dışına çıkarılması 1780’lerin sonuna doğru yasaklanmıştı. Fink’e (2002, ss.9-10) göre, Cartwright dokuma tezgâhlarının üretim bilgilerinin ABD’ye gelmesi sadece Sanayi Devriminin başlangıcında etken olmamış aynı zamanda Amerikan İç Savaşı öncesi Kuzey’in refah seviyesini artırması nedeniyle bu savaşta Kuzeylilerin Güneylilere üstün gelmesini de sağlamıştır.

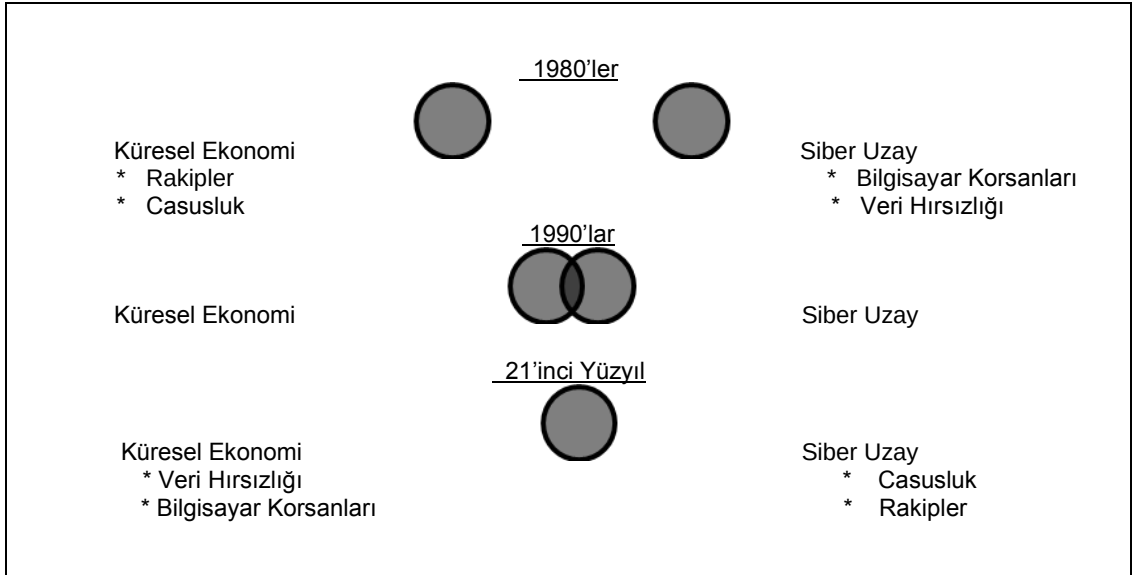
18. ve 19. yüzyıllarda yaşanan Sanayi Devrimi ile birlikte buhar gücünün kullanılmaya başlanması ve yeni buluşların insan hayatına girmesi sonucu devletler de sanayilerini korumaya yönelik tedbirler almaya başlamışlardır. Patent, marka ve tasarım gibi sınai haklar Sanayi Devrimi ile birlikte modern anlamda şekillenmeye başlamıştır (Karahan, Sukuk, Saraç ve Nal, 2011, s.23). Nitekim 1873 yılında Viyana Fuarı’na ülkelerin kendi buluşlarının kopya edileceği kaygısıyla katılmak istememeleri uluslararası ortamda da sınai mülkiyetin korunması gerektiği ihtiyacını ortaya çıkarmış, sonucunda da 20 Mart 1883’te Paris Sözleşmesi imzalanmıştır (Topçu, 2007, s.37).

I. ve II. Dünya Savaşı ile Soğuk Savaş’ın yaşandığı dönemlerde istihbarat faaliyetlerinin doğal olarak askeri ve siyasi alanda yoğunlaştığı görülmektedir. 1995 yılında Ulusal Güvenlik Ajansı (National Security Agency-NSA) tarafından açıklanan

TASNİF DIŞI

VENONA Belgelerinde 1940'lı yıllarda ABD ve İngiliz istihbarat örgütlerinin Sovyet istihbarat örgütünün haberleşmesini çözerek nasıl takip ettikleri anlatılmaktadır. Sovyetler adına ABD'nin nükleer sırlarını temin eden Klaus Fuchs, Theodor Alvin Hall ve Julius Rosenberg gibi isimler çözülen şifreler sayesinde tespit edilebilmişlerdir (Macrakis, 2010, s.379).

Soğuk Savaş süresince istihbarat örgütlerinin hedefinde, rakip devletlerin siyasi koşulları, liderleri, askeri ve ekonomik kapasiteleri, birliklerinin konuşlanma durumu, yeni geliştirdikleri silahların özellikleri vb. gibi güvenlik kaynaklı başlıklar bulunmaktaydı. Berlin Duvarı'nın yıkılışı ve Varşova Paktı'nın çöküşünün ardından askeri üstünlükten ziyade ekonomik üstünlüğün artan önemi devletler arası ilişkilerin de yeni anlamlar kazanmasını sağlamıştır. Bu dönem de küresel ekonomi ve siber uzayın iç içe geçmesi taşıdıkları risk ve tehditlerin de bir araya gelmesine neden olmuştur (Şekil-5).



Şekil-5: Küresel Ekonomi ve Siber Uzayda Risk ve Tehditlerin Birleşimi

(Kaynak:Christopher Burgess, Richard Power. Secret Stolen, Fortunes Lost. Preventing Economic Espionage in the 21st Century. Burlington, Syngress Publishing, 2008, s.xvi)

İnternetin yaygınlaşmasıyla birlikte sınır düşüncesinin ve yargılamanın yeni boyutlar kazanması endüstriyel-ekonomik casuslukla mücadelede sorunlar çıkarmaktadır. Yeni teknolojiler var olan yasalara meydan okumaktadırlar. Suçlular giderek işledikleri suçun etkilerinin görüldüğü yerin uzağında barınır hale gelmişlerdir (Nasheri, 2005, s.1).

Endüstriyel casusluğun pek çok nedeni bulunmaktadır. Samlı ve Jacobs (2008, s. 109-110)'a göre başlıca nedenleri;

TASNİF DIŐI

- Rekabet avantajı sağlamak,
- Know-how çalışması için yeterli zaman ve imkânın bulunmaması,
- Yenilik için yeterli kaynak yokluğu,
- Bilginin gücünün anlaşılması,
- Küreselleşmenin etkisi,
- Ticari sırların gün geçtikçe artan değerinin anlaşılmasıdır.

Siyasi Soğuk Savaş sona ermiş gibi gözükse de ekonomik Soğuk Savaş tüm hızıyla devam etmektedir. Son dönemde endüstriyel casusluğun hedef aldığı alanlara bakıldığında bunların büyük çoğunluğunun ileri teknoloji içeren iş dalları, ilaç şirketleri, üretim firmaları ve hizmet endüstrisi olduğu görülmektedir. Bunun haricinde; havacılık, biyoteknoloji, bilgisayar yazılımı ve donanımı, savunma sanayi, haberleşme, enerji araştırmaları, gizleme teknolojileri, lazerler, üretim süreçleri ve yarı iletkenler de diğer önemli hedefler arasındadır. Sadece ürünle ilgili değil pazarlama verileri de endüstriyel casusluk yolu ile elde edilmek istenmektedir. Müşteri bilgileri, ürün gelişim bilgisi, fiyat bilgileri, pazarlama planları, personel bilgileri, teklif miktarları, üretim maliyet analizleri ve stratejik planlama bilgileri de istihbarat elemanları tarafından toplanan bilgiler arasındadır (Nasheri, 2005, s.4).

b. Endüstriyel Casuslukta Kullanılan Yöntemler

Ticari sır hırsızlığı ya da genel bilinen adıyla ekonomik casusluk genellikle iki şekilde meydana gelmektedir.

- Hoşnutsuz bir çalışanın kendi finansal yararına ya da şirkete zarar vermek için şirkete ait ticari sırları çalması. Örneğin Science Applications Şirketinde proje yöneticisi olan Ronald Hoffmann, 1992 yılında Stratejik Savunma İnisiyatifi bünyesinde gerçekleştirilen gizli bir projeye ait yazılımları 750.000 dolar karşılığında Japon çok uluslu şirketlere (Nissan, Mitsubishi, Ishikawajima-Harima) satmaktan dolayı yakalanmıştır (Schweizer, 1996, s.9). Diğer bir örnek de Gillette firmasına ait ticari sırların Steven L. Davis isimli çalışanınca rakip, Warner-Lambert, Bic ve American Safety Razor şirketlerine verilmesi olayıdır¹⁹. Gillette Şirketi'nin "Mach 3" traş bıçağı projesi için Wright Industries firmasında tasarım mühendisi olarak görev yapan Davis, Gilette'nin isteği üzerine projeden uzaklaştırılmıştı. Davis de projeden çıkarılmadan hemen önce tasarımları, sistem çizimlerini ve ticari sır içeren verileri

¹⁹ United States of America v. Steven Louis Davis, Criminal No. 97-00124 (M.D. Tenn. 1997).

TASNİF DIŐI

diz üstü bilgisayarına kaydederek, belgegeçer ve e-posta yolu ile rakip şirketlere gönderdi. Bu şirketlerden hiçbir şekilde para isteğinde bulunmayan Steven L. Davis yapılan sorgusunda, niyetinin para kazanmak olmadığını ancak işini kaybetme korkusuyla şirketten intikam almak ve zarar vermek için ticari sırları rakip firmalara gönderdiğini belirtmiştir (Fink, 2002, s.82-83).

- Rakip şirketlerin veya yabancı bir devletin kendi ekonomik çıkarları için hedef şirkete ait ticari sırları ele geçirmesi. Konu ile ilgili örnek olarak Japonya'daki Rus Ticaret Temsilciliğinde görevli Vladimir Saveliev tarafından Toshiba Firmasına ait ticari sırların elde edilmesi gösterilebilir. Yetkililer, kimliği açıklanmayan Toshiba personelinin 1 milyon yen (yaklaşık 9 bin dolar) karşılığında Saveliev'e yarı iletkenlerle ilgili bilgiler verdiğini, bu bilgilerin de füze güdümlü sistemleri, denizaltılar ve radarlar için kullanılabileceğini belirtmektedirler. Japon Hükümeti olayın açığa çıkmasından önce ülkeden ayrılan Saveliev'i "istenmeyen adam" (persona non grata) ilan etmiştir (The Japan Times Online, 2005).

Ticari sırları ele geçirmek maksadı ile pek çok yöntem kullanılmaktadır. Bazen tek başına bazen de bir arada kullanılan bu yöntemler zaman içerisinde de değişim göstermektedirler. İnternet üzerinden yapılan endüstriyel casusluk faaliyetleri ayrı başlık altında değerlendirilecektir. Siber alan dışında endüstriyel casuslukta kullanılan temel yöntemlerin bazıları şunlardır:

- Ticari bilgiler için yapılan beklenmedik istekler.
- İş ziyareti boyunca karşılaşılan sıra dışı olaylar.
- Şüpheli iş teklifleri.
- Uluslararası sergi, seminer ve toplantıların kullanılması.
- Ortak girişim ve araştırmaların istismar edilmesi.
- Şirketlerin veya teknolojinin satın alınması.
- Eski çalışanların kullanılması.
- Kültürel benzerliklerin kullanılması (CSIS, 2011).
- Çöp Karıştırma

TASNİF DIŞI

- Sızdırma (Toplum Mühendisliği) (Samlı ve Jacobs, 2003, s.102)

CSIS yukarıdaki faaliyetlerin ekonomik casusluğun göstergeleri olarak kabul edilebileceğini, ancak yabancı bir ülkenin müdahalesi olduğu anlamına gelmeseler bile bir işaret olarak değerlendirilebileceğini belirtmektedir (CSIS, 2011).

(1) Ticari Bilgiler İçin Yapılan Beklenmedik İstekler

Amerikan Savunma Güvenlik Servisi (Defense Security Service-DIS)'ne göre 2000 yılında bilgi toplandığı şüphesiyle yapılan şikâyetlerin %41'ini bu tarz istekler oluşturmaktadır (ONCIX, 2001, s.1). Yapılan istekler şirketlerin pazarlama bölümlerinden ziyade, kişiler tarafından telefon, elektronik posta veya belgegeçer üzerinden yapılmaktadır. Sıklıkla internet üzerinden yapılan istekler anket veya araştırma hakkında sorular içerebilir. Pazarlama anketleri hassas teknolojik ve ticari bilgileri açığa çıkarabilir. Bu yöntemde bilginin son kullanıcısının kim olduğu ve anketi kimin sonuçlandıracağını öğrenmek son derece önemlidir. İnternet kullanımındaki artışla birlikte şirketlerin ana sayfalarına, ilan sayfalarına ulaşan yabancı istihbarat unsurları toplama çalışmaları için önemli veriler elde edebilirler.

Belirtileri:

- İnternet adresinin yabancı bir ülkeye kayıtlı olması.
- Anket isteğinde bulunan kişilere ulaşılamaması.
- Hakkında bilgi isteğinde bulunulan teknolojinin; gizli, gümrük kontrollü veya hem ticari hem de askeri alanda kullanılabilir olması.
- Anket\araştırma isteğinde bulunan kişinin kendini öğrenci veya danışman olarak tanıtmaması.
- Anket isteğinde bulunan kişinin, işverenin yabancı bir hükümet olduğunu, ya da işin yabancı bir hükümet veya programı için yapıldığını söylemesi.
- Savunma ile ilgili program, proje veya sözleşmeler hakkında sorular sorulması.
- Soru soran kişinin istediği bilginin gizli veya kontrol altında olduğuna dair bilgi sahibi olması (CSIS, 2011).

(2) İő Ziyaretinde Karőılaőılan Sıra Dıőı Olaylar

İő ziyaretine gelen kiőiler tarafından yapılan beklenmedik davranıőlar da őüphe ile yaklaőılması gereken durumlar arasındadır. Tesise gelen ziyaretçinin, bilgi toplama faaliyeti dođrultusunda gezi güzergâhını deđiőtirmeye çalışması ya da konu dıőında ısrarlı sorular sorması gibi durumlar karőılaőılan olaylar arasındadır (NCC, 1997, s.12)

Belirtileri:

- Tesis içinde refakatçisiz, görüntü veya ses kaydı yapan ziyaretçiler.
- Ziyaretin görünen amacın dıőında başka bir gündeminin olması. Gelen ziyaretçinin konusunun haricinde belirli konular üzerine yoğunlaőarak detaylı sorular sorması.
- Son anda sürpriz kiőilerin ziyarete katılması.
- Getirilen ziyaretçinin öneminin ve sahip olduđu teknik bilginin saklanmak istenmesi.
- Ziyaret için farklı zamanlarda deđiőik mazeretlerin kullanılması (ONCIX, 2001, s.2).

(3) őüpheli İő Teklifleri

Yabancı bilimadamları ve mühendisler, araştırma tesisleri, akademik enstitüler ve savunma sanayinde hizmet etmek için teklifte bulunabilirler. Bu durum hedeflenen bilgiye erişmek için tesis içine adam sokmak maksadıyla istihbarat örgütleri tarafından istismar edilebilir bir durum yaratmaktadır.

Belirtileri:

- Başvuruda bulunan kiőinin bilimsel uzmanlık alanı ülkesinin konu ile ilgili büyük yatırımlar yapmayı planladıđı bir alanda olabilir.
- İő teklifinde ücret istenmeyeceđinin beyan edilmesi.
- Yabancı stajyerlerin (yüksek lisans veya doktora öğrencileri) proje uzmanının yanında belirli bir süre ücretsiz çalışmak istemeleri

TASNİF DIŞI

- Yabancı bilimadaminin yer almak istediği araştırmadaki teknolojik bilginin niteliğin ticari sır, gizli veya gümrük kontrollü olması (CSIS, 2011).

(4) Uluslararası Sergi, Seminer ve Toplantıları Kullanma

Uluslararası sergi, seminer ve toplantılar uzman personelin katılımıyla birlikte bilgi teknoloji ve tecrübe aktarımı konusunda son derece faydalıdır. Ancak dinleyici olarak gelen bilim adamları ve uzmanlar bilgi toplama konusunda istihbarat görevlilerinden bile daha fazla tehdit yaratmaktadırlar. Uzman kişiler alanları ile ilgili konularda sordukları sorularla daha önemli bilgilere ulaşabilirler. Konferans vermek üzere çağrılıp da içinde bulunduğu ortamdan kuşku duymayan katılımcılar, meslektaşları ile yaptıkları tartışmalarda paylaştıkları bilginin önemini göz ardı ederek hassas ve gizli bilgileri ifşa edebilirler. Bunların haricinde yabancı bir ülkeye giden bilim adamı ve uzmanların havaalanlarında çantalarının araştırılması, bilgisayarlarındaki bilgilerin kaydedilmesi, kaldıkları odalara dinleme cihazı yerleştirilmesi, normal güvenlik önlemlerinin ötesinde sorulara muhatap olmaları da karşılaşılan olaylar arasındadır (ONCIX, 2003, s.6). Örnek vermek gerekirse, 1992 yılında Fransız İstihbarat Örgütü DGSE'nin (Direction Générale de la Sécurité Extérieure-Dış Güvenlik Genel Müdürlüğü), Air France Havayollarına ait uçakların birinci sınıf kabinlerine yerleştirdiği dinleme cihazları ile seyahat eden Amerikalı iş adamlarını dinlediği ortaya çıkmıştır. İş adamlarının kaldığı otel odaları da dinleme yapılan yerler arasındadır. Fransızların uygulamış olduğu bu tarz operasyonlara karşı CIA, 1993 yılında Paris Hava Gösterine (Paris Air Show) katılacak şirketleri, Fransızların ticari sırları çalma ihtimaline karşı uyarmıştır (Nasheri, 2005, s. 16).

Belirtileri:

- Seminer veya toplantı konusunun gizli ya da ticari sırları barındıran teknolojilerle ilgili olması.
- Yabancı bir ülkede konferans ya da ders vermek üzere yapılan davette masrafların tümünün karşılanmış olması.
- Sunum özetinin toplantıdan oldukça erken bir tarihte istenmesi.
- Şüpheli fotoğraf ve görüntü alma tekniklerinin bulunması.
- Yanlış veya eksik isimlik takan davetlilerin varlığı (CSIS, 2011).

(5) Ortak Giriřim ve Arařtırmaların İstismar Edilmesi

Ortaklařa üretim ve arařtırma anlařmaları yabancılar tarafından hedeflenen ticari sırların ele geçirilmesinde uygun ortamlar yaratmaktadır. Örnek olarak, Toshiba řirketi ortağı Lexar Media'ya ait ticari sırları kullanmaktan dolayı 2005 yılında 465,4 milyon dolar cezaya çarptırılması gösterilebilir. Toshiba ve Lexar Media harici bellek pazarında daha iyi rekabet edebilmek için 1998 yılının Nisan ayında ortaklık kurmuřlardı. Daha sonraları iki řirket arasında yařanan anlařmazlık sonucunda kendisine ait ticari sırların, Toshiba'nın üretim bandında bulunan NAND çipleri, Compact Flash, xD-Picture ve Secure Digital kartlarında kullanıldığını iddia eden Lexar, davayı kazanan taraf olmuřtur (Burgess ve Power, 2008, s.25-26).

Belirtileri:

- Teknoloji paylaşımı teklifinin sadece yabancı ortağın yararına olacak řekilde yapılması.
- Yabancı temsilcinin tesis içinde sınırsız dolařım isteğinde bulunması.
- Yabancı temsilcinin řirketin kapalı internet sistemine girmek istemesi.
- Yabancı ortağın proje için gereğinden fazla uzman göndermesi (ONCIX, 2002, s.8).

(6) řirketlerin veya Teknolojinin Satın Alınması

Bir diğeri yöntemde (pahalı olmasına rağmen) hedeflenen teknoloji ya da ticari sırrın ele geçirilmesi maksadıyla řirketlerin veya teknolojinin kısmen ya da tamamen satın alınmasıdır. Alımı gerçekleřtiren řirketlerin diğeri ortakları son derece önemlidir. Gerçekte alımı yapmak isteyenler başka bir řirkete ortak olarak hedefledikleri řirket veya teknolojiye ulařmak istemektedirler. "Üçüncü kiři" olarak adlandırılan bu řirketler genellikle ambargo konulan ya da kontrollü gümrük uygulanan devletlere aittir (ONCIX, 2001, s.2). Örneğinin 1988 yılında Airbus řirketi ile birlikte bazı Fransız řirketleri, Boeing řirketine ait alt yüklenicileri (tařeron) satın almak istemiřlerdir. Eğer satıř gerçekleřmiř olsaydı Airbus, Boeing hakkında; üretim süreçleri, kapasiteleri ve gelecek planları gibi son derece önemli bilgilere sahip olacaktı (Schweiser, 1996, s.5).

TASNİF DIŐI

Belirtileri:

- Alımı gerçekleřtiren řirketin bařka bir yabancı ortaęının bulunması.
- Yeni yabancı ortak tarafından görevlendirilen personelin řirkete ait hassas bilgi ve ticari sırlara bir an evvel ulařmak istemesi (CSIS, 2011).

(7) Eski alıřanların Kullanılması

Hassas bilgilere, ticari sırlara ve gizli programlara önceden erişim imkânına sahip olan eski personel karşı istihbarat konusunda ciddi riskler yaratmaktadırlar. 2002 yılında Silikon Vadisi'ndeki Transmeta, Trident Microsystems, NEC Electronics ve Sun Microsystems'ten elde ettikleri bilgisayar çiplerine ait ticari sırları kullanarak Çin Hükümeti tarafından finanse edildięi öne sürülen Supervision Arařtırma řirketini kuran Fei Ye ve Ming Zhong ekonomik casusluk ile suçlanmışlardır (Richardson ve Luchsinger, 2007, s.43).

Sadece üst düzey yönetici ve mühendisler deęil alt düzeyde alıřan personel de endüstriyel casusluk maksadı ile kullanılmaktadır. Bunlar arasında özellikle ihtiyaç duyulan bilgiye erişebilmeleri nedeniyle sekreterler, bilgisayar operatörleri ve bakım görevlileri sahip oldukları düşük maař ve statülerinden dolayı istihbarat örgütleri tarafından angaje edilebilmektedirler (NCC,1995, s.17).

Belirtileri:

- Eski alıřanın aynı sektör üzerinde faaliyet gösteren yabancı bir řirkette işe başlaması.
- Eski alıřanın önceki řirketi ve alıřanları ile irtibatını sürdürmeye alıřması.
- Personelin aynı sektörde sıra ile hem kendi ülkesinde hem de yurt dışında farklı firmalarda alıřması (CSIS, 2011).

(8) Kültürel Benzerliklerin Kullanılması

Yabancı unsurlar, řirket personelinden bilgi sızdırmak maksadıyla alıřanların kültürel kökenlerini istismar edebilirler. Konu ile ilgili olarak Avery Dennison ve Four Pillars řirketleri arasında yaşanan ticari sır hırsızlıęı örnek olarak verilebilir. Yapıřkan etiketler alanında sahip olduęu formül nedeniyle ABD'nin önde gelen řirketlerinden biri olan Avery Dennison'a ait ticari sırların, 1989-1997 yılları arasında

TASNİF DIŞI

şirketin araştırma bölümünde mühendis olarak çalışan Victor Lee tarafından Tayvan menşeli Four Pillars'a sızdırıldığı tespit edildi. Yapılan soruşturmada, Tayvan'daki Endüstriyel Teknoloji Araştırma Enstitüsü tarafından konferans vermek üzere ülkeye davet edilen Victor Lee'nin, burada kendisiyle irtibata geçen Four Pillars'ın CEO'su Pin Yen Yang'ın "gizli danışman" olması karşılığında yıllık 25.000 dolarlık teklifini kabul ettiği ortaya çıktı. 1989 yılından itibaren Lee'nin Avery Dennison'a ait ticari sırları aktarmasıyla birlikte "gizli danışmanlık" ücreti de Tayvan'da yaşayan akrabalarının hesaplarına yatırıldığı tespit edildi. Yetkililer tarafından yapılan incelemede 150.000 dolardan fazla para aldığı saptanan Victor Lee'nin Avery Dennison'a uğrattığı zararın 30-50 milyon dolar civarında olduğu tahmin edilmektedir (Burgess ve Power, 2008, s.22-23).

Belirtileri:

- Çalışanlara menşe ülkelerine ait elçiliklerden beklenmedik tebrikler ve yazılar gelmesi.
- Konferans verdirmek ya da ödül vermek maksadıyla şirket çalışanlarına menşe ülkeden davetiye gelmesi.
- Aynı etnik kültürel kökene sahip yabancı ziyaretçiler tarafından kaynaşmak adına şirket çalışanına yaklaşımları (CSIS, 2011).

(9) Çöp Karıştırma

Bu yöntemde rakip şirketlere ait çöpler araştırılarak kullanılabilecek bilgiler elde edilmeye çalışılmaktadır. İmha edilmemiş belgeler, raporlar, faturalar, istatistik sonuçları, kredi kartı hesap özetleri vb. her türlü yazılı doküman belirli bir süre zarfında toplanıp bir araya getirildiğinde hedef şirket ya da çalışanlar hakkında önemli bilgiler ortaya koymaktadır. Konu ile ilgili olarak dünyanın önde gelen yazılım şirketlerinden biri olan Oracle'nin, Microsoft'a ait ticari bilgilere ulaşmak için çöp karıştırma yöntemine başvurması gösterilebilir. Oracle Şirketi 27 Haziran 2000 tarihinde, Microsoft'un desteklediği şirketler hakkında araştırma yapmak için Investigative Group International (IGI) adlı özel bir araştırma şirketini kiraladığını açıkladı. Açıklanan rapora göre, IGI çalışanlarından Bianca Lopez 02 Haziran 2000 tarihinde temizlik işlerinden sorumlu çalışanlara çöpleri kendine vermeleri karşılığında 60 dolar teklif eder ancak temizlikçiler kabul etmezler. 06 Haziranda çöpleri almak için tekrar gelen Lopez bu sefer işçiler için 500 şefferi için de 200 dolar

TASNİF DIŞI

teklifte bulunur. İşçilerin üst üste gelen tekliften şüphelenip polise haber vermelerinin ardından da olay açığa çıkar (Hemphill, 2002, s.501-504).

(10) Sızdırma (Toplum Mühendisliği)

Aldatma veya ikna yolu ile hassas bilgilerin elde edilmesi, dolandırıcılar kadar istihbarat görevlileri tarafından da kullanılan yaygın bir metottur. Bu yöntem bilgi güvenliği sektöründe “toplum mühendisliği²⁰ (social engineering)” adıyla da anılmaktadır. Kanaatimizce siyaset bilimine ait olan bu kavram yerine istihbarat terminolojisinde kullanılan “sızdırma” teriminin kullanılması daha doğru olur. Sızdırma, haber kaynağı ile yapılan görüşmede, kaynağa hissettirilmeden istenilen belirli bir bilginin alınmasını sağlayan tekniğe verilen isimdir. Soru sorma tekniklerinin etkisiz kaldığı durumlarda kullanılmaktadır. Son derece dikkatli bir hazırlık dönemi gerektiren, planlı ve sistematik bir süreç olan sızdırma, akıldaki önemli bir amaca yönelik uygulanır. Hedef ise istenilen bilgiye erişim imkânına sahip kişilerdir (FM 2-22.3, 2006, s.9-5).

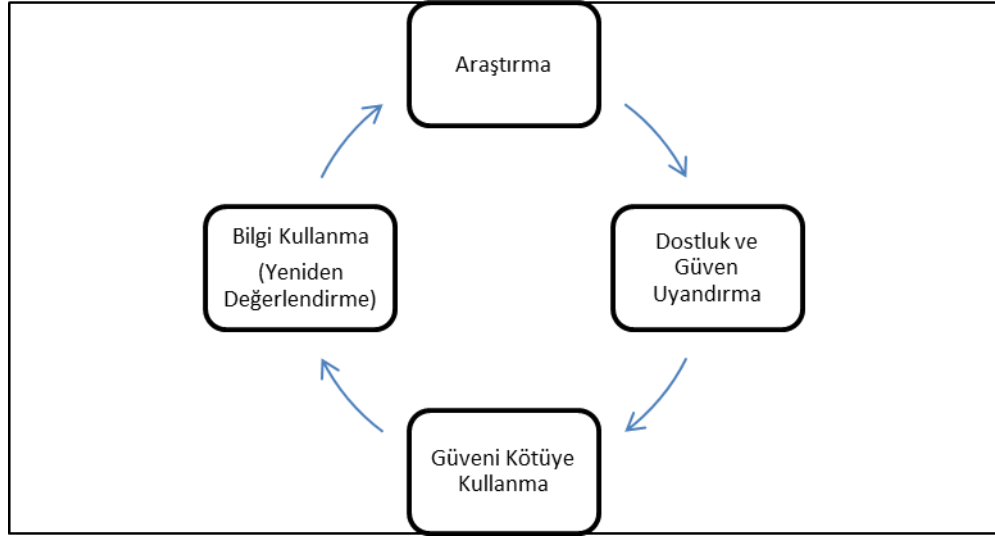
Pek çok karmaşık siber saldırının ilk basamağını sızdırma oluşturmaktadır. Bu yolla şirketlere ait ağların güvenlik duvarları aşılabildiği gibi fikri mülkiyetlerin bulunduğu verilere de erişim imkânı sağlanabilmektedir. Sızdırma yöntemi ile önemli bilgiler elde edilmeden yapılan siber saldırının başarıya ulaşma ihtimali oldukça düşüktür. Sızdırma için yapılan saldırılarda çoğu kez sosyal medya ve ağlarda kişilerin kendileri hakkında verdikleri bilgiler kullanılmaktadır. Öncelikle saldırgan hedefinin ilgi alanlarını, hobilerini, bağlantıda olduğu kişileri öğrenmeye çalışır. Bu yolla yapacağı saldırının ikna gücünü artırır (Symantec, 2011, s.2).

İnsan doğasının zaafılarını kullanmak sızdırmanın temelini oluşturmaktadır. Hangi çalışanın ne kadar bilgi sızdırdığının tespitinin neredeyse imkânsız olması nedeniyle şirketlerin büyük çoğunluğu bu durumdan zarar görmektedir. Aşağıdaki yöntemlerin bazıları sızdırma maksadı ile kullanılmaktadır:

- Zararsız gibi görünen bilgileri istemek.
- Güven duygusu uyandırmak.
- Yardımcı olduğuna inandırmak.
- Yardım istemek.
- Acındırma, sindirme ve suçluluk duygusu uyandırmak (ODTÜ Bilgisayar

Topluluğu Elektronik Dergisi, 2007).

²⁰ Detaylı bilgi için bkz. Mitnick, K.(2009). *Aldatma Sanatı*. Ankara: ODTÜ Yayıncılık ve Long, J. (2008). *No Tech Hacking: A Guide to Social Engineering, Dumpster Diving and Shoulder Surfing*. Burlington: Syngress Publishing.



Şekil-6:Toplum Mühendisliği (Sızdırma) Döngüsü

(Kaynak:Kevin Mitnick. Aldatma Sanatı. Ankara, ODTÜ Yayıncılık, 2009, s.303'deki bilgilerden oluşturulmuştur)

Sızdırma yoluyla hassas bilgilerin elde edilmesi dört aşamalı bir döngüden oluşmaktadır (Şekil 6). İlk aşama olan araştırma safhasında hedef şirket, kurum ya da çalışan hakkında yıllık raporlar, internet sayfası, basın bültenleri vb. açık kaynaklardan işe yarayacağı düşünülen tüm bilgiler toplanır. İkinci aşamada ise hedefle irtibata geçilir ve araştırmadan da elde edilen bilgiler kullanılarak karşı tarafta dostluk ve güven duygusu uyandırılır. Bu doğrultuda sızdırmayı gerçekleştirmek isteyen kişi başka bir kimliğe (kamu görevlisi, çalışan, ortak vs.) bürünebilir. Bir sonraki safhada hedeften bilgi vermesi ya da istenilen amaç doğrultusunda işlem yapması istenerek önceden tesis edilmiş olan güven duygusu istismar edilir. Son olarak arzu edilen bilgiye ulaşıp ulaşılmadığı yeniden değerlendirilir. Başarı sağlanamazsa önceki adımlara yeniden dönülür (Mitnick, 2009, s.303).

Casusluk faaliyetinde bulunanlara bakıldığında bunların geniş bir yelpazede olduğu söylenebilir. Bu konuda en yaygın çalışanlar; rakipler, soruşturma yapanlar, iş istihbaratı danışmanları, basın ve hükümet yetkilileridir. Bazı ülkeler kendileri adına casusluk yapmaları için büyük organizasyonlar ve istihbarat örgütleri yerine kişileri kiralamaktadırlar. Kimi ülkelerse yabancı şirketlere girmek ve şirketlerin ticari sırlarını çalmak için belirli bir grupta anlaşmaktadırlar (Nasheri, 2005, s.7).

c. Bilişim Teknolojileri ve Endüstriyel Casusluk

Son yıllarda bilişim teknolojilerinde yaşanan baş döndürücü gelişmeler bilgi paylaşımını kolaylaştırdığı başkaları gibi tarafından bilinmesi istenmeyen ekonomik değeri olan bilginin elde tutulmasını da zorlaştırmaktadır. Fikri mülkiyetlerden, ticari sırlara, kişisel bilgilerden, banka hesapları, e-ticaret işlemlerine kadar pek çok ekonomik değeri olan bilgi siber uzayda endüstriyel casusluğa hedef olabilmektedir. Günümüzde bir fabrikaya ait bütün planlar, belgeler, üretim sırları gibi binlerce sayfa bilgi avuç içi büyüklüğündeki harici belleklerde rahatlıkla taşınarak çok hızlı bir şekilde kopyalanabilmektedir. Yakın bir gelecekte daha küçük ve farklı şekillerde yeni belleklerin kullanıma gireceğini tahmin etmek çok da zor değildir. Bununu yanında şirketlerin bilgi sistemlerinde ağ yapılarını kullanmaları gizli bilginin farklı kişilere de ulaşmasına neden olmuştur. Küreselleşme ile birlikte yöneticilerin artan yurt dışı seyahatleri ve beraberinde taşıdıkları diz üstü bilgisayar ve harici bellekler endüstriyel casusların işini daha da kolaylaştırmıştır (Temporary Committee, 2001, s.115-116).

Saldırı	Hedef Güvenlik Unsuru	Yöntemler
Yarıda kesme (interruption)	Kullanılabilirlik	- Donanım yıkımı - İletişim hatlarına fiziksel hasar verme - Gürültü yayma - Rota (routing) şaşırtma - Program ve dosya silimi - DoS (hizmet aksattırma) saldırıları
Gizli dinleme (intercept)	Gizlilik	- Gizli dinleme (Eavesdropping) - Hat izleme - Paket yakalama
Değiştirme (modification)	Bütünlük	- Sistemle uzlaşma - Veri tabanı kayıtlarını değiştirme - İletişimde gecikmelerden yararlanma
İmalat veya üretim (fabrication)	Asıllık (authenticity)	- Donanımda değişiklik yapma - Veri tabanına yeni kayıt ekleme - IP kandırma ile yeni ağ paketi ekleme - Sahte e-posta veya bölge adları kullanma

Tablo 11: Güvenlik Unsurlarına Yapılan Saldırıları ve Kullanılan Yöntemler

(Kaynak: Canbek, G. ve Sağiroğlu, Ş. (2007). Bilgisayar Sistemlerine Yapılan Saldırıları ve Türleri: Bir İnceleme. *Erciyes Üniversitesi Fen Bilimleri Enstitüsü Dergisi* 23 (1-2), s.5).

Siber uzayda kullanılan saldırı yöntemleri üçüncü bölümde detaylı olarak anlatılmakla beraber bu teknikler endüstriyel casusluk maksadı ile de kullanılmaktadır. Şirketlerin ve kurumların siber ortamdaki iletişim ve veri tabanlarına yönelik saldırı ve yöntemler Tablo-11’de yer almaktadır.

TASNİF DIŐI

Satış Oranı	Birimler ve Servisler	Tarife Aralığı (dolar)
18%	Banka Hesap Bilgileri	10–1.000
16%	Kredi Kartı Bilgileri (Güvenlik numarası-CVV2 dahil)	0.50–12
6%	E-posta Şifreleri	4–30
5%	Kimlik Bilgileri	0.90–25
5%	Nakit Servisleri	Toplam değerin 8%–50%
4%	Proksi	0.30–20
3%	Sahte hesap	2.50–100/haftalık hizmet;

Tablo-12: Yeraltı Dünyasında Saldırı Çeşitleri ve Fiyatları

(Kaynak: Symantec (2008). Report on the Underground Economy July 07- June 08, s.20. 11 Ocak 2012 tarihinde Symantec Bilgi Portalı: <http://www.symantec.com/business/threatreport/archive.jsp> adresinden alınarak düzenlenmiştir)

Siber uzay bilgisayar korsanları için yasa dışı kazanç kapısı haline de gelmiştir. Yazılım güvenliği şirketi Symantec'in 2008 yılında hazırladığı raporda, özel ve tüzel kişilere ait verilerin elde edilmesinde kullanılan saldırı çeşitlerine ait fiyatlar yer almaktadır (Tablo-12). Yapılan araştırmada banka hesap bilgilerinin satış listesinin ilk sırasında yer aldığı görülmektedir. Bunun en önemli nedeni olarak internet bankacılığının hızla yaygınlaşması sonucu pek çok kişinin ödemelerini, para transferlerini, borsa vb. yatırım işlemlerini ağ üzerinden gerçekleştirmeleri gösterilebilir. Banka hesabının yeri, çeşidi ve hesaptaki paranın kullanılabilirlik durumuna göre bu bilgiler suç dünyasında 10-1000 dolar arasında alıcı bulmaktadır. Kredi kartı bilgileri, güvenlik numarası (CVV2²¹) da dâhil olmak üzere %16'lık oran ile ikinci sırada yer almaktadır. POS²² cihazı ve bankamatikler haricinde kredi kartlarının internet üzerinde e-alışveriş için de kullanılması siber suçlulara istismar edilecek yeni bir alan sunmuştur. Fiyatı 0.5 ile 12 dolar arasında değişen kredi kartı bilgileri, hesabın ait olduğu bölgeye göre değişiklik göstermektedir. Birleşik Arap Emirlikleri, Katar ve Kuveyt gibi ülkelerdeki bilgiler daha yüksek fiyatlara alıcı bulurken ABD bankalarına ait bilgilerin daha düşük olduğu ifade edilmektedir. Diğer bir grupta yer alan e-posta şifreleri 4-30 dolar arasında alıcı bulurken, doğum tarihi, adres, telefon numarası, anne kızlık soyadı vb. kişiye özel kimlik bilgilerinin fiyatı 0,9

²¹ Güvenlik numarası olarak bilinen "Card Verification Value 2"nin kısaltması.

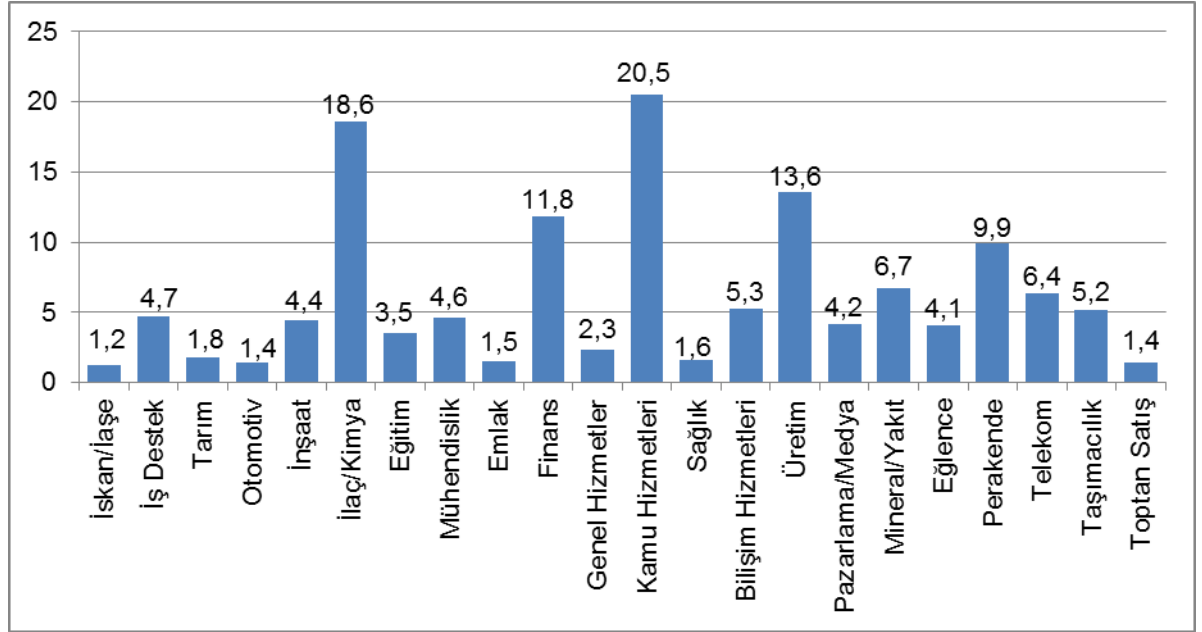
²² Satış noktası anlamına gelen "Point Of Sale"nin kısaltması.

TASNİF DIŞI

ile 25 dolar arasında değişmektedir. Bu bilgiler de çoğunlukla diğer dolandırıcılık türleri için kullanılmaktadır. Yapılan araştırmada nakit hesapları, proksiler ve sahte hesap açma fiyatları da yer almaktadır (Symantec, 2008, s.20-25)

Bilgisayarla ilgili işlenen suçlarda hırsızlık ve dolandırıcılık en hızlı artış gösteren alan olmakla birlikte, bilgisayar korsanları fikri mülkiyet içeren patent, tasarım, pazarlama planları, müşteri bilgileri vb. bilgileri hedef almaktadırlar (Nasheri,2005, s.102). Amerikan Ulusal Karşı İstihbarat İcra Dairesi (Office of National Counterintelligence Executive)'nin 2011 yılında hazırlamış olduğu rapora göre, bilişim sistemlerine yönelik tehditler arasında endüstriyel/ekonomik casusluk da bulunmaktadır ve klasik casusluk yöntemlerinden daha büyük bir tehlike arz etmektedir (ONCIX, 2011, s.i). Örnek vermek gerekirse Rockwell ve Boeing Şirketinde mühendis olarak çalışan ve B-1 bombardıman uçağı, uzay mekiğı vb. gibi önemli projelerde görev alan Dongfan Chung, Çin havacılık sanayiine casusluk yapmaktan dolayı 2010 yılında 15 yıl hapis cezası ile cezalandırılmıştır. Evinde yapılan aramada CD'ye kayıtlı 250.000 sayfalık hassas doküman ele geçirilen Chung'un bu bilgileri 1979-2006 yılları arasında Çin'e gönderdiği tahmin edilmektedir. Basılı olarak bulundurulması halinde oldukça geniş yer kaplayacak bu kadar bilginin CD ortamında kaydedilmiş olması şüphesiz endüstriyel casusluk açısından büyük kolaylıklar sağlamaktadır (ONCIX, 2011, s.2). Benzer şekilde 2009 yılında Starwood şirketi, kendilerine ait lüks W otel zinciri, pazar araştırmaları ve ticari sırları içeren 100.000 belgeyi elektronik ortamda ele geçirdiği iddiasıyla Hilton'a dava açmıştı. Starwood grubuna ait Sheraton, Westin ve Le Meridien otellerinde görev yapan 10 yönetici Hilton tarafından işe alınmıştı. İddiaya göre, Ron Klein ve Amar Lalvani isimli iki eski yönetici kişisel e-posta yolu ile bilgisayarlarına yükledikleri ve maliyeti 1 milyon dolardan daha fazla olduğu değerlendirilen Starwood'a ait ticari sırları, yeni çalıştıkları Hilton'a vermişlerdi. Dava sonucunda Hilton 75 milyon dolar tazminat öderken, Amar ve Klein'e de sektörde iki yıl süreyle çalışma yasağı getirildi (The New York Times, 2010). Karşılaşılan diğer bir olayda otomotiv sektöründe meydana gelmiştir. Ford Motor Şirketinde üretim mühendisi olarak görev yapan Yu Xiang Dong, 2006 yılında şirketin teklifiyle Ford'un Çin şubesinde görev yapmayı kabul eder. Ancak çalıştığı şirkete ait ticari sırları ihtiva eden 4.000 belgeyi kendi taşınabilir harici belleğine kaydederek, bu bilgileri başka bir Çinli otomobil şirketine kabul girmek için kullanmak isteyen Dong, Nisan 2011'de ticari sırlar çalmaktan dolayı 70 ay hapis cezası ile cezalandırılmıştır (ONCIX, 2011, s.4).

TASNİF DIŐI



Tablo-13: 2011 Yılında Sektörel Bazda Engellenen Günlük Ortalama Saldırı Sayısı

(Kaynak: Symantec (2011). Intelligence Report: November 2011, s.5. 11 Ocak 2012 tarihinde SymantecBilgiPortali: http://www.symanteccloud.com/globalthreats/overview/r_mli_reports?om_ext_cid=biz_socmed_twitter_facebook_marketwire_linkedin_2011Nov_worldwide_intelligencereportnov2011 adresinden alınarak düzenlenmiştir)

Bilgi ekonomisindeki yükseliőle birlikte őirketlere ait fikri mülkiyetlerin sayısallaőtırılarak aė sistemlerinde depolanmaya baőlaması ticari sırlara uzaktan yetkisiz erişim için rakiplere olanak saėlamaktadır. Bu tarz yapılan endüstriyel casusluėu tespit etmek son derece güçtür. Çünkü erişimi yapan kiői çoėunlukla bilgiye zarar vermemekte sadece rekabet avantajı saėlamak için o bilgiyi takip etmektedir (Moore, 2010, s.104). Symantec'in Kasım 2011'de hazırlamıő olduėu raporda sektörel bazda engellenen saldırılar görölmektedir (Tablo-13). Listenin baőında günlük ortalama 20,5 saldırı ile kamu sektörü gelmektedir. İlaç ve kimya endüstrisi günlük 18,6 saldırı ile ikinci sırada yer alırken, üretim sektörü ise 13,6 saldırı ile üçüncü sırada bulunmaktadır. Saldırılar çoėunlukla hedeflenen kuruluőun aė sistemlerine sızarak hassas verileri ele geçirme maksadıyla yapılmaktadır (Symantec, 2011, s.5). Aynı araőtırmaya göre gelen her 255 e-postadan biri zararlı yazılım içermektedir. Bu zararlı yazılımlar belirli bir hedefi gözetmemekle birlikte, 8300 e-postadan birinin ise belirli hedeflere yönelik gönderildiėi belirtilmektedir (Symantec, 2011, s.1). Zararlı yazılımlarla ilgili olarak 2005 yılında bazı büyük İsrail őirketlerinde görev yapan 21 yönetici ile rakip firmalara ait ticari sırları ele geçirebilmek için casus yazılımlar yükleyen Michael Haeprati ve eőı Ruth B. Haeprati'nin tutuklanmaları örnek gösterilebilir. İsrail'de faaliyet gösteren üç farklı özel araőtırma için çalıştıkları deėerlendirilen Haepratiler'in ürettikleri "Truva atı" virüsü ile yaklaşık 80 őirkete haksız fayda saėladıkları tahmin edilmektedir (The

TASNİF DIŞI

Guardian, 2005). 2006 yılının Mart ayında Haeprati'ler endüstriyel casusluk yaptıkları gerekçesiyle İngiltere'den İsrail'e iade edilmişlerdi. Hedef aldıkları şirketlerin arasında İsrail'in önde gelen halkla ilişkiler kurumu olan Rani Rahav (müşterileri arasında İsrail'in ikinci büyük cep telefonu operatörü Partner Communications bulunmaktaydı), bir kablolu televizyon kanalı ile Audi ve Volkswagen araçlarının ithalini yapan Champion Motors gibi şirketler bulunmaktaydı. Ruth Haephrati, yasa dışı bilgisayar erişimi, virüs yerleştirme, klavye kaydedici yerleştirme, özel hayatın gizliliğini ihlal, yasa dışı veri tabanı oluşturma ile suçlanırken eşi de kendisine yardımcı olmaktan yargılanmıştır (OECD, 2008, s.17).

Siber uzayda endüstriyel casusluk olaylarındaki artış nedeniyle devletler de özel şirketlerini uyarmaktadırlar. İngiliz istihbarat servisi MI-5 kendi şirketlerini Çin'in casusluk faaliyetlerine karşı ikaz etmiştir. Mandiant güvenlik şirketine göre, Çin kaynaklı saldırılar ile zararlı yazılım bulaştırılmış bilgisayarlar kullanılarak, ticari sırlar sistematik olarak şirketlerden çalınmaktadır (Moore, 2010, s.104). Amerikan Savunma Bakanlığı'na bağlı Savunma Bilgi Sistemleri Ajansı (Defense Information Systems Agency-DISA), siber saldırılarda farkındalık durumlarını ortaya koymak maksadıyla, 1992-1995 yılları arasında kendi bilgisayarlarına 38.000 saldırıda bulundu. İnternette bulunan zararlı yazılımlar aracılığıyla gerçekleştiren saldırıların ancak %4'ü Savunma Bakanlığı yetkililerince tespit edilebildi. Nasheri (2005, s.115-116)'ye göre bir devletin askeri sistemlerine bile yapılan saldırının tespit edilme oranının bu kadar düşük olduğu bir durumda, özel kişilere ve şirketlere yapılan saldırıların miktarının belirlenmesi oldukça güçtür. Kanaatimizce yazılım şirketleri tarafından ortaya konulan veriler son derece önemli olmakla birlikte, devletlere ait kamu kurumlarının siber alanda uğradıkları zararlar göz önüne alındığında, endüstriyel casusluk amaçlı gerçekleştirilen saldırıların görünenden çok daha fazla olduğu söylenebilir.

ç. ECHELON ve Endüstriyel Casusluk

Avrupa Parlamentosunun oluşturduğu Geçici Komisyon²³ tarafından 11 Temmuz 2001 yılında hazırlanan raporda, ABD ve bazı devletlerin Soğuk Savaş döneminde kurulan küresel bir dinleme sistemini endüstriyel casusluk maksadı ile kullandıklarının tespiti ECHELON sisteminin gündemdeki yerini almasını sağlamıştır.

²³ Temporary Committee on the ECHELON Interception System (11 July 2001). Report on the Existence of a Global System for the Interception of Private and Commercial Communications, Part I. European Parliament Session Document A5-0264/2001

TASNİF DIŞI

Kelime anlamı olarak Fransızca “kademe, basamak” anlamına gelen ECHELON sistemi yer istasyonları vasıtasıyla dünya genelindeki bütün telefon, uydu, faks, telsiz, teleks, e-posta gibi haberleşme kanallarını izleyebilmektedir. Sistem ABD, Kanada, İngiltere, Yeni Zelanda ve Avustralya’nın ortaklığında yürütülmektedir (Girgin, 2003, s.324-325). ABD Ulusal Güvenlik Ajansı (National Security Agency-NSA), İngiltere Hükümet Haberleşme Merkezi (Government Communications Headquarters-GCHQ), Kanada Haberleşme Güvenlik Kurulu (Communications Security Establishment-CSE), Avustralya Savunma Haber Direktörlüğü (Defence Signals Directorate-DSD) ve Yeni Zelanda Devlet İletişim Güvenlik Bürosu (Government Communications Security Bureau-GCSB), adı geçen ülkelerde ECHELON’un takibinden sorumlu birimlerdir (Yılmaz, 2007, s.453).

ECHELON’un temelleri 1947 yılında ABD ve İngiltere arasında imzalanan ve her alanda istihbarat paylaşımını öngören UKUSA Anlaşmasıyla atılmıştır. İngiltere (UK) ve ABD (USA)’nin ingilizce kısaltmalarının birleşiminden oluşan Anlaşmaya daha sonra diğer üç devlet de müdahil olmuştur. Bu durumun en önemli sebebi olarak, elektronik izleme için dünyanın farklı noktalarına üs kurma ihtiyacı, lisan birliği ve köken akrabalığı gösterilmektedir (Girgin, 2003, s.326-327). UKUSA Anlaşması 1971 yılında yerini ECHELON’a bırakmış, dünyanın çeşitli bölgelerinin takibi üye ülkelere paylaştırılmıştır. İngiltere; Afrika ve Avrupa’ya (Ural Dağları’na kadar), Kanada; kuzey enlemlerini ve kutup bölgesini, Avustralya ve Yeni Zelanda; Okyanusya²⁴ ve Hint Okyanusu çevresindeki alanı, ABD ise Kuzey ve Güney Amerika ile Pasifik’teki Intelsat hattını takip etmektedir (Nabbali ve Perry, 2004, s.92).

ABD, İngiltere ve Kanada bahse konu anlaşmanın varlığı ve içeriğini kabul etmemekle birlikte konu ile ilgili ilk resmi açıklama Avustralya ve Yeni Zelanda’dan gelmiştir. Avustralya’daki DSD Başkanı Martin Brady’nin 1999 yılında verdiği bir beyanatta kendilerinin denizaşırı diğer istihbarat örgütleri ile UKUSA Anlaşması çerçevesinde hareket ettiklerini söylemesi bu konuda yapılmış ilk resmi ifadeydi. 2000 yılında Yeni Zelanda Başbakanlığı tarafından yayınlanan bir yayımda²⁵ da GCSB’nin yukarıda sıralanan diğer dört istihbarat örgütü ile olan işbirliği vurgulanarak Yeni Zelanda’nın bu ortaklıktan oldukça faydalandığı ifade edilmektedir. Diğer bir kaynak ise ABD’de 1966 yılında çıkarılan “Freedom of

²⁴ Büyük Okyanus’a dağılmış adaları içine alan ülkelerden ve Avustralya’dan oluşan kıta. Asya’nın güney ve güneydoğusunda, Antarktika’nın kuzeyinde ve Büyük Okyanus ile Hint Okyanusu’nun arasında yer alır.

²⁵ “How New Zealand manages its security and intelligence agencies (2000)”, <http://www.dpmc.govt.nz/dpmc/publications/securingoursafety/gcsb>, E.T: 08 Nisan 2012.

TASNİF DIŞI

Information Act (FOIA)” kanunu ile Savunma Bakanlığı’nın 1997 yılı FOIA düzenlemesi çerçevesinde kamuya açıklanan gizli belgelerdir. Ulusal Güvenlik Arşivi olarak adlandırılan bu belgeler 1985 yılından itibaren George Washington Üniversitesinde araştırmacıların hizmetine sunulmuştur. ABD hükümeti her ne kadar ECHELON’un varlığını kabul etmese de yayınlanan bu belgelerin²⁶ içinde ECHELON sisteminin adı geçmektedir (Temporary Committee, 2001, s.61-63).

UYDU	YÖRÜNGE(mil)	ÜRETİCİ	ÖZELLİĞİ
KH-11	200	Lockheed Martin	Yer Çözünürlüğü: 12 cm. (Casus fotoğraflar için)
LaCrosse	200-400	Lockheed Martin	Yer çözünürlüğü.1-3 m. (Casus fotoğraflar için)
Orion/Vortex	22.300	TRW	Telekomünikasyon izleme.
Trumpet	200-22.300	Boeing	Cep telefonlarını dinleme.
Parsae	600	TRW	Okyanus keşif.
Satellite Data Sys.	200-22.300	Boeing	Veri nakli (röle)
Defense Support Prg.	22.300	TRW/Aerojet	Füze erken uyarı
Defence Meteorological Support Prg.	500	Lockheed Martin	Meteoroloji, nükleer patlama tespiti.

Tablo-14: ABD Casus Uyduları

(Kaynak: The Phoenix Journal, 2000, s.5 ve <http://mondediplo.com/1999/01/07/sat>)

Merkezi ABD’de Ford Mead’da bulunan sistem sekiz ana üsten oluşmaktadır. 100’ün üzerinde irili ufaklı haberleşme ve casus uydulardan (Tablo-14) gelen bilgiler dünya geneline yayılan merkezlere iletilmekte daha sonra da ana üslerde toplanmaktadır. 1998 yılındaki imkânları ile ECHELON’un dakikada 2 milyon, günde ise 3 milyar telefon görüşmesini dinleyebildiği ifade edilmektedir (Yılmaz, 2007, s.453-454).

²⁶ “Document 9: NAVSECGRU Instruction C5450.48A, Subj: Mission, Functions and Tasks of Naval Security Group Activity (NAVSECGRUACT) Sugar Grove, West Virginia, September 3, 1991. “ ve “Document 12: ‘Activation of ECHELON Units’, from History of the Air Intelligence Agency, 1 January - 31 December 1994, Volume I (San Antonio, TX: AIA, 1995).” E.T:09 Nisan 2012, <http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB23/index2.html>.



Resim-2: Menwith Hill İstasyonu (İngiltere)

Kaynak: <http://www2.warwick.ac.uk/fac/soc/pais/people/aldrich/vigilant/lectures/gchq/menwith/>, E.T: 09 Nisan 2012.

Bilinen gözlem istasyonları arasında, ABD’de Yakima-Washington ve Sugar Grove-Batı Virginia, Porto Riko’da Sebana Seca; İngiltere’de Morwenstow ve Menwith Hill (Resim-2); Japonya’da Misawa; Yeni Zelanda’da Waihopai; Kanada’da Leitrim-Ontario ve Almanya’da Bad Aibling (Resim-3) istasyonları bulunmaktadır (Nabbali ve Perry, 2004, s.92).



Resim-3: Bad Aibling İstasyonu (Almanya)

(Kaynak: <http://aib.de/nsa.htm>, E.T: 09 Nisan 2012)

Burada sıralanan istasyonlar ve diğ er merkezlerden ECHELON sistemine anahtar kelimeler girilerek d nya genelindeki haberleŐme trafiđi  zerinde tarama

TASNİF DIŐI

yapılmaktadır. Anahtar kelimeler olarak toplanmak istenen bilginin çeşidine göre kişi adları, adresler, telefon numaraları, kurum ve kuruluşlar, adresler gibi akla gelebilecek her türlü ifade seçilebilmektedir. Sistem anahtar kelimeleri bulmakla kalmaz, istasyonların özel olarak araştırdıkları bilgileri de herhangi bir yerde elde etmesi halinde ilgili birime otomatik olarak da iletir (Nabbali ve Perry, 2004, s.93). ECHELON'un bir diğer önemli özelliğı ise ses tanıma ve optik karakter saptama özelliğine sahip olmasıdır. VOICECAST sistemi ile belirli bir kişinin haberleşmesi ses özelliğinden dolayı takip edilebilir, ileride kullanılmak üzere yazılı forma çevrilebilir (The Phoenix Journal, 2000, s.5). Ses analizinden kimlik tanımlama özelliğı yapabilen yazılımların 1995 yılından beri kullanıldığı düşünülmektedir (Sloan, 2001, s.1481).

ECHELON benzeri küresel dinleme ve takip sistemlerine Fransa ve Rusya'nın da sahip olduğu belirtilmektedir. Dünyanın çeşitli bölgelerinde yer istasyonlarına sahip olan bu iki ülkenin dinleme kapasiteleri hakkında yeterli bilgi bulunmamaktadır (Temporary Committee, 2001, s.11).

ECHELON sisteminin özel hayatın gizliliğı ve iş yaşamına yönelik yarattığı tehditler sadece güçlü bir gözlem sistemi olmasından değil aynı zamanda oldukça geniş bir alanda kanuni sınırlar olmaksızın hareket etmesinden de kaynaklanmaktadır. Bu ülkelerin yasama organlarının da sistem üzerindeki denetimleri son derece sınırlıdır (Temporary Committee, 2001, s.24).

Geçici Komisyon tarafından hazırlanan raporda, ABD'li resmi kaynaklar tarafından yayınlanan belgelerde kişilerin endüstriyel casus olarak kullanımı konusu oldukça geniş yer tutarken elektronik yöntemler konusunda çok az değinilmesi eleştirilmektedir (Temporary Committee, 2001, s.110).

d. Rekabet İstihbaratı ve Endüstriyel Casusluk

Rekabet istihbaratı kavramı zaman zaman endüstriyel casusluk kavramı ile bir arada kullanılmaktadır. Her ikisi de rekabette öne geçmeyi amaç edinse de endüstriyel casuslukta yasal ve etik olmayan yöntemlerin kullanılması iki kavramı da birbirinden ayırmaktadır (Özdemir, 2010, s.71).

İngilizce karşılığı "competitive intelligence" olan rekabet istihbaratı, hem süreç hem de ürün olarak kabul edilmektedir. Kanunlara uygun olarak ve iş ahlakıyla çelişmeyecek şekilde gerek resmi gerek özel kaynaklardan rakipler hakkında bilgi toplanması faaliyeti rekabet istihbaratının süreç boyutunu oluşturmaktadır. Ürün olarak değerlendirildiğinde ise "rakiplerin, tedarikçilerin, müşterilerin, kamu

TASNİF DIŐI

kurumlarının, iřtiraklerin, pazarların ve genel iřletme evresinin gncel ve gelecekteki davranıřları ve teknolojik eęilimler, ekolojik geliřmeler hakkında edinilen enformasyondur.” (Akpınar ve Edin, 2007, s.2).

Rekabet istihbaratının genel zelliklerini sıralamak gerekirse;

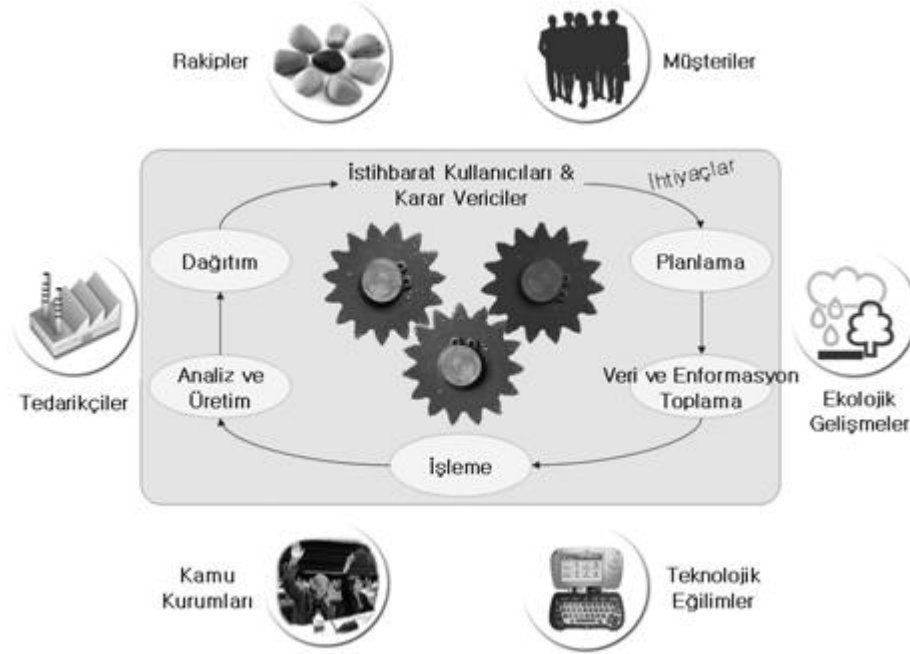
- Rekabet istihbaratında toplanan veri ve bilgiler kullanıcının istekleri doęrultusunda analiz edilerek, hareket tarzına ynelik bilgi retilir.
- İřletme ve evresi btn olarak deęerlendirilerek geliřmeler srekli takip edilir.
- Hedeflenen bilgilerin toplanmasında gncel bilgi teknolojileri ile analitik yntemlerden yoęun řekilde faydalanılır.
- İřletmelerin ynetimlerini stratejik aıdan daha etkin kılmayı amalar.
- Sadece aık kaynakları kullanması ve etik deęerlere sahip olması nedeniyle endstriyel casusluktan net izgilerle ayrılır (Akpınar ve Edin, 2007, s.2).

Bugn binlerce řirket tarafından pazarda yer alan rakipleri hakkında bilgi edinmek maksadıyla rekabet istihbaratı teknikleri uygulanmaktadır. İř dnyasında rakipler hakkında internet zerinde arařtırma yapmaktan, gazete kuprlerini takip etmeye kadar yaklařık 2 milyar dolarlık bir pazarın bulunduęu iddia edilmektedir. Rekabet İstihbaratı Profesyonelleri Topluluęu (Society of Competitive Intelligence Professionals-SCIP)’na gre rakipler hakkında bilgi toplama amacıyla 2000 yılında kendilerine ye řirketlerden %25’i 100.000 dolarlık harcama yaparken, %14’lk bir blm 500.000 dolardan daha fazla harcama yapmıřtır (SCIP, 2012).

Gnmzde rekabet istihbaratı konusunda řirketlere danıřmanlık hizmeti veren ve ihtiya duyulan bilgileri aık kaynaklardan toplayan ve analiz eden řirketler bulunmaktadır. rnek vermek gerekirse 1985 yılında Motorola rekabet istihbaratı uzmanları Japon řirketlerinin Avrupa’ya ynelik stratejileri zerine bir alıřma yaptı. O dnemde Motorola-Avrupa yneticileri Japonlar tarafından Avrupa’ya yapılacak bir hamleyi beklemiyorlardı. Yapılan alıřma, Japonların 1987 yılında sermaye yatırımlarını ikiye katlamayı planladıklarını ancak bundan nce Avrupa yarı iletken pazarına girmeyi hedeflediklerini ortaya koyuyordu. Sonu olarak Motorola stratejisini deęiřtirerek Avrupalı ortakları ile ortak alıřmaya giriřti ve bu sayede Japon řirketlerini pazarın dřunda tutmayı bařardı. Her ne kadar pazar payı ve kr oranı ykselmemiřse de, Japonların uyguladıkları pazar stratejileri nedeniyle dibe vuran dięer Amerikan řirketleri ile aynı kaderi paylařmamıřtır (Gilad, 1995).

TASNİF DIŐI

Rekabet istihbaratı süreci birbirini tamamlayan beř ayrı basamaktan oluřmaktadır (řekil-7). Sırasıyla planlama, veri ve enformasyon toplama, iřleme, analiz ve üretim son olarak dağıtım ařamalarından oluřan bu süreçte her bir bölümün kendine özgü iřlevleri bulunmaktadır.



řekil-7: Rekabet İstihbaratı Süreci

Kaynakça: (Akpınar ve Edin, 2007, s.5)

Planlama: Planlama safhası, ihtiyaç duyulan bilgilerin neler olduėunun tespit edildiėi safhadır. İnternet ve bilgi iletiřimi teknolojileri sayesinde açık kaynaklardan istenilen pek çok bilgiye ulařılmasına kolaylařmasına raėmen aynı kaynaklarda bilgi kirliliėi ve ilgili olamayan bilgiler de mevcuttur. Haber toplama faaliyetlerinin daha düzenli, koordineli ve hedef odaklı çalışabilmesi adına hangi bilgilerin toplanacaėının önceden belirlenmesi zaman ve kaynakların etkin kullanımı açısından son derece önemlidir. Bu ařamada ařaėıdakilere benzer soruların cevapları aranır.

- Rakiplerin finansal hedefleri nelerdir?
- Rakiplerin risklere yaklařımı nedir?
- Organizasyonel yapısı ne řekildedir?
- Hangi kontrol ve teřvik sistemleri uygulanmaktadır?
- Yöneticilerinin yönetme becerileri ve liderlik kapasiteleri hangi seviyededir ?(Porter, 2007, s.64-65)

TASNİF DIŐI

Veri ve Enformasyon Toplama: Bu safhada belirlenen haber toplama vasıtaları ile birlikte planlama safhasında cevaplanması istenen sorulara ilişkin veriler toplanır. İstenilen bilgilerin toplanılmasında saha verileri ve basılı verilerden yoğun şekilde faydalanılır. Reklam ajansları, rakip firmalardan işe alınan personel, mesleki toplantılar, ticaret birlikleri, pazar araştırma firmaları, tedarikçiler, hisse senedi analistleri ve satış gücü gibi bilgiler saha araştırmaları arasında yer almaktadır. Basılı verilere örnek olarak, analist raporları, patent kayıtları, mahkeme kayıtları, yönetim tarafından yapılan konuşmalar, devlet kurumlarına gönderilen belgeler, eleman arama ilanları gösterilebilir (Porter, 2007, s.92). Kullanılan teknik ve yöntemler yasa dışı olması halinde bu safha endüstriyel casusluğa dönüşür.

İşleme: İşleme safhasında elde edilen veriler güvenilirlik açısından kontrol edilerek, düzenlenir ve kaydedilir. Uygulama aşamasında en zahmetli ve maliyetli aşama olarak ifade edilmektedir.

Analiz ve Üretim: Toplanan ve kaydedilen verilerin çeşitli analiz yöntemleri ile değerlendirilerek istihbarata dönüştürüldüğü aşama, analiz ve üretim aşamasıdır. Burada portföy analizi, güçlü ve zayıf yönler analizi, rekabet ve müşteri analiz teknikleri, finansal ve çevre analiz teknikleri gibi yöntemler kullanılmaktadır. Bunların haricinde, STEPP, Delphi metodu, yapay sinir ağları, kritik başarı faktörleri analizi ve veri madenciliği de faydalanılan diğer yöntemler arasındadır (Akpınar ve Edin, 2007, s.6).

Dağıtım: Bu safhada analiz edilerek istihbarat dönüştürülen bilgiler ilgili bölümlere iletilir. Çalışma sonucunda hazırlanan, düzenli rakip bültenleri, durum raporları ve brifingler şirketin o konuda bilgiye ihtiyacı olan birimine gönderilir.

Rekabet istihbaratı sürecinde, istihbaratın isteğinde bulunan işletmeler ile öncelikli istihbarat ihtiyaçlarını belirleyen, istihbaratı toplayan, derleyen analiz eden ve zamanında uygun yerlere dağıtımını yapan uzmanlar rekabet istihbaratının aktörlerini oluşturmaktadır. İstihbarat uzmanları genellikle işletmenin içinde yer alan, farklı bilgi ve tecrübe birikimine sahip kişilerden oluşmaktadır. Nicel ve nitel analiz tekniklerini kullanan uzmanlar çoğunlukla işletmenin pazar ve rekabet araştırması yapan birimlerinde görev yapmaktadırlar (Edin, 2008, s.593). Analiz edilen niceliksel bilgiler arasında pazar payı, finansal veriler, büyüme oranları gibi bilgiler yer alırken niteliksel veriler arasında rakiplerin hareketleri, pazarlama yaklaşımları, organizasyonlar veya gelecekteki olası yönelimleri gibi bilgiler yer almaktadır (Özdemir, 2010, s.69).

TASNİF DIŐI

Biliřim teknolojilerinde yařanan geliřmeler ve internetin yaygınlařması rekabet istihbaratı konusunda yapılan alıřmaların daha kolay ve etkin yapılmasını saęlamıřtır. Rakiplerin fikri mülkiyet konusundaki geliřmeleri ve stratejik planları gibi bazı bilgiler kamu veya özel sektöre ait web sitelerinden, ya da haber, forum ve sosyal paylařım siteleri gibi bilgi aęının getirdięi yeni kanallardan da elde edilebilmektedir (Nasheri, 2005, s.74).

Rekabet istihbaratı birbirini tamamlayan dört kademeli bölümden oluřmaktadır.

- Stratejik Seviyede Rekabet İstihbaratı: Yüksek seviyede yönetim kademesine iřletmenin içinde bulunduęu ekonomik, politik ve yasal konularla birlikte rakiplerin güncel ve gelecekteki durumları hakkında bilgi saęlayan istihbarat eřididir. Aynı zamanda pazarda birleřme, satın alma ya da ortaklık kurma ihtimali bulunan firmaların da geliřimini takip eder. Bu tarz faaliyetler 1980-1990'lı yıllarda "iř istihbaratı" olarak da adlandırılmaktaydı.
- Taktik Seviyede Rekabet İstihbaratı: Pazar veya satıř ve pazarlama istihbaratı olarak da adlandırılan bu seviyede rakip řirketlerin müşteri ve tüketicilerle olan iliřkileri takip edilmektedir. İřletmelere, taleplere daha hızlı cevap verme ya da pazarlamada geliřen fırsatlara göre deęiřiklik yapma avantajı saęlar.
- Teknolojiye Yönelik Rekabet İstihbaratı: İřletmenin teknoloji stratejilerini desteklemek maksadıyla rekabet istihbaratının özellikle ARGE alıřmalarına yöneltildięi faaliyetlerdir. Teknoloji istihbaratı veya rekabet teknik istihbaratı olarak da adlandırılmaktadır.
- Hedefe Yönelik Rekabet İstihbaratı: Pazarın geneli deęil sadece belli rakiplerin hedef alındıęı faaliyetlerdir (Nasheri, 2005, s.75-76).

Rekabet istihbaratı kamuya aık olan bilgilerden elde edildięi halde sadece etik deęerler aısından endüstriyel casusluktan ayrılması "bilgi" temelli olarak beraberinde bazı soruları da gündeme getirmektedir. Örneęin özel ya da gizli bilgiler iřletme tarafından rakiplerin bilmesini istemedięi, etik ya da yasal koruma altında bulunan bilgilerdir. Bir řirketin özel bilgilerinin gizlilięinin saęlanması bireylerin özel hayatlarının korunmasından daha zordur. Örneęin řirketler pek ok alıřan kiřiden oluřmaktadır. Bu durum da daęılan bilginin kontrolünü güçleřtirmektedir. Dięer bir özellik ise insanların özel hayatları ile mukayese edildięinde özel hayatın nerede

TASNİF DIŞI

başlayıp nerede bittiği kesin olarak bilinmekle birlikte, şirketlerin özel olarak nitelendirilebilecek sınırları çok fazla belirgin değildir. Son olarak pek çok şirket faaliyeti kamu yararına ve kamuya açık olan satış büroları, ofisler, hastaneler vb. gibi yerlerde yapıldığı gibi ulaşım, haberleşme, iletişim faaliyetleri kamunun da kullandığı ortak alt yapılar üzerinden gerçekleşmektedir. Bu alanlar genellikle meşru bir şekilde takip edilebilir ve izlenebilir durumdadır (Crane, 2005, s.237).

Crane (2005, s. 234)'e göre rekabet istihbaratı konusunda pek çok yasal tanım bulunmakla birlikte, endüstriyel uzmanlar ve yorumcular “endüstriyel casusluk” terimine küçük düşürücü bir anlam yüklemekte ve onun yerine daha “tarafsız” bir kavram olan rekabet istihbaratını kullanmaktadırlar. Buna neden olarak da endüstriyel casusluk ve rekabet istihbaratı arasındaki etik çizgisinin sorgulanabilir nitelikte olduğunu belirtmektedir.

e. İstihbarat Örgütlerinin Endüstriyel Casusluk Faaliyetleri

İstihbarat örgütleri, sınırları oldukça belirsiz bir kavram olan “ulusal güvenlik” düşüncesi çerçevesinde faaliyet gösteren resmi kurumlardır. Genel olarak istihbaratta aktif yaklaşım, devletin stratejik çıkarlarının belirlenmesi ve takibine odaklanırken, pasif yaklaşımda kamu güvenliği veya ulusal güvenliğe yönelik tehditlerin ortaya çıkarılması hedeflenmektedir (Portoeus, 1995). İstihbarat örgütleri, ekonomik/endüstriyel casusluk maksadıyla pek çok istihbarat toplama yöntemini kullanabilmektedir. Bu yöntemler arasında en çok kullanılanlar ise İnsan İstihbaratı (Human Intelligence-HUMINT) ile Sinyal İstihbaratıdır (Signal Intelligence-SIGINT) (IOSS, 1996, s.5-2). Amerikan Ordusu İnsan İstihbaratı Talimnamesine²⁷ göre İnsan İstihbaratı (HUMINT), eğitilmiş personel tarafından, insanlardan, onlarla ilgili belgelerden ve medya kaynaklarından; niyetleri, unsurları, tertipleri, güçleri, ekipmanları, personeli ve yetenekleri hakkında bilgi toplama faaliyetine verilen addır. Bu yöntemde ihtiyaç duyulan bilgiler insan kaynaklarından elde edilir (FM 2-22.3, 2006, s.1-4). İnsan istihbaratında bilgi toplama faaliyeti, diplomatlar ve diğer resmi görevliler tarafından açık olarak yapılabileceği gibi casusluk gibi kapalı/gizli metotlarla da gerçekleştirilebilir (Özdağ, 2009, s.129). Sinyal istihbaratı ise “elektronik sistemler tarafından yayımlanan elektromanyetik enerjinin alınması, kaydedilmesi, değerlendirilmesi ve yorumlanması ile elde edilen istihbarattır” (Özdağ, 2009, s.135).

²⁷ FM 2-22.3 (FM 34-52). Human Intelligence Collector Operations Headquarters, Department of the Army. September 2006.

TASNİF DIŞI

Portoeus, ekonomik ve ticari çıkarların korunması amacıyla istihbarat örgütlerinin beş alanda görev yapabileceğini belirtmektedir.

- Karşı İstihbarat Desteği: İstihbarat örgütleri, ülkelerinin ekonomik çıkarlarına aykırı faaliyet gösteren yabancı istihbarat örgütlerinin faaliyetlerini takip ederek hükümetlerine bildirir.
- Karar Alıcılara Ekonomik İstihbarat Desteği Sağlama: İstihbarat örgütleri, sahip oldukları imkânları kullanarak topladıkları ve yorumladıkları bilgiler vasıtasıyla siyasi karar alıcıları destekleyebilir.
- Ticari Anlaşmaların Gözlemlenmesi ve Haksız Rekabet Hakkında Bilgi Toplama: Uluslararası anlaşmalarda bağlı devletin ulusal ekonomik ve ticari çıkarının gözetilmesi maksadıyla rakiplerin gizledikleri yetenek ve niyetleri araştırılabilir.
- Yabancı ülkede Olay, Davranış ve Politikaları Etkilemek Maksadıyla Özel Operasyonlar Düzenleme: Yabancı ülkedeki ekonomik kararları etkilemek için yapılan gizli faaliyetlerden, pazarlarında bilgi kirliliği yaratmak için yapılan eylemlere kadar çeşitli hareket tarzlarını kapsar.
- Seçilen Özel Bir Ticari Kurum için İstihbarat Desteği Sağlanması: İstihbarat örgütleri tarafından özel şirketlere elde edilen teknolojik ve ticari sırların verilmesi pek çok Batılı devlet tarafından resmi olarak kabul edilmemektedir (Portoeus, 1995).

ABD Kongresinde Senatör Brown tarafından hazırlanan rapora göre, açık olmayan kaynaklardan elde edilen istihbaratın %5'i ekonomik istihbarat maksadıyla toplanmaktadır. Buna göre sağlanan istihbarat sayesinde imzalanan ticari anlaşmalar ABD sanayiine yıllık 7 milyar dolarlık bir kazanç sağlamaktadır (Temporary Committee, 2001, s.14). ABD istihbarat örgütleri, sadece genel ekonomik durumu araştırmakla kalmayıp şirketler arasındaki haberleşmeyi, rüşvetin önüne geçme iddiasıyla da dinlemektedir. Haberleşmenin böylesine detaylı takibi yolsuzlukla mücadele yerine rekabet istihbaratı amacıyla bilgi toplamaya açıktır. Her ne kadar Amerikan ve İngiliz yetkililer elde ettikleri istihbaratı haksız rekabet maksadıyla kullanmadıklarını iddia etseler de Amerikan Ticaret Bakanlığı'na bağlı "Advocacy Center"ın faaliyetleri tam olarak anlaşılabilmiş değildir (Temporary Committee, 2001, s.13). 2001 yılında bir yöneticisi ve on iki çalışanı olan "Advocacy Centre"da proje yöneticilerinin faaliyet alanları ve konuları şunlardı: Rusya ve yeni bağımsız devletler; Afrika Doğu Asya ve Pasifik; Orta Doğu, ve Kuzey Afrika; Güney Asya-Bangladeş, Hindistan, Pakistan, Sri Lanka; Avrupa ve Türkiye; dünya genelinde havacılık, otomobil ve savunma sanayi; telekomünikasyon, bilişim

TASNİF DIŐI

teknolojileri. Amerikan řirketlerinin ihracatını desteklemek için kurulan merkez, sadece ABD ulusal ıkarlarının bulunduđu projelerde yardımcı olmaktadır. Örneđin herhangi bir anlaşma sonucu üretilen ürünlerin en az %50'sinin ABD içinde üretilmesi şartını koymaktadır (Temporary Committee, 2001, s.113). ABD daha ok teknolojik ortamda ekonomik değeri olan bilgileri toplamakla suçlanmaktadır. Bununla birlikte istihbarat personelinin karıştığı endüstriyel casusluk olaylarıyla da zaman zaman gündeme gelmektedir. Örnek vermek gerekirse 1997 yılında ABD Bonn Büyükelçiliđi'nde görev yapan kimliđi açıklanmayan bir CIA ajanı, Almanya Ekonomi Bakanlığı'nda ileri teknoloji içeren projelere erişim yetkisine sahip üst düzey bir görevliyi angaje etmeye alışmasının ortaya ıkması üzerine Alman hükümeti tarafından sınır dışı edilmiştir (Cowell, 1997). Diğer bir olayda ise, 26 Ocak 1995 tarihinde ABD'nin Fransa Büyükelçisini ađıran Fransız İç İşleri Bakanı Charles Pasqua, beř Amerikan diplomatının ve CIA sorumlusunun Paris'ten gönderilmesini istemiřtir. Diplomatlar, 1993 yılı GATT görüşmelerinde Fransa'nın tutumunu öğrenmek maksadıyla yetkililere rüşvet vermeye teşebbüsle suçlanıyordu (Todd ve Bloch, 2004, s.121). ABD'nin karıştığı endüstriyel casusluk faaliyetleri nedeniyle CIA'nın Berlin, Roma ve Paris'teki istasyonlarının büyüklüğü ve alışma alanı da Avrupa'da sorgulanır hale gelmiştir (Clark ve Johnston, 1998, s.424). 1994 yılında Brezilya'nın Amazon yağmur ormanlarının gözlemi için yapmayı planladığı 1,3 milyar dolarlık SIVAM (Sistema de Vigilância da Amazônia) projesi için Fransız Thomson-CSF ile Brezilyalı yetkililer arasındaki görüşmenin de NSA tarafından dinlendiđi iddia edilmektedir. İhaleyi kazanan Amerikan Raytheon firması, Ticaret Bakanlığı'nın bu projede Amerikan sanayiini desteklemek için ok alıştığını açıklamıştır. Raytheon aynı zamanda Sugar Grove'da bulunan ECHELON istasyonunun da bakım ve mühendislik hizmetlerini sağlamaktadır (Campbell, 1999, s.18). 1990 yılında Endonezya'nın gerçekleřtirmeyi düşündüğü haberleşme ile ilgili bir projede yarışan Amerikan AT&T řirketi ile Japon konsorsiyumunun tekliflerinden Japonların kazanacağı bilgisini alan istihbarat örgütleri, durumu dönemin Bush yönetimine iletmışlerdi. Endonezya Hükümetine konunun yeniden düşünülmesi için yapılan ađrı üzerine ihale Amerikan ve Japon řirketleri arasında paylaştırılmıştır. CIA'nın sadece 1994 yılında bunun gibi toplam değeri 28 milyar dolar olan 51 ihaleyi açığa ıkardığı ifade edilmektedir. Bunun yanında CIA'nın Nisan 1994'ten 17 ay önce Amerikan řirketlerinin dezavantajlı konuma düřtüğü ve toplam değeri 30 milyar doları bulan ihalelerde de karar alıcıları 72 kez ikaz ettiđi belirtilmektedir. Rüşvetin önlenmesi ve ihalelerin kazanılması konusunda eski Merkezi İstihbarat Başkanı (Director of Central Intelligence-DCI) James Woolsey “ Bu işte ok iyiyiz” demiřtir (Gregory, 1997).

TASNİF DIŐI

İsrail'e baęlı Bilimsel İliřkiler İrtibat Brosu (LAKAM)'nın da endstriyel casusluk faaliyetinde bulunduęu deęerlendirilmektedir. rneęin 1967 yılındaki Altı Gn Savařları'nda hava gcnn %10'unu kaybeden ve byk çoęunluęunun da bakıma ihtiyacı olan İsrail'e Fransızlar'ın da dâhil olduęu pek çok Batı'lı devlet silah satıřını yasaklamıřtı (Dugdale-Pointon, 2001). 1971 yılında MOSSAD ve LAKAM İsviçre'de irtibata geçtikleri Alfred Frauenknecht isimli mhendisten, Fransızların Mirage III savař uçaęına ait planları ele geçirdiler. Frauenknecht, Fransız řirketin lisansı altında İsviçre'de faaliyet gsteren bařka bir řirkette st dzey mhendis olarak grev yapıyordu. İsraililerden 200.000 dolar aldıęını kabul eden mhendis, olayın açıęa çıkmasından sonra 4,5 yıl hapis cezasına çarptırıldıęı gibi İsrail'in İsviçre Askeri Atařesi de sınır dıřı edildi (Los Angeles Times, 1991). İsrail Mirage III savař uçaęı (Resim-4) hakkında elde ettięi bilgilerden sonra bu uçaęın benzeri olan "Kfir" savař uçaęını (Resim-5) retmiřtir (Blood, 2002, s.232).



Resim-4: Dassault Mirage III Savař Uçaęı



Resim-5: IAI Kfir Savař Uçaęı

Kaynak: (Global Aircraft, 2012 ve Aviatia Site, 2012)

Amerikan Endstriyel Gvenlik Topluluęu (American Society for Industrial Security-ASIS)'nin 2007 yılında yayınladıęı rapora gre ABD bilgi varlıklarına ynelik en byk saldırılar Çin, Rusya ve Hindistan kaynaklıdır (ASIS, 2007, s.12). Aynı raporda FBI'nın 2005 yılı tahminlerine gre Çin hkmeti tarafından kurulan 3.000'den fazla paravan řirket Çin'in çıkarları doęrultusunda faaliyette bulunmaktadır (ASIS, 2007, s.20). Çin İstihbarat Servisi "Guojia Anquan Bu (Guoanbu)"nın hassas bilgilerin toplanması konusunda çalıřmalar yaptıęı ifade edilmektedir (Ramcharan, 2005, s.143). rneęin radara yakalanmayan seyir fzesine ait gizli bilgileri 110.000 dolar karřılıęında Çinlilere verdięi tespit edilen Hint asıllı mhendis Noshir Gowadia, 2011 yılında 32 yıl hapis cezasına çarptırılmıřtı (BBC, 2011). Amerikan Ulusal Karřı İstihbarat İcra Dairesi (Office of National Counterintelligence Executive-ONCIX)'nin 2011 yılında hazırladıęı raporda Çin,

TASNİF DIŐI

dünya genelinde endüstriyel/ekonomik casusluğu en etkin kullanan devlet olarak gösterilmektedir (ONCIX, 2011, s.i). Aynı rapora göre sadece 2010 bütçe yılı içerisinde “Ekonomik Casusluk Kanunu (EEA)” kapsamında yargılanan yedi kişiden altısı Çin ile bağlantılıydı. 2010 yılının Haziran ayında ABD’de yakalanan 10 Rus Gizli Servisi (SVR) üyesinin de ekonomik ve teknolojik bilgileri toplamakla görevli oldukları ifade edilmektedir (ONCIX, 2011, s.6).

Fransız istihbarat örgütü DGSE’nin başkanlarından Pierre Marion kendisi ile yapılan bir röportajda endüstriyel casuslukla ilgili olarak “Ekonomik alanda bizler (Fransa ve ABD) müttefik değil rakibiz. En çok teknik bilgiye ABD sahip ve bu bilgilere kolaylıkla erişilebilir durumda. Doğal olarak istihbarat örgütlerinin ilgisini bu ülke çekmektedir” demektedir (Schweizer, 1996, s.11). 1996 yılında Fransa Savunma Bakanlığı ile bağlantılı yarı-resmi bir kurum olan Uluslararası Savunma Konseyi tarafından (Défense Conseil International-DCI) Ekonomik Savaş Okulu (l'Ecole de Guerre Economique-EGE) kuruldu. Fransız akademisyen, gazeteci, emekli asker ve istihbarat uzmanlarının görev yaptığı EGE’de ekonomik istihbarat toplamak maksadı ile eğitim verildiği belirtilmektedir (WND, 2004). Fransız istihbarat örgütü DGSE’nin haberleşme uydu teknolojilerine yönelik Loral Space Systems ve Hughes Aircraft; MILSTAR askeri uydu haberleşme sistemleri için Lockheed ve TRW; mikrodalga teknolojileri konusunda GTE şirketlerini takip ettiği belirtilmektedir (IOSS, 1996, s. 5-6).

Almanya’nın da İstihbarat örgütleri vasıtasıyla rakip firmalardan elde ettiği bilgileri kendi ülkesindeki şirketlere aktardığı iddia edilmektedir. Alman istihbarat örgütü BND’nin Frankfurt dışında bulunan ve RAHAB adı verilen bir dinleme sistemi sayesinde ABD, Rusya, İngiltere, Japonya, Fransa ve İtalya’daki bilgisayar sistemlerine erişebildiği ifade edilmektedir (IOSS, 1996, s.5-6). Almanya ilgili diğer bir olay da Aralık 1989 yılında ABD’ye gelen BND ajanı Heinrich Stohlze tarafından biyo-teknolojik araştırma bilgilerinin çalınması hadisesidir. Stohlze, Boston’daki bir firmada çalışan personelle kurduğu ilişki sayesinde ticari sır niteliği olan hassas bilgilere ulaşabilmiştir. Firma yöneticilerince sızıntının fark edilmesi üzerine Stohlze de elindeki yüzlerce sayfa belge ile Almanya’ya kaçmıştır (Stewart, 1994, s.14).

Endüstriyel casusluk konusunda Güney Kore’nin de faaliyetleri bulunmaktadır. ABD Deniz Kuvvetlerinde görev yapan Güney Kore kökenli Robert Kim, uydular ile gemiler arasındaki komuta kontrolü sağlayan sistem hakkında gizli bilgileri vermekten dolayı mahkûm olmuştur. Güney Kore’deki Ulusal Planlama Ajansı (National Planning Agency-NPA)’nın diğer ülkelerden elde ettiği fikri mülkiyet

TASNİF DIŐI

ieren bilgileri kendi ok uluslu řirketlerine verdiđi belirtilmektedir (Brenner ve Crescenzi, 2006,412). Diđer bir endüstriyel casusluk olayı ise Güney Kore sanayi devi Ssangyong ile Amerikan Litton Systems arasında meydana gelmiştir. F-16 savaş uçaklarında kullanılan mikrodalga teknolojisi üzerinde alışmalar yapan Litton Systems, M Square Microtec firması ile ortak alışmalar yapmaktaydı. Ssangyong, önce M Square Microtec firmasını satın alarak bu firma üzerinden Litton'a ait F-16 savaş uçaklarında kullanılacak mikrodalga teknolojisine ait bilgileri ele geçirmiştir. Litton'un açtığı davayı kaybeden Ssangyong 1995 yılında 65 milyon dolar tazminat ödemeye mahkûm edildi (Clarke ve Johnston, 1998, s.421).

Schweizer (1996, s.12), Japonya'da bulunan Uluslararası Ticaret ve Sanayi Bakanlığı (Ministry of International Trade and Industry-MITI) ile Japon Dıř Ticaret Organizasyonu (Japan External Trade Organization-JETRO)'nun aralarında kurduđu işbirliđi ile Japon řirketlerine ticari istihbarat sağladığını iddia etmektedir. Japon řirketlerinin karıştığı endüstriyel casusluk olaylarına örnek olarak, 1982 yılında Hitachi Şirketi tarafından IBM'e ait 3380 bilgisayar modeli ile "Adirondack Workbooks"a ait ticari sırların ele geçirilmeye alışılması gösterilebilir. Olayın açığa ıkması üzerine Hitachi Şirketi IBM'ye 300 milyon dolar tazminat ödemek zorunda kalmıştır (Ramcharan, 1996, s.143).

2002 yılında Rus diplomatları İsve'te bir endüstriyel/ekonomik casusluk olayına karışmışlardır. Gripen savaş uçakları için radar ve füze güdüm sistemleri geliřtiren İsve'in Ericsson Şirketi'nden hassas bilgileri elde eden iki Rus diplomat, İsve Hükümeti'nin "istenmeyen adam (persona non grata)" ilanı üzerine ölkelerine gönderilmişlerdir. İsve Polisi'nce beř Ericsson personelinin karıştığı düşünölen olayda, eski alışanlardan biri Rus elilik görevlilerine gizli bilgileri verirken suçüstü göröntölenmiştir (Osborn, 2002).

Endüstriyel casusluk konusunda son dönemde adı geen ölkelerden biri de Avustralya'dır. Avustralya, ECHELON dinleme sistemindeki konumu nedeniyle suçlanmakla birlikte İngiliz-Avustralya ortaklıđındaki Rio Tinto Şirketi'nin karıştığı endüstriyel/ekonomik casusluk olayı kendisini in Hükümeti ile karşı karşıya getirmiştir. 2009 yılında Rio Tinto Madencilik Şirketi'nin řanghai bürosunun başında olan Avustralya vatandaşı Stern Hu ve üç şirket alışanı rüşvet almak ve ticari sırları almak suçundan in polisi tarafından yakalanmıştı. Rio Tinto ile in elik sanayiinin demir cevheri konusunda pazarlık yaptıkları dönemde meydana gelen olayda, Hu ve arkadaşları 13 milyon dolar rüşvet almaktan ve ticari casusluktan

TASNİF DIŐI

dolayı suçlu bulundular. 2010 yılında Stern Hu 10 yıl hapse mahkûm edildi (Garnaut ve Liu, 2010).

ÜLKE	İSTİHBARAT ÖRGÜTLERİ ve KURUMLAR
ABD	NSA (ECHELON), CIA, Advocacy Center
İngiltere	GHCQ (ECHELON)
Avustralya	DSD (ECHELON)
Kanada	CSE (ECHELON)
Yeni Zelanda	GCSB (ECHELON)
Rusya	FSB, GRU, SVR
Japonya	MITI, JETRO
Güney Kore	Ulusal Planlama Ajansı (NPA)
Çin	Guoanbu
Fransa	DGSE, DRM, EGE
Almanya	BND
İsrail	LAKAM, MOSSAD

Tablo-15: Endüstriyel Casusluk Faaliyetinde Bulunduğu Değerlendirilen İstihbarat Örgütleri ve Kurumlar

Kaynaklar: [(Blood, 2002, s.230-233), (ASIS, 2007, s.12), (Fraumann,1997, s.305-306), (Brenner ve Crescenzi, 2006, s.401-413), (Ramcharan, 2005, s.142-145), (Temporary Committee on ECHELON, 2001) ve ONCIX 2011 Report'dan elde edilen bilgilerden düzenlendi.]

Meydana gelen olaylardan, medyada yer alan haberlerden, devlet adamlarının yapmış oldukları açıklamalardan, bu konudaki yazılardan ve raporlardan anlaşıldığı kadarıyla endüstriyel/ekonomik casusluk konusunda etkin olan ülkeler ve istihbarat kurumları (Tablo-15)'de yer almaktadır. Bahse konu devletler, uluslararası ticarete uygulanan bu etik dışı davranışı kınamakla birlikte sanayilerini desteklemek adına istihbarat örgütlerini aktif olarak kullanmaktan da çekinmemektedirler. Fraumann (1997, s.306), endüstriyel casusluk faaliyetlerini ülkelerin istihbarat örgütlerinin teknolojik kapasitesi ile bu teknolojiyi etkin bir şekilde kullanabilecek uzman personelin varlığına bağlamaktadır. Kanaatimizce de bu doğru bir yaklaşımdır. Az gelişmiş ya da gelişmekte olan ülkeler ancak kendi teknolojilerinin yetebileceği ürünleri taklit etmek için ticari sırları ele geçirmeye çalışırken, gelişmiş ülkeler küresel rekabette öne geçmek amacıyla daha yüksek ve gelişmiş teknolojileri kullanarak fikri mülkiyet haklarını ele geçirmeye çalışmaktadır.

İstihbarat örgütleri tarafından ekonomik/endüstriyel casusluk faaliyetinde bulunulması beraberinde bazı sorunları da gündeme getirmektedir. Örneğin

TASNİF DIŐI

istihbaratın hangi řirketlerin lehine kullanılacağı sorusu bařlı bařına bir meseledir. Eęer istihbarat örgütlerinin imkânları ulusal sanayii desteklemek maksadıyla kullanılacaksa kuřkusuz bazı řirketler aynı alanda ülke içinde faaliyet gösteren dięer rakiplerine göre bu durumdan daha fazla faydalanacaktır. Bu durum devlet içinde sadece rüşvete deęil beraberinde farklı yolsuzluk türlerine de neden olabilir. Gittikçe siyasileřen bir çevrede řirketler, istihbarat örgütlerinin yönetim kademesinde bulunan bürokratların desteęini kazanma uğruna yasa dıřı (rüşvet, pahalı hediye vb.) veya etięe aykırı (emeklilik durumunda řirkette yüksek ücretli görev vaadi vb.) yollara başvurabilirler. Zira řirketler açısından peřinde oldukları bilgi milyonlarca hatta milyarlarca dolar deęerinde olabilir. Bilgiyi elde edecek řirketler çok büyük kârlara sahip olacakları halde bundan mahrum kalanlar pazarda dezavantajlı konuma düşecektir. Bunun da ötesinde istihbarat örgütlerinin desteęini alan řirketler, küresel pazardaki rekabet yeteneęinden ziyade siyasi etki gücüne dayanmaya başlayacaktır. İstihbarat örgütleri ile řirketler arasında meydana gelebilecek bu tarz bir ilişkinin kötüye kullanılma ihtimali oldukça açıktır (Kobler, 1992).

f. Endüstriyel Casusluęun Ekonomiye Olan Etkisi

Devletler seviyesinde bir ülkenin rekabet edebilme kabiliyeti üretim seviyesi ile ilgilidir. Devletin temel görevi vatandaşlarına yüksek yařam standartları sunmaktır. Bununla birlikte řirketlerin yüksek oranda ve kaliteli üretim yapmaları da refah seviyesini etkilemektedir. Sürdürülebilir üretim artıřı, sürekli kendisini güncelleyen bir ekonomi ile mümkün olur. Bu yüzden řirketlerin var olan endüstri dallarında üretimlerini arttırabilmeleri; üretim kalitesini arttırmasına, üretim tekniklerini geliřtirmesine, yeni özellikler ekleyebilmesine ve üretim etkinlięini yükseltmesine baęlıdır (Porter, 1990, s.76). Günümüzde řirketlerin sahip oldukları ekonomik deęer büyük ölçüde geliřtirdikleri fikri mülkiyete dayanmaktadır. Örneęin ASIS'in 1999 yılında yapmış olduęu arařtırmaya göre ABD řirketlerinin pazar deęerinin %70'i ticari sır ve fikri mülkiyetlerden oluşmaktadır (Fitzpatrick, DuLilo ve Burke, 2004, s.57). Fikri mülkiyet haklarını kaybetmeleri halinde devletlerin ve řirketlerin uğrayacağı zararlar;

- Ülke ekonomisine ait varlıkların deęerinin azalması,
- Potansiyel alıcılarla yapılacak ticaretin bozulması,
- Ekonomik istikrarın sekteye uğraması,
- Yenilik ruhunun zarar görmesi,
- Güven bunalımı nedeniyle devletlerarası askeri ittifak ve ticari birliklerde zayıflama (Danielson, 2009, s.507).

TASNİF DIŞI

- Boşa giden ARGE harcamaları,
- Rekabet avantajının kaybı,
- Pazar liderliğinin yitirilmesi,
- Taklit ürünlerinin piyasaya sürülmesi,
- Marka güvenilirliğinin zedelenmesi, şeklinde sıralanabilir. Bununla birlikte işletmenin uğradığı zarar nedeniyle çalışanların işten çıkarılmaları veya batma riski gibi durumlar da karşılaşılabilecek tehditler arasındadır (Syngress, 2009, s.87-88).

Gerek bilgi elde etme gerekse işletmeye zarar verme amacıyla yapılan zararlı yazılım saldırısının muhtemel zararı ise aşağıdaki hususlardan oluşmaktadır.

- Hedef işletmenin bilgisayar sistemlerinin uğradığı hasar,
- Hasarın giderilmesi, düzeltilmesi ve yeniden çalışır hale getirilmesinin maliyeti,
- Hedef işletmedeki çalışanların verimliliğinde azalma,
- İşletmenin müşteri hizmetleri veya üretim sürecinde yaşanan gecikmeler,
- İşletmenin bulunduğu bölgenin ekonomisinde meydana gelebilecek olumsuz etkiler,
- İşletmenin müşterilerinin bulunduğu bölgenin ekonomisinde meydana gelebilecek olumsuz etkiler,
- İşletmeye yatırım yapan kişilere yönelik olumsuz etki,
- İşletme, müşteri ve yatırımcıların bulunduğu ulusal ekonominin uğrayacağı zarar (Stanley, 2010, s.134).

Endüstriyel casusluğun en etkili olduğu alan olarak, ileri teknoloji içeren ürünlerin üretildiği sektörler gösterilmektedir. Daha önceden piyasaya sürülmemiş, bilinmeyen bir ürünle ilgili kayıplar şirketler açısından çok daha yıkıcı sonuçlar doğurabilmektedir. Rekabet avantajını yitiren firma, pazar içinde daha ucuz veya gelişmiş bir ürünle mücadele etmek zorunda kalabilir. Finans ve hizmet sektöründe ise müşteri listeleri ve müşterilere ait çeşitli ticari veriler endüstriyel casusluğa hedef olabilmektedir. Şirket birleşmeleri, satın alma planları ve stratejik iş planları endüstrinin her seviyesinde takip edilmektedir (Fink, 2002, s.197).

Güvenlik alanında çalışmalar yapan ASIS'in araştırmalarına göre endüstriyel/ekonomik casusluğun ABD'ye verdiği zararın bedeli 1998 yılında 250 milyon dolar civarındadır (Fink, 2002, 193). FBI ile koordineli olarak çalışan Bilgisayar Güvenlik Enstitüsü (Computer Security Institute-CSI)'nin Amerikan şirketleri üzerinde yaptığı araştırmaya göre, 2002-2005 yılları arasında irtibata geçilen şirketlerin %90'ı son 12 ay içerisinde güvenlik ihlali ile karşılaştıklarını

TASNİF DIŞI

belirtirken, %80'i ise bu durumdan dolayı mali kayba uğradıklarını ifade etmiştir. Araştırmaya göre 2002 yılında bu şirketlerin uğradıkları toplam zarar 450 milyon dolar civarındadır. FBI tarafından 2006 yılında hazırlanan ve 2000 katılımcının yer aldığı bilişim suçları ile ilgili daha kapsamlı başka bir araştırmaya göre ise bu tür suçların Amerikan iş dünyasına toplam maliyeti yıllık 67 milyar dolar civarındadır (Boulanger, 2010, s.27).

1996 yılında FBI, 23 devletin karıştığı yaklaşık 800 endüstriyel/ekonomik casusluk olayını araştırıyordu. Uluslararası Ticaret Komisyonunun (International Trade Commission-ITC) tahminlerine göre sadece 1987 yılında ABD sanayiinin kaybı 23,8 milyar dolar civarındaydı. ABD'li yetkililerin tahminine göre ise zarar 450.000 kişinin iş kaybına bedeldi (Internet Archive, 1996).

İngiliz yetkililere göre, gerek endüstriyel casusluk gerekse ticari sırların çalınması maksadı ile yapılan saldırıların İngiliz ekonomisine maliyeti yıllık 34 milyar dolar civarındadır. Bu rakam, tasarım, formül, şirkete ait ticari sır gibi toplam mülkiyet haklarının değerinin %40'ından da fazladır (ONCIX, 2011, s. B-2).

Endüstriyel casusluğun ekonomiye olan etkisi ile ilgili araştırmalara bakıldığında birbirinden çok farklı sonuçlara ulaşıldığı görülmektedir. Hesaplamalarda standart bir yöntemin kullanılmaması, işletmelerin uğradıkları zararı çeşitli nedenlerle eksik ya da fazla göstermeleri veya marka güvenilirliği zedelenir endişesiyle hiç bildirmemeleri, kaybedilen ticari sırrın bugünkü ve gelecekteki gerçek değerinin ne olduğunun objektif olarak değerlendirilememesi meseleyi daha da güçleştirmektedir. Sahip olunan bir ticari sırrın ekonomik değerinin belirlenmesinde pazar, maliyet ve gelir yaklaşımı olmak üzere üç çeşit klasik yöntem uygulanmaktadır.

Pazar Yaklaşımı: Ticari sırrın değerinin belirlenmesinde kullanılması en zor olan yöntemdir. Değerlendirilmesi istenen benzer ürünlerin satışlarını mukayese eden pazar yaklaşımında, ticari sır içeren bir ürünün başka bir ürünle karşılaştırılması oldukça göreceli bir faaliyettir (Fink, 2002, s.230). Ayrıca patentlenmiş buluşlar tektir. Bu yüzden benzer bir buluşun bulunması da mümkün değildir (Poltorak ve Lerner, 2002, s.78). Bununla birlikte fikri mülkiyet içeren bir buluşun üretiminde sağlanan gelişme, daha önceden denenmemiş etkin organizasyonel yapı, başarısızlıkla sonuçlanan denemeler (negative know-how) gibi veriler de pazar yaklaşımında göz önüne alınmamaktadır (Halligan ve Weyand, 2006, s.19).

TASNİF DIŞI

Maliyet Yaklaşımı: Fink (2002, s.230)'e göre, ticari sırların değerlendirilmesi açısından daha uygun bir yöntemdir. Ticari sırrın oluşturulmasının ne kadar zaman aldığı, maliyeti gibi soruların cevabını araştırır. Bu yaklaşımda kullanılan yöntemler arasında tarihi maliyet ve yerine koyma maliyeti kullanılmaktadır. Tarihi maliyette, patentin oluşturulma sürecinde katlanılan gerçek maliyet hesaba alınır. Yerine koyma maliyetinde ise “aynı fayda ve fonksiyonu sağlayacak benzer bir patentin yeniden yaratılması ya da patentli buluşun yerine konması maliyetleri için, cari fiyatlardan gerekli toplam maliyetlerin belirlenmesi doğrultusunda hazırlanır” (Alper, 2011, s.160). Bu yaklaşımın olumsuz tarafları ise;

- Buluş için yapılan masraf ve buluşun değeri arasında ilişki kurmaması,
- İşletme giderleri ile patente yapılan yatırım arasındaki ayrımın zorluğu,
- Yerine koyma maliyetinde hesaplamanın sübjektif nitelik taşıması ve bazı patentlerin yerini başka bir buluşun alamayışdır (Scheffer ve Zieger, 2005, s.4).

Gelir Yaklaşımı: Ticari sırrın gelecekte getireceği kar üzerine odaklanan bir yaklaşımdır. Çeşitli ekonomik modeller kullanması nedeniyle pazar yaklaşımına göre daha tercih edilebilir bir uygulamadır (Fink, 2002, s.230). Gelir temelli yaklaşımda patentin değeri, “patentin belirli bir süre kullanılması sonucu gelecekte elde edilecek nakit akışlarının, uygun bir iskonto oranı üzerinden iskonto edilmiş bugünkü değerinden, patent ve ticarileştirme için yapılan maliyetlerin bugünkü değerinden düşürülmesi ile hesaplanır” (Alper, 2011, s.161). Gelir yaklaşımının gelecekteki kazanımları ve nakit akışlarını dikkate almak gibi olumlu tarafları olmakla birlikte;

- Gelecek nakit akışları tahmininin sübjektif olması,
- Pratikteki uygulamalarının sınırlı varsayımlara dayanması,
- İhtiyaç duyulan bilgilere her zaman ulaşılamaması, bu yöntemin eleştirilen yönleridir (Scheffer ve Zieger, 2005, s.5).

Halligan ve Weyand (2006,s.19)'a göre, gelecekteki nakit akışının net bugünkü değeri ticari sırların değerinin belirlenmesinde en etkin yöntemdir. Pazarda bulunmayan bir ürünle ilgili ticari sırrın değerinin hesaplanması bu yöntemle daha kolay olmaktadır. Endüstriyel/ekonomik casusluğun zararının tespitinde Amerikan mahkemeleri ölçüt olarak kayıp gelirleri baz almaktadır. Pazar durumu, kârlılık gibi öznel değerlendirmeleri içerse de diğer yöntemlere göre daha etkin hesaplama yöntemi olduğu ifade edilmektedir (ONCIX, 2011, s.4).

TASNİF DIŞI

Endüstriyel casusluğun şirketlere olan etkisini tespit etmek maksadıyla Samlı ve Jacobs, hasar kontrol stratejisinin uygulanması gerektiğini belirtmektedir. Bu yaklaşım kendi içerisinde; önleyici tedbirler, hassasiyet değerlendirmesi, olasılık planları, tespit ve yıkımı kontrol altına almak üzere beş aşamadan oluşmaktadır ve sahip oldukları risk ile maliyet bakımından değerlendirilmektedir (Samlı ve Jacobs, 2003, s.105).

Önleyici Tedbirler: Bir sonraki başlıkta değerlendirilecek olan endüstriyel casusluğa karşı alınması gereken tedbirler bu konuda örnek olarak gösterilebilir. Ancak bu tedbirlerin bir bütün olarak ele alınmaları gerekmektedir.

Hassasiyet değerlendirmesi: Bu aşamada işletmenin hangi seviyede endüstriyel casusluğa hedef olabileceğinin değerlendirilmesi yapılır. Farklı iş kolları değişik seviyelerde veri toplama faaliyetine hedef olabilir. Bu nedenle alınacak tedbirler öncelikle daha hassas alanlara yönlendirilmelidir.

Olasılık Planları: Endüstriyel casusluk olaylarına karşı uyarı sistemi geliştiren bir işletmenin böyle bir durumla karşılaşması halinde seçeceği hal tarzlarına yönelik planlardır. Ticari sırrın kaybına yönelik olarak farklı ürün geliştirme ve pazarlama planları oluşturulabileceği gibi endüstriyel casusu aldatmaya veya yakalamaya yönelik planlar da yapılabilir (Samlı ve Jacobs, 2003, s.107).

Tespit: Endüstriyel casuslukla mücadelede en kritik aşama ticari sırların ele geçirildiğinin tespit edilmesidir. Ekonomik değeri yüksek bilginin rakiplerin eline hiç geçmemesi daha önemli olmakla birlikte kaybın farkında dahi olmama işletme açısından geri dönülemez zararlara yol açabilir. Tespit ne kadar erken yapılırsa şirket açısından o kadar faydalı olur. Tespit üretim ya da süreç döngüsünün herhangi bir aşamasında gerçekleşebilir. Örneğin şirket, bilgi kaybının ürünün fikren tasarlandığı aşamada gerçekleştiğini tespit ederse önceden tedbir alarak, yeni çözümler üretebilir, geliştirebilir. Ancak tamamlanmış veya üretimine başlanmış bir ürün hakkındaki ticari sırların ele geçirilmesi sonucu şirketin pazarda rekabet gücünü yitirmesi durumunda önleyici tedbirlerden ziyade yıkımı önleyici stratejilerinin uygulanması gerekmektedir.

Zararı Kontrol Altına Almak: Endüstriyel casusluk sonucu kaybedilen bilginin vereceği zarara yönelik tedbirleri kapsar (Samlı ve Jacobs, 2003, s.105-108).

Bir işletme kendi sistemlerine yapılan sızıntının veya müdahalenin aylarca farkında olamayabilir. Pazar payının küçülmesini, rakibinin kendisinden çaldığı bilgilerle geliştirdiği ürünlerden kaynaklandığını da değerlendiremeyebilir. Böyle durumlar meydana gelen zararın tespitini oldukça değişken kılmaktadır (Danielson, 2009, s.506). Ayrıca yapılan çeşitli çalışmalar²⁸ da endüstriyel casusluğa hedef olduğu duyulan şirketlerin borsadaki hisse senedi değerlerinin düştüğünü göstermektedir. Bu nedenle endüstriyel casusluğun ekonomiye olan etkisi konusunda pek çok rakam ileri sürülse de gerçek zararın ne kadar olduğunu tahmin etmek son derece güçtür. İşletme tarafından aşağıdaki soruların cevabının bulunması son derece önemlidir:

- Endüstriyel casusluk olaylarının ne kadarlık kısmı bilinmektedir?
- Bilinen ticari sır kayıplarının gerçek değeri nedir?
- Bilinmeyen kayıpların değeri nedir? (Bunu öğrenmek muhtemelen hiçbir zaman mümkün olmayacaktır) (Roche, 2007, s.24).

Yukarıdaki soruların cevapları objektif bir şekilde değerlendirildiği takdirde endüstriyel casusluğun işletmeye verdiği zarar hesaplanabilir.

g. Endüstriyel Casusluğa Karşı Alınması Gereken Tedbirler

İşletmenin sahip olduğu ticari sırların ekonomik değeri ile bu sırlara yönelik risk ve tehditlerin belirlenmesi, alınması gereken tedbirlerin kapsamını belirleyen şartlardır. Sonuç olarak güvenliğin de bir maliyeti bulunmaktadır. Şüphesiz elde edilecek güvenlik ile ticari sırrın değeri arasında bir tutarlılık bulunması gerekmektedir.

Endüstriyel/ekonomik casusluğun işletmelerle birlikte, işletmelerin ait olduğu ülke ekonomisine de zarar vermesi bu konuda alınması gereken tedbirlerin sadece işletmeler tarafında değil ulusal kuruluşlarca da alınmasını zorunlu kılmaktadır. Bu nedenle alınacak tedbirleri işletme ve devlet seviyesi olmak üzere iki gruba ayırmak mümkündür.

²⁸ Bkz. Carr, C. ve Gorman, L. (2001). The Revictimization of Companies by the Stock Market who Report Trade Secret Theft under the Economic Espionage. *Business Lawyer*, vol. 57, no. 1 ile Campbell K. , Gordon, L.A. , Loeb M.P. ve Zhou, L. (2003). The economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence from the Stock Market. *Journal of Computer Security*, vol.11, issue.3, s.431–448.

(1) İşletme Seviyesinde Alınması Gereken Tedbirler²⁹

Küresel rekabet ortamında endüstriyel/ekonomik casusluk ile rekabet istihbaratının devreye girmesi, pazarlama stratejilerini de daha karmaşık hale getirmiştir. Güvenlik konusundaki belirsizliğin giderek arttığı bir dönemde endüstriyel/ekonomik casusluk fikri mülkiyete yönelik ciddi bir tehdit olarak yer almaktadır. Teknolojinin gelişim ve maliyetindeki artış ile rekabet istihbaratının yasal veya yasa dışı kullanımı ticari sırların ele geçirilme riskini de gün geçtikçe artırmaktadır (Richardson ve Luchsinger, s.44).

CSI/FBI'nın 2005 yılı araştırmasına katılan 700 bilgisayar güvenliği uzmanından 465'ine göre organizasyonlar aşağıdaki sebeplerden dolayı sistemlerine yapılan müdahaleleri güvenlik birimlerine bildirmek istememektedirler:

- Kamuda oluşacak yargının hisse senetlerini ve kurumun imajını olumsuz yönde etkilemesi %43,
- Rakiplerin bu durumdan avantaj sağlaması %33,
- Güvenlik güçlerinin ilgisiz olması %16 (Gordon, Loeb, Lucyshyn ve Richardson, 2005, s.20).

ASIS'in Fortune 1000 şirketleri üzerinde yaptığı araştırmaya göre ticari sır hırsızlığının;

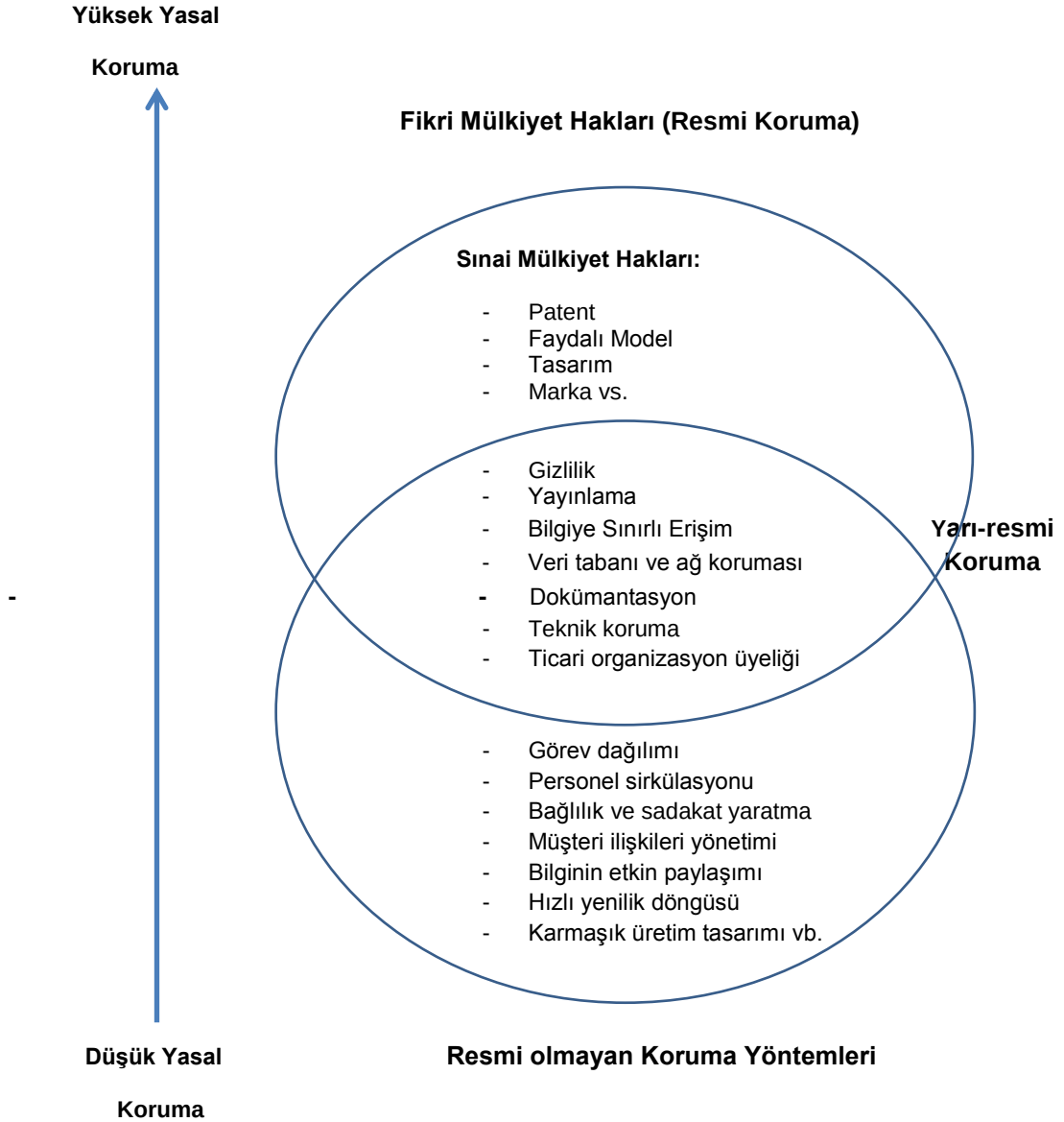
- %30'u çalışanlar,
- %28'i eski personel,
- %22'si bayiiler, sözleşmeli çalışanlar, orijinal parça üreticileri gibi çalışanlar vasıtası ile dışarıdan işletmeye giriş imkânı bulanlar,
- %20'sini de ülke içi ve yabancı rakipler ile yabancı hükümetler ve onlara bağlı çeşitli kuruluşlar oluşturmaktadır (Fink, 2002, s.266).

İşletmelerin ticari değeri olan bilgi varlıklarını koruma konusunda ilk akla gelen üçüncü bölümde de detaylı olarak anlatılan patent ve tasarım gibi tescil edilen fikri mülkiyet haklarıdır. Patent sahibi olma bir işletmeyi pazarda tanınır kıldığı gibi yeni ürünün pazar değerini de artırmaktadır. Patent koruması, rakiplere karşı ürünün korunmasında da önemli etkiye sahiptir (Paallysaho ve Kuusisto, 2011, s.63). Ancak küçük ve orta ölçekli işletmelerin maliyet, süreç, ürün ömrünün

²⁹ Bilgi güvenliği konusu oldukça geniş bir araştırma konusu olmakla birlikte, işletme seviyesinde asgari olarak ISO'nun belirlediği standartlar uygulanmalıdır. Çalışmanın kapsamı nedeniyle bilgi güvenliği konusu temel seviyede ele alınmıştır.

TASNİF DIŞI

kısalığı veya ürünün tescil için gerekli nitelikleri taşınamaması gibi nedenlerden dolayı resmi olmayan koruma yöntemlerini tercih ettikleri gözlemlenmektedir.



Şekil-8: Yasal Durumlarına Göre Fikri Mülkiyet Hakları Koruma Yöntemleri

Kaynak: (Paallysaho ve Kuusisto, 2011, s.64)

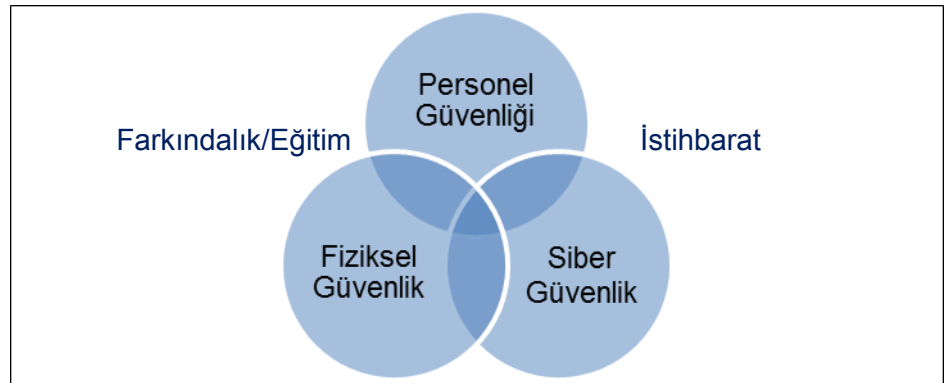
Yukarıdaki şekilde (Şekil-8) yasal durumlarına göre koruma yöntemleri yer almaktadır. Patent, faydalı model ve tasarım gibi tescili yapılan fikri mülkiyet hakları, ekonomik değeri olan koruma şartlarını yerine getiren ürünlere yasal koruma sağlamaktadır. Aynı zamanda uluslararası kuruluşlara (EPC, PCT) da tescili yapılan patentlerin ihlali, işletmelere tazminat talebi gibi haklar da sağlamaktadır. Yarı-resmi koruma ise yasal sistem belirtilen koruma sistemini destekliyorsa var olabilir. Örneğin ABD hukuk sisteminde ticari sırrın unsurlarından biri olan “gizliliğin” sağlanabilmesi için hassas bilgilerin fiziksel olarak korunması gerekmektedir. Yasal

TASNİF DIŐI

olmayan koruma yöntemleri ise kanuni açıdan hak doğurmayan ancak uygulamaya dayalı yöntemlerdir (Paallysaho ve Kuusisto, 2011, s.63-64). Örnek vermek gerekirse, hızlı yenilik döngüsü ile yeni ürünlerin kısa aralıklarla piyasaya sürülmesi endüstriyel casusluğu doğrudan engellememekle birlikte bu konuda rakiplerin yapacağı faaliyetleri kısa sürede boşa çıkaran etkin bir yöntemdir. Özellikle yazılım ve mobil iletişim sektörü gibi gelişmelerin süratli yaşandığı sektörlerde işletmeye rekabet avantajı sağlayan ana unsurdur. Ürünün pazardaki rakiplerce taklit edilmesini de engeller (Paallysaho ve Kuusisto, 2011, s.72).

Yıllarca üzerinde çalışılmış ve yatırım yapılmış bir formülün ya da prototipin rakiplerin eline geçmesi özellikle ileri teknoloji alanında çalışan şirketler pazarda rekabet avantajını kaybederek batma tehlikesiyle karşılaşabilirler. Böyle bir durumla karşılaşan işletmelere zararı kontrol altına alabilmeleri adına Samlı ve Jacobs çeşitli hareket tarzları önermektedir.

- Anında Karşılık Vermek: Ticari sırrı ele geçiren rakiplerden önce ürünü en kısa sürede piyasaya sürmek.
- Endüstriyel Casusu Satın Almak: Ticari sırrı çalmaya çalışan kişinin satın alınarak hedef ürünü koruma altına almak. Bu yöntem etik dışı gözükse de benzer şekilde bilişim suçu işleyen bazı bilgisayar korsanlarının da istihbarat örgütlerince kullanılmaları bilinen bir durumdur.
- Projeyi Sona Erdirmek: En yüksek maliyeti içeren bu yöntemde, ticari sırrının çalındığını fark eden şirket ürün üzerinde yapacağı bütün araştırma faaliyetleri ile yatırıma son vermeyi tercih edebilir (Samli ve Jacobs, 2003, s.108-109). Burada güdülen amaç her ne kadar endüstriyel casusları amaçlarından yoksun bırakmak gibi gözükse de işletmenin pazar dışında kalması her hâlükârda rakiplerinin çıkarına olacaktır.



Şekil-9: İşletmelerde Bilgi Güvenliği

Kaynak:Syngress(2009). Securing Intellectual Property. Protecting Trade Secrets and Other Information Assets'den alınarak düzenlenmiştir.

TASNİF DIŞI

İşletmelerde endüstriyel casusluğa karşı alınması gereken tedbirlerin temelini bilgi güvenliğine yönelik önlemler almaktadır (Şekil-9). Bu konudaki önlemler de personel güvenliği, fiziksel güvenlik, siber güvenlik olmak üzere üç ana başlık etrafında toplanmaktadır. Bununla birlikte personele verilen eğitim düzeyi ile yaratılan farkındalık durumu ve bu konudaki dış tehditleri tespit etmeye yönelik milli istihbarat kuruluşlarınca da sağlanan istihbarat desteğinin de tamamlayıcı bir etki etki sağlayacağı değerlendirilmektedir.

(a) Personel Güvenliği

Yapılan araştırmalar endüstriyel casusluk olaylarında personelin bireysel hata payının (sızdırma, phishing vb.) oldukça büyük olduğunu göstermektedir. Bu doğrultuda,

- “Bilmesi gereken (need to know) prensibi” kapsamında sınırlı sayıda yetkili kişinin hassas bilgilere erişmesi,
- Çalışanlarda bağlılık ve sadakat duygusu yaratma,
- Görev dağılımı,
- Personel rotasyonu (Paallysaho ve Kuusisto, 2011, s.69-70),
- İşe alınmadan önce çalışanların özgeçmişlerinin incelenmesi,
- Belirli periyotlarla mali durumlarının kontrol edilmesi (Fitzpatrick, DuLilo ve Burke, 2004, s.62), (istihbarat örgütlerince istismar edilebilecek aşırı borçlanma veya mal varlığında ani yükselme gibi durumlar)
- Personel tarafından ticari sırların sosyal medyada paylaşılmasını önlemek amacıyla eğitim programları düzenlenmesi (Ulsch ve Sullivan, 2012),
- İşletmeye ait ticari sırlar hakkında çalışanlarla gizlilik anlaşması yapılması, alınabilecek başlıca tedbirler arasındadır.

(b) Fiziksel Güvenlik

Fiziki güvenlik tedbirleri, işletmenin sahip olduğu tesisleri korumak maksadıyla alınan tedbirleri kapsar. Fiziksel güvenlik tedbirlerinin bütünsel bir anlayışla ele alınması gerekmektedir. Örnek vermek gerekirse bilgisayar ve ağların fiziksel açıdan güvenliği kesinlikle göz ardı edilmeyecek bir durumdur. Bilgisayar ve ağ sistemlerinin fiziksel olarak korunmaması, ileri teknoloji içeren güvenlik çözümlerini (şifreleme, anti-virüs programları, güvenlik duvarları vs.) de geçersiz kılar. Ekonomik açıdan önemli bilgilerin bulunduğu alanlara dinleme cihazı, klavye kaydediciler yerleştirilebilir; sistemdeki veriler, çalınabilir, değiştirilebilir ya da sisteme zararlı yazılımlar yüklenebilir (Stanley, 2010, s.118). İşletmenin fiziksel güvenliğinin sağlanması konusunda alınabilecek tedbirlerden bazıları aşağıda yer almaktadır;

TASNİF DIŐI

- İőletmeye ait tesisin güvenlik görevlilerince korunması,
- Kritik bölgelerin güvenlik kamerası ile görüntülenmesi,
- Alarm sistemleri,
- Üretim yerleri ve laboratuvarların dışarıdan gözetlenmemesi için fiziki tedbir alma,
- Dışarıdan gelen ziyaretçilerin giriş-çıkışları kontrol edilerek, işletme içerisinde ziyaretçi kartı takmalarının zorunlu kılması,
- Tüm personelin işletme içerisinde görünür bir isimlik taşıması,
- Hassas bilgilerin bulunduğu yerlere giriş için sadece yetkili personele izin verilmesi ve ziyaretçilerin bu gibi yerlerden uzak tutulması (Halligan ve Weyand, 2006, s.23),
- Hassas belgelerin üzerine gizlilik derecesini gösteren damgalar veya işaretler konulması, kilit altında tutulması veya dijital ortamda şifrelenerek saklanması (Dexter ve Beckett-McWalter, 2006, s.3),
- İşletme içerisindeki personelin ikaz edilerek gizli belgelerin ilgisiz yerlerde bulunmasının engellenmesi, görüldüğü takdirde uygulanması gereken hareket tarzlarının neler olduğunun tüm personel tarafından bilinmesi,
- Her türlü evrak ve belgenin çöpe atılmadan imha edilmesi (kağıt kıyma makinası veya yakma),
- Kişisel harici bellek vb. depolama aygıtlarının işletme içerisine sokulmaması,
- Hassas veri barındıran bilgisayarların internet ile bağlantısının kesilmesi.

(c) Siber Güvenlik

Carnegie Mellon Üniversitesi'nde bilgisayarlara yönelik müdahaleleri araştırmak üzere kurulan birime (CERT) göre, bilgisayar sistemlerine yapılan ihlaller her geçen yıl katlanarak artmaktadır. 2001 yılında 52.000 güvenlik ihlali meydana gelirken bir önceki yıla göre %140 oranında bir artış meydana gelmiştir. F-Secure'nin 2009 raporuna göre dünya genelinde 9.000.000 bilgisayara tek tip de olsa zararlı yazılım bulaşmıştır (Boulanger, 2010, s.27).

TASNİF DIŞI

Gizli ve ekonomik değeri olan bilgiye erişim konusunda işletmeleri alması gereken temel tedbirler bulunmaktadır. Ancak teknolojinin gelişim çizgisine paralel olarak bu güvenlik önlemleri sürekli güncellenmeli ve çeşitlendirilmelidir.

- Bilgisayar erişim koruması: Önemli bilgilerin bulunduğu bilgisayarlara ve ağlara şifre ile girilmesi zaruret halini gelmiştir. Bilgisayar korsanlarının saldırılarına karşı bu şifreler belirli sürelerle güncellenmeli ve kolaylıkla kırılmayacak derecede karmaşık olmalıdır. Aynı zamanda belirli sayıda sınırlı erişim sağlamak maksadıyla parmak izi ya da retina tarama sistemlerinden de faydalanılabilir. Örneğin LG firmasında araştırmacıların üzerinde çalışmadıkları projelerle ilgili inceleme yapmaları yasaktır (Roche, s.71).

- Sistem Koruması: İnternet ve diğer ağlara bağlı olan bilgisayarların güvenlik duvarı ve sızma tespit sistemleri tarafından korunmaları gerekmektedir. Bununla birlikte sistemdeki hassas noktaların tespit edilmesi maksadıyla işletmeler kendi sistemlerine saldırı tatbikatları yaptırabilirler.

- Şifreli veri akışı ve depolama: Verilerin şifrelenerek kayıtlı tutulmaları daha güvende olmalarını sağlar. Aynı zamanda ticari sırların korunabilmeleri açısından alınan bu tarz önlemler işletme sahiplerinin gelecekte hak iddia etmeleri açısından da önemlidir. Sadece kaydedilmiş veriler değil internet ya da diğer sistemler üzerinden aktarılan veriler de şifrelenerek gönderilebilir (Syngress, 2009, s.13).

ABD’de Bilgisayar Güvenlik Enstitüsü (Computer Security Institute-CSI) ile FBI’nın şirketler, kamu kurumları, finansal kuruluşlar, sağlık kurumları ve üniversitelerde görev yapan 700 bilgisayar güvenlik uzmanından derlediği 2005 yılı araştırmasına³⁰ göre kurumların %25’inin siber tehditlere karşı sigortası bulunurken %75’i bu korumadan yoksundur. Aynı çalışmada en büyük zararın virüsler, bilgiye yetkisiz erişim ile fikri mülkiyet haklarının çalınmasında meydana geldiği belirtilmektedir (Gordon, Loeb, Lucyshyn ve Richardson, 2005, s.15).

(ç) Farkındalık/Eğitim:

Endüstriyel casusluğun engellenmesi konusunda en önemli husus işletme içerisinde çalışanlara sürekli eğitim verilerek bu konuda karşılaşılabilecek sorunlar karşısında bir farkındalık yaratmaktır. Aksi takdirde bunun maliyeti işletme açısından çok büyük olabilir. Örneğin Ağustos 2002 yılında Niku Şirketi sunucu kayıtlarında, rakip Business Engine Şirketi’ne ait olduğu tespit edilen bir IP adresinden Niku’ya ait

³⁰ 2005 CSI/FBI Computer Crime and Security Survey.

TASNİF DIŐI

őifre ile őirketin ađ sistemine 6.000'den fazla giriő yapıldıđı tespit edilmiőti. Bu giriőler esnasında Niku'nun fiyatlandırma, satıő bilgileri, potansiyel mőőteri listelerinin bulunduđu 1000 kadar belge de sisteme girenler tarafından indirilmiőti. Ancak FBI tarafından yapılan araőtırma, Ekim 2001 yılından itibaren 15 farklı hesap ve őifre ile Niku'nun kendi internet sistemindeki hassas bilgilerin bulunduđu verilere dıőarıdan eriőildiđini ortaya ıkarmıőtı (Brenner ve Crescenzi, 2006, s.415-416). Bu nedenle sisteme verilen zararın baőlangıő zamanını ve hasarın ne olduđunu tespit etmek son derece nemlidir.

alıőanlar, gerekenden daha fazla bilginin mőőterilere, danıőmanlara ve hatta iő arkadaőlarına aıklanmaması gerektiđi konusunda eđitilmelidirler. Bununla birlikte ticari fuarlardaki sunumlarında ve satıő konuőmalarında hangi bilgileri kullanacakları veya kullanmayacakları konusunda ynlendirilmelidir. Satıő materyalleri, web siteleri ve teknik makaleler ise yayınlanmadan nce uzman bir kurul (rneđin fikri mőlkiyet kurulu) tarafından gzden geirilmelidir.

İőletme tarafından alıőanların ticari sırlar konusundaki sorularına ve sorunlarına yardımcı olacak bir bađlantı noktasının kurulması son derece faydalı olacaktır. Bu birim tarafından, alıőanların aőađıdakilere benzer sorularının cevaplanması son derece nemlidir.

- Hangi bilgilerin iőletme aısından korunması gereken ticari sırlar olduđu,
- İőletme dıőından yabancı kiőilerce veya iőletme iindeki konu ile ilgisiz personel tarafından yapılabilecek ticari sırlara ynelik isteklerde, alıőanların nasıl bir tutum takınması gerektiđi,
- İőletmeden ayrılmıő eski personelin ticari sırlara ynelik bilgi taleplerinde, alıőanların ne őekilde hareket etmesi gerektiđi, vb.

Kurumsal farkındalık yaratılması amacıyla őüpheli olaylarla karőılaőtıđını dőőnen alıőanlar iőletme ierisinde kiminle ya da hangi birimle irtibata gemeleri gerektiđini bilmelidirler (Dexter ve Beckett-McWalter, 2006, s.3).

Alınan tedbirlerin yeterliđini lmek maksadıyla eőitli zamanlarda yapılan gzlem ve tatbikatların da kurum ierisindeki farkındalıđı canlı tutacađı deđerlendirilmektedir.

(d) Rekabet İstihbaratı

İőletmelerin aynı alanda rekabet halinde oldukları zellikle ok uluslu őirketler hakkında rekabet istihbaratı toplamaları kaınılmaz olmuőtur. Rakiplerin durumu kadar, iőletmenin elinde bulunan ticari sırlara kimlerin eriőmek isteyeceđinin bilgisi

TASNİF DIŞI

de alınacak tedbirlerin etkinliği açısından son derece önemlidir (Burgess ve Power, 2008, s.94). Rekabet istihbaratı konusu önceki bölümlerde detaylı olarak yer verilmiştir.

(2) Devlet Seviyesinde Alınması Gereken Tedbirler

Endüstriyel casusluğa karşı şirketler bazında alınan tedbirler son derece önemli olmakla birlikte, belirli bir devlet tarafından yürütülen bilgi toplama faaliyetine karşı işletmenin kendi imkânları ile karşı koyması oldukça zordur. Çünkü hiçbir işletme kendi ticari sırlarının peşine düşen bir devletin sahip olduğu kaynaklarla tek başına mücadele edemez (Danielson, 2009, s.523). Örnek vermek gerekirse “Stuxnet” virüsü gibi “APT” saldırısına veya sinyal istihbaratı ekipmanı kullanılarak yapılan dinleme faaliyetine karşı bir işletmenin kendisini koruması mümkün değildir.

Fikri mülkiyet haklarının ve ticari sırların korunması sadece işletmelerin sorumlu olduğu bir alan değildir. Devletlerin de ekonomiyi destekleyen ve istihdam sağlayan özel sektörün gelişimini koruma adına ulusal güvenlik çerçevesinde endüstriyel casusluğa önleyici tedbirler alması gerekmektedir.

Endüstriyel casusluğun ulusal ekonomiye vermiş oldukları zarar istihbarat örgütlerini de bu konuda tedbire yöneltmiştir. Örneğin ABD’de FBI tarafından 1993-1994 yıllarında 20.000 şirkette çalışan toplam 250.000 kişiye endüstriyel/ekonomik casusluğa karşı alınması gereken tedbirler hakkında brifing verilmiştir. Çalışanlara ek olarak akademik enstitüler, laboratuvarlar ve yerel yönetimler de bilgilendirilmektedir (Moisier, 2001, s.428). Türkiye’de de bu alanda Milli İstihbarat Teşkilatı’nın hizmet verdiği görülmektedir. MİT’in internet sitesinde yer alan bilgilere göre;

“ (...) stratejik kurum/kuruluşlar ile özel firmalarda görevli kritik personel nezdinde farkındalık oluşturulması ve mevcut farkındalığın artırılması amacıyla, istihbarata karşı koyma (İKK) ve koruyucu güvenlik başta olmak üzere endüstriyel güvenlik, ulusal bilgi güvenliği ve siber tehditlere karşı koyma konularını içeren İKK ve Koruyucu Güvenlik Brifingleri” düzenlenmektedir.

Ayrıca yaklaşık 200 kişiye brifing verildiği ifade edilen internet sitesinde “kritik bilginin korunması doğrultusunda yerli Savunma Sanayiinin gelişimine uluslararası rekabet gücünün artırılmasına katkı sağlanması amaçlandığı” ifade edilmektedir (MİT, 2012).

Bilgi güvenliği konusunda hizmet veren diğer bir kurum da TÜBİTAK’tır. TÜBİTAK bünyesinde yer alan Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma

TASNİF DIŞI

Merkezi (BİLGEM)'e bağlı, Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü (UEKAE) ve Bilişim Teknolojileri Enstitüsü (BTE) doğrudan endüstriyel/ekonomik casusluğa karşı tedbirleri içermese de “güvenlik” ve “bilişim teknolojileri” konusunda kamu sektörü ile özel sektörü destekleyen proje ve çalışmalarda bulunmaktadır. Her iki enstitünün bugüne kadar gerçekleştirdikleri proje ve faaliyet alanları arasında; elektronik, elektromanyetik, optik, akustik sistemler, kriptoloji, elektronik harp, sensör sistemleri, benzetim ve modelleme, platform entegrasyon teknolojileri, yazılım ve yazılım mimarileri, doğrulama ve geçerleme teknikleri, veri madenciliği, güvenlik kritik yazılım geliştirme, bilgi ve ağ teknolojileri, bilgi ve ağ güvenliği bulunmaktadır (TÜBİTAK, 2012b).

ABD’de endüstriyel/ekonomik casusluğa karşı önlemler konusunda görev yapan Amerikan Ulusal Karşı İstihbarat İcra Dairesi (Office of National Counterintelligence Executive-ONCIX), her yıl bu konuda ABD’deki diğer 13 kurum ve kuruluşla birlikte ortak rapor hazırlamaktadır (ONCIX, 2011, s.iv) . Kanaatimizce, ülke seviyesinde kurumsal işbirliği gerektiren böyle bir tehdide karşı ABD’de bu sayıdaki kuruluş ve istihbarat örgütünün endüstriyel casusluğa karşı katkıda bulunduğu bir ortamda, Türkiye’de bu konuda tedbir alması gereken kamu kurum, kuruluşları ile özel sektörün daha koordineli çalışması gerekmektedir.

ğ. Endüstriyel Casusluğun Önlenmesinde Karşılaşılan Zorluklar

Uluslararası alanda endüstriyel casusluğu engelleyememenin çeşitli nedenleri bulunmaktadır. Bunlardan ilki uluslararası hukukta bu konuda kesin bir hüküm bulunmaması ile ilgilidir. Pek çok devletin istihbarat toplama faaliyetinde bulunması yapılan eylemin uluslararası hukuku çok da ihlal etmediği gibi bir algının doğmasına neden olmaktadır. Diğer bir husus ise ticari sırlarla ilgili anlaşmaların bu konudaki yetersizliğidir. Ticari sırların korunması ile ilgili Paris Sözleşmesinden TRIPs Anlaşmasına değin pek çok anlaşma bulunmasına rağmen devlet destekli endüstriyel/ekonomik casuslukla ilgili açık bir hüküm veya caydırıcı yaptırımlar bulunmamaktadır (Blood, 2002, s.233-235). Örneğin sınai mülkiyet haklarının anayasası olarak kabul edilen Paris Sözleşmesinin 10’uncu maddesinde “*Ticari ve sınai konularda dürüst uygulamalara aykırı bir rekabet davranışı, haksız rekabet fiilini oluşturur*” denilmektedir. Ancak fikri mülkiyet içeren bilginin çalınmasının bu madde kapsamında ele alınıp alınmayacağı açıkça belirtilmemiştir. Yüz yıldan fazla bir zamandır yürürlükte olan bu sözleşme endüstriyel casusluğa karşı yeterli koruma sağlamamaktadır. Fikri mülkiyet haklarının korunmasında önde gelen anlaşmalardan biri olan ve asgari standartları belirleyen TRIPs Sözleşmesinin

TASNİF DIŞI

39(1)'uncu maddesinde “*Üyeler, (...) haksız rekabete karşı etkin koruma sağlarlarken, açıklanmamış bilgileri (...) ve hükümetlere veya hükümet kuruluşlarına sunulmuş verileri (...) koruyacaklardır*” denilmektedir. Bu madde yabancı devletlerin faydalı bilgi bulma amacıyla hükümet kayıtlarını incelemelerini engellemektedir. Ancak TRIPs Sözleşmesinde ekonomik/endüstriyel casusluk suçu açık olarak ifade edilmemiştir. Sözleşmede “dürüst ticari uygulamalara aykırı” nitelikte sıralanan faaliyetler arasında ekonomik/endüstriyel casusluk ifadesi yer almamaktadır. Aynı Sözleşmenin 8(1)'inci maddesinde yer alan “ (...) sosyo-ekonomik ve teknolojik gelişmeler açısından hayati önem taşıyan sektörlerle halkın ilgisini artırmak (...)” ifadesi hükümetlerin karşı önlem almaları konusunda ayrıksı bir durum yaratmaktadır. Bu durum da sözleşme de açıkça yasaklanmamış olan ekonomik/endüstriyel casusluğun devletler tarafından istismar edilmesi bakımından açık kapı bırakmaktadır (Danielson, 2009, s.519-520).

Diğer bir neden ise endüstriyel casusluk çözülmesi gereken acil bir sorundan ziyade küreselleşmenin yarattığı karşı konulamaz bir etki olarak algılanmaktadır (Danielson, 2009, s.512). Blood (2002, s.233)'a göre uluslararası alanda endüstriyel casusluğun engellenmesi konusundaki isteklilik oldukça azdır. Bazı ülkeler endüstriyel casusluğu uluslararası hukukun ihlali olarak görmemektedir. Bunun da ötesinde casuslar, ülkelerinde genellikle “kahraman³¹” olarak kabul edilmektedir. Bugüne kadar endüstriyel/ekonomik casusluk suçlaması ile sınır dışı edilen hiçbir diplomat ya da devlet görevlisinin kendi ülkesinde yargılandığı veya cezalandırıldığı görülmemiştir. Örneğin ABD’de başka bir ülkede casusluk yapılmasını yasaklayan hukuki bir mevzuat yoktur³². Gerçekte pek çok devletin iç hukuku yabancı bir devlette istihbarat toplamayı engellememektedir. Bu durum bütün devletlerin bu tür faaliyetleri şu ya bu şekilde kendi çıkarlarına uygun görmeleriyle açıklanabilir (Scott, 1999). Aynı zamanda ülkeler, başka ülkeler tarafından endüstriyel/ekonomik casuslukla suçlanan vatandaşlarına yönelik yapılan iade taleplerini de reddetmektedirler. Örneğin, Cleveland Clinic Foundation’dan genetik materyalleri çalarak Japon Hükümeti’ne bağlı RIKEN (Fizik ve Kimya Araştırma Enstitüsü) yararına endüstriyel/ekonomik casusluk yapmakla suçlanan Tetsuya Morimoto adlı mühendisin ABD tarafından iade talebi, Japon Hükümeti tarafından reddedilmiştir. Her iki ülke arasında 24 yıllık suçlu iade anlaşması olduğu halde Japonya ilk kez

³¹ Scofield, D.(12 June 2004). South Korea's 'heroic' spy. Asia Times Online. <http://www.atimes.com/atimes/Korea/FF12Dg04.html> Erişim Tarihi: 27 Nisan 2012.

³² Bu konuda farklı bir çalışma için bkz. Mosier, M. (2001). Causes of Action for Foreign Victims of Economic Espionage abroad by U.S.. Intelligence. *Duke Journal of Comparative & International Law*, vol.11, no.2, s.427-450.

TASNİF DIŐI

ABD tarafından yapılan iade talebini geri çevirmiŐtir (Brenner ve Crescenzi, 2006, s.439).

Ekonomik/endüstriyel casusluğun suç mu yoksa bir savaş yöntemi mi olduđu sorusu tartışılabilen bir durumdur. Suç çerçevesinde değerlendirildiğinde toplumu oluşturan bireylere pek çok zararı olduđu görölmektedir. Hırsızlık suçu ile özdeşlik kurulacak olursa endüstriyel/ekonomik casusluk da vatandaşların yasal olarak elde ettiđi değerli varlıklara zarar vermektedir. Ancak klasik suçlulardan farklı şekilde endüstriyel casuslar sadece kendi menfaatleri açısından bu eylemi yerine getirmezler. Ekonomik/endüstriyel casusluk herhangi bir savaş yöntemine benzer şekilde egemen bir devletin güvenliđini ve istikrarını hedef alır. Bu durum da endüstriyel/ekonomik casusluğu kolluk güçlerinin müdahale ettiđi klasik suç türlerinden ayırmaktadır (Brenner ve Crescenzi, 2006, s.448-449).

SONUÇ ve DEĞERLENDİRME

Tarihin başlangıcından günümüze kadar olan dönem incelendiğinde insanoğlunun kurmuş olduğu medeniyetin tarım, sanayi ve bilgi temelli olmak üzere üç aşamadan geçtiği görülmektedir. İçinde bulunduğumuz çağda bilginin öne çıkan ekonomik değeri devletlerin, kurumların, işletmelerin bilgi üretiminin ve üretilen bilginin etkin bir şekilde kullanımı konusunda kıyasıya rekabet etmelerine yol açmaktadır. Günümüzde malvarlıksal bir değer kazanan bilginin pazarlanması konusunda öncü olan devletler ile az gelişmiş ülkeler arasındaki mesafe giderek açılmaktadır. Fikri mülkiyet üretemeyen ve haklarını koruyamayan toplumlar ciddi problemlerle karşılaşmaktadırlar.

İnsan düşüncesinin ürünü olan gayri maddi malları tanımlamak için kullanılan fikri mülkiyet; patent, faydalı model, tasarım ve entegre devre topografyaları gibi sınai mülkiyet haklarından, ticari sırlara ve telif haklarına uzanan oldukça geniş bir kavramdır. Sanayi Devrimi ile birlikte artan üretim ve yeni bilimsel ilerlemeler modern anlamda sınai mülkiyet haklarının doğmasını sağlamıştır.

Buluşların ekonomik anlamda artan değeri devletleri, kendi vatandaşlarının ve işletmelerinin sahip olduğu fikri mülkiyeti koruma adına kanuni olarak çeşitli koruma tedbirleri almaya itmiştir. Bu konuda imzalanan Paris Sözleşmesi, TRIPs, GATT gibi anlaşmalar da konuya uluslararası standart getirme amacındadır. Örneğin tescil edilen patentlerde (incelemeli) 20 yıl, faydalı model ve entegre devre topografyalarında 10 yıllık koruma süreleri öngörülmüştür. Devletler almış oldukları koruma tedbirleri ile buluş sahibinin haklarını kanuni güvence altına alarak, ekonomik ve sosyal gelişim açısından yaratıcılığı teşvik etmeyi amaçlamaktadır. Bu doğrultuda fikri mülkiyet haklarının korunması konusunda çeşitli ilkeler getirilmiştir. Tescil ilkesi, ön kullanım hakkı, ülkesellik ilkesi, rüçhan hakkı, gerçek hak sahipliği ilkesi ve tükenme ilkesi fikri mülkiyet haklarının belirlenmesinde son derece önemlidir.

Üretim ile ulusal refah arasında doğrudan bir ilişki bulunmaktadır. Nitekim, patent, faydalı model, tasarım, entegre devre topografyaları gibi sınai mülkiyet hakları konusunda lider olan ülkelerin refah seviyesinde de üst sıralarda olduğu görülmektedir. Örneğin ABD, Japonya ve Çin'deki patent bürolarına yapılan başvurular dünya genelinde yapılan başvuruların %60'ını oluşturmaktadır. 2010 yılında dünyada 7.3 milyon kadar patent bulunurken sadece ABD'ye ait olan patent

TASNİF DIŐI

sayısı 2 milyon civarındadır. Yüksek kaliteli patentler firmaların deęerini arttırırken, güçlü bir patent portföyüne sahip olan şirketler de borsalarda yüksek fiyattan işlem görmektedir.

Patentin konusunu buluş oluşturmaktadır. Buluş ise bir ürün ya da yöntemle ilgili probleme getirilen teknik çözümdür. Teknolojik, ekonomik ve sosyal alanda ilerlemeyi sağlamak için buluşlar patent belgesi ile koruma altına alınırlar. Ancak bir buluşun patent korumasından yararlanabilmesi için çeşitli şartlar aranmaktadır. Bahse konu buluşun yeni olması, tekniğin bilinen durumunu aşması ve sanayiye uygulanabilir olması gerekmektedir. Buluş olduđu halde bu niteliklerden bazılarını taşımayan ve işletme açısından ekonomik değeri olan ürünler de bulunmaktadır. Bunlara ek olarak, bağımsız bir ekonomik değeri olan, ekonomik faaliyetlerde sahibine rekabet avantajı sağlayan, aleni olmayan ve sahibinin gizli kalmasını istediđi “ticari sırlar” da ekonomik değer taşımaktadır. Kıta Avrupa’sından ziyade Anglo-Sakson hukuk sisteminde kullanılan bir kavram olan ticari sırlara planlar, prototipler, müşteri ve tedarikçi bilgileri, numuneler, üretim süreçleri, kimyasal formüller, depolama ve dağıtım yöntemleri, maliyet ve fiyatlandırma bilgileri, makine çizimleri, pazarlama teknikleri, personel kayıtları, mühendislik raporları, iş metotları ve ürün test sonuçları, örnek olarak gösterilebilir. Farklı isimlerle adlandırılmış olsalar da işletme sırrı, meslek sırrı, müşteri sırrı ve iş sırrı gibi kavramlar da ticari sır kapsamında değerlendirilmektedir.

Pazarların bir araya gelerek ekonominin küresel bir nitelik kazanması, sanayinin itici gücü olan ticari sırların uluslararası ortamda korunması ihtiyacını ortaya koymuştur. Bu koruma, özellikle dünya ölçeğinde ticaret yapan ve değerli bilgilere sahip şirketler ile bu şirketlerin katkılarının bulunduğu ülke ekonomileri açısından son derece önemlidir. Bu konuda imzalan anlaşmalardan ilki 1883 Paris Sözleşmesi’dir. Sınai mülkiyetin korunması konusunda uluslararası alanda kabul gören en temel anlaşmadır. Sınai mülkiyetin anayasası olarak kabul edilen Sözleşme, bugün sınai mülkiyet ile ilgili pek çok yasal düzenlemeye kaynaklık ederek ülkelerin iç hukuklarına dâhil olmuştur. Fikri mülkiyet ve ticari sır korumasında önem taşıyan diđer bir anlaşma ise GATT’dır. Azgelişmiş ülkelerin karşı çıkmalarına rağmen sınai mülkiyet hakları GATT kapsamında yeniden ele alınmıştır. Fikri haklar bakımından uluslararası bir standart getirme amacını taşıyan en kapsamlı düzenleme olarak TRIPs Sözleşmesi gösterilmektedir. TRIPs hâlihazırdaki sözleşmeleri ortadan kaldırmamakla birlikte bunlara ek düzenlemeler içermektedir. Üye devletler DTÖ bünyesinde serbest ticaret sisteminin dışında

TASNİF DIŐI

kalmamak için asgari standartları yerine getirmek zorundadır. TRIPs'e ilave olarak PCT ve EPC de uluslararası patent tescilini saęlayan önemli sözleşmelerdir.

Fikri mülkiyet haklarının korunmasına yönelik olarak 1883 Paris Anlaşması'ndan günümüze deęin imzalanan pek çok sözleşme ve kurumun varlığına rağmen bilişim teknolojilerinde yaşanan baş döndürücü gelişmeler bu konuda alınan tedbirleri yetersiz kılmaktadır. Bilişim teknolojilerinin neredeyse bütün endüstri dallarının altyapısını oluşturduğu ve elektronik ortama dâhil olan alanlara yeni anlamlar yükledięi görölmektedir. Elektronik ortamda mesaj gönderme için kullanılan e-postanın ardından, e-reklam, e-ticaret, e-devlet, e-oylama vb. pek çok kavram yeni teknoloji ile birlikte gittikçe gelişerek gündelik yaşamımızın birer parçası haline gelmiştir. İnternet bağlantılı cep telefonları, diz üstü, kişisel ve tablet bilgisayarlar gibi üretilen her yeni sistem de bilgisayar tanımının sınırlarını zorlamaktadır.

Verilerin elektronik ortamda işlenmesi, depolanması ve iletilmesi kolaylaşmış ancak hassas bilgileri ve ticari sırları saklamak da bir o kadar zorlaşmıştır. Basılı haliyle saklanması mümkün olmayan binlerce sayfalık gizli bilgi barındıran veriler, saniyeler içinde kaydedilerek tek tuşla dünyanın herhangi bir yerine gönderilebilmektedir. Coęrafi sınır tanımayan siber uzay kendisine özgü bir suç dünyası yaratırken, bilgisayar korsanları da sanayi casusluęunun yeni aktörleri olarak karşımıza çıkmaktadır. Dolayısıyla küresel ekonomi ile siber uzayın birleşmesi, bambaşka bir mücadele alanının doğmasına yol açmıştır. Bu doğrultuda bilişim sistemlerindeki gelişmeleri takip etmek, siber uzayda meydana gelen tehdit ve riskleri öngörmek ve bilgi teknolojilerinin güvenlięini saęlamak her seviyedeki kurum ve kuruluşun başat görevi haline gelmiştir.

Siber uzayın fiziksel dünya ile bütünleşerek, güvenlik, ulaşım, enerji, finans vb. altyapılarına bağlanması, getirdięi faydaların yanında daha önce karşılaşılmayan risk ve tehditlerin doğmasına neden olmuştur. Siber uzaydaki her türlü veri, program ve aę sisteminin deęiştirilmesi, bozulması, sahtesinin üretilmesi, kesintiye uğratılması ya da yok edilmesi siber saldırı olarak adlandırılmaktadır. Klasik saldırı şekilleri ile karşılaştırıldığında siber saldırı oldukça deęişik bir karakter sergilemektedir. Saldırıda bulunanların kontrolünü ele geçirdikleri dięer bilgisayarları da kullanabilmeleri saldırı kaynaęının tespit edilmesini güçleştirmektedir. Bu durum saldırıya uğrayanlarda, görünmeyen ya da bilinmeyen bir düşmanla savař duygusunu yaratmaktadır. Dięer bir özellik ise saldırının yarattıęı hasarın tespitinin son derece güç olmasıdır. Saldırının ne zaman bařladıęı, hangi sistem ve bilgilerin

TASNİF DIŞI

zarar gördüğü, bu bilgilerle saldırganların hangi kazançları sağladığı, elde ettikleri bilginin saldırganlar tarafından gelecekte de kullanılabilme ihtimalleri vb. hususlar hesaplamayı oldukça zorlaştırmaktadır. Siber saldırının diğer bir özelliği de saldırganlara zaman ve mekân açısından sunduğu fırsatlardır. Saniyenin onda biri kadar bir zaman diliminden yıllara uzanan bir saldırı dizisi, hedef sisteme çok yakın bir yerden gerçekleştirilebildiği gibi sınır ötesinde, dünyanın herhangi bir noktasından da yapılabilir.

Siber ortamda sisteme sızan saldırganların verinin gizliliği, bütünlüğü ve kullanılabilirliğini hedef aldıkları gözlenmektedir. Uyguladıkları yöntemleri de zararlı yazılımlar, servis saldırıları, kimlik saldırıları ve gizli dinleme olmak üzere dört ana başlık altında toplamak mümkündür. Bilgisayar virüsleri, solucanlar, Truva atları, arka kapı, klavye kaydediciler, casus yazılımlar ve reklam yazılımlar zararlı yazılımlar kategorisinde yer almaktadır. Kullanıcının bilgisi ve izni olmaksızın, kullanıcı bilgisayara ait her türlü veriyi saldırgana gönderen casus yazılımların endüstriyel casusluk maksadı ile etkin kullanıldığı değerlendirilmektedir. Kullanıcının internet gezintisindeki alışkanlıklarından, klavyede bastığı her bir tuşa ya da e-postalarından kimlik bilgilerine kadar pek çok veri bu tarz saldırının hedefini oluşturmaktadır. Bu bağlamda işletmelerin internete bağlı olan bilgisayarları hassas veri içeriyorsa önemli risk altında demektir. Son dönemde bilgi güvenliğine yönelik en büyük tehlikelerden biri olarak APT saldırıları gösterilmektedir. İran'ın nükleer çalışmalarını kesintiye uğratan "Stuxnet" solucanı ile adını duyuran APT saldırılarına karşı önlem alınabilmesi için kanaatimizce devlet seviyesinde araştırmalar yapılması ve önlemler alınması gerekmektedir. Diğer bir saldırı türü olan servis saldırıları daha çok hizmet aksatma amacıyla yapılmaktadırlar. Sürekli yapılan saldırılar sonucunda sistem çalışmaz ve hizmet veremez hale gelir. Endüstriyel casusluk maksadı ile olmasa bile hedef işletmenin sistemlerini kesintiye uğratması nedeniyle rakiplerinin gerisinde kalmasına neden olabilir. Kimlik saldırıları ise genellikle dolandırıcılık ve hırsızlık gibi suçları kolaylaştırmak maksadıyla başka kişilere ait kişisel ya da finansal bilgileri çalmayı içermektedir. Ticari sırlara erişim konusunda yetkili kişilere ait şifre ve bilgilerin ele geçirilmesi endüstriyel casusluk olaylarında sıklıkla kullanılan bir durumdur. Gizli dinleme, ağ sistemi veya herhangi bir iletişim kanalı üzerinden yapılan veri alışverişinin üçüncü kişiler tarafından takip edilmesidir. Eskiden sadece istihbarat örgütleri tarafından kullanılan dinleme aygıtlarına bugün herkes rahatlıkla ulaşabilmektedir. Gizli dinlemede ses ve görüntüler değil herhangi bir sistem ya da ağa bağlı olmayan bilgisayarlar; mikroişlemci, ekran, yazıcı, klavye vb. donanımların elektromanyetik enerji yayımları da dinlenebilir. Bugün istihbarat

TASNİF DIŐI

örgütlerinin gelişen uydu teknolojisi ile birlikte dinleme konusunda çok daha gelişmiş teknolojilere sahip oldukları tahmin edilmektedir.

Fikri mülkiyetin artan değeri ile bilginin üretilmesi, depolanması ve iletiminde bilişim sistemlerinde yaşanan gelişmeler kadar Soğuk Savaş sonrası güvenlik algısında yaşanan değişim de endüstriyel casusluğa etki eden bir unsur olarak karşımıza çıkmaktadır. SSCB'nin dağılmasıyla birlikte iki kutuplu dünya düzeni yerini ABD'nin başı çektiği tek kutuplu dünya düzenine bırakmıştır. Bu dönemde askeri ve stratejik etmenler önemlerini korumakla beraber, ekonomik güç ve teknolojik gelişme gibi unsurlar giderek öne çıkmaya başlamıştır.

Değişen güç dengeleri ile teknoloji ve ticarete yaşanan gelişmeler sonrasında dünyanın gelmiş olduğu aşamaya “küreselleşme” adı verilmektedir. Küreselleşmenin karar ve kontrol merkezinde ABD başta olmak üzere gelişmiş devletler yer almaktadır. Küreselleşme sonucu şirketlerin sınır ötesi nitelik kazanmasıyla birlikte, devletlerin, bölgesel örgütlenmelerin ve şirketlerin kıyasıya yarıştığı bir rekabet ortamı doğmuştur. Özellikle, mikro elektronik, biyo-teknoloji, telekomünikasyon, havacılık, yazılım, mekanik gibi anahtar sanayilerde herkesin sahip olamayacağı alanlarda rekabet tüm hızıyla sürmektedir.

Küresel rekabet ortamının tanımlanmasında “sürekli yenilik” ve “hiper rekabet” önemli yer tutmaktadır. İşletmelerin rekabeti devam ettirebilmeleri için çok farklı ve esnek teknolojik yetenekler geliştirmesi gerekmektedir. Rekabet gücü yeni teknolojiler üreterek bu teknolojileri hızla yeni ürünlere ve üretim süreçlerine dönüştürme yeteneğine bağlıdır. Teknoloji transferi ile teknoloji yeteneği belirli bir noktaya kadar idame edilse bile üretimi gerçekleştirenler her zaman bir adım önde olacaklardır.

Pazarda bulunan rakipler hakkında bilgi edinmenin anlaşılan değeri şirketleri bu yönde faaliyette bulunmaya teşvik etmektedir. Rekabet istihbaratı adı verilen bu yeni alanda endüstriyel casusluktan farklı olarak, kanunlara uygun ve iş ahlakıyla çelişmeyecek şekilde resmi ve özel kaynaklardan rakipler hakkında bilgi toplanmaktadır. Bugün binlerce şirket tarafından pazarda yer alan rakipleri hakkında bilgi edinmek maksadıyla rekabet istihbaratı teknikleri uygulanmaktadır. İş dünyasında rakipler hakkında internet üzerinde araştırma yapmaktan, gazete kupürlerini takip etmeye kadar yaklaşık 2 milyar dolarlık bir pazarın bulunduğu belirtilmektedir. Bununla birlikte rekabet istihbaratı ile endüstriyel casusluk arasındaki çizgi oldukça incedir. Belirli bir şirket hakkında bilgi toplamanın sınırları

TASNİF DIŞI

ve içerikleri net olarak belirlenmediği müddetçe bu durumun istismara açık bir alan yaratacağı değerlendirilmektedir.

Dünya genelinde ticaret ve rekabet gün geçtikçe çok uluslu şirketlerin faaliyetleri ile ilintili hale gelmektedir. Örneğin 1999 yılında dünyadaki en büyük 100 ekonominin 51'ini şirketler, 49'unu ise ülkeler oluşturmaktaydı. Mukayese yapmak gerekirse General Motors Danimarka'dan, DaimlerChrysler Polonya'dan, Royal Dutch Shell Venezüella'dan, IBM Singapur'dan ve Sony şirketi de Pakistan'dan daha zengin durumdaydı. ABD'de ilk beş sırada yer alan General Motors, Wal-Mart, Exxon Mobil, Ford Motor ve DaimlerChrysler'ın 1999 yılı satış rakamları 182 ülkenin GSYİH toplamlarından daha fazladır. Çok uluslu şirketlerin yapmış oldukları üretim ve ticaretin ulusal ekonomi üzerinde yaptığı katma değer anlaşılmaması, bu şirketlerin kendi devletleri tarafından ekonomik güvenlik çerçevesinde korunması ve kollanmasına yol açmıştır. Yaşanan tecrübeler ekonomik anlamda karşılaşılan problemlerin ulusların ekonomik çıkarlarını sekteye uğrattığını göstermiştir. Geçmişte toprak kazanmak için savaşan devletler günümüzde küresel pazara sahip olabilmek adına teknolojik liderlik için mücadele etmektedirler. Bu nedenle ülkeler ekonomik çıkarlarının korunmasına son derece önem vermektedirler.

Ekonomik anlamda küresel rekabetin tırmanması devletlere ait istihbarat kuruluşlarının da ekonomik ve teknolojik istihbarata daha çok önem vermelerine neden olmuştur. Görüntü alma, izleme, iletişimin dinlenmesi amacıyla kullanılan uydular sadece askeri maksatlarla değil ekonomik mücadele açısından da önemli hale gelmiştir. Soğuk Savaş döneminin önde gelen devletleri, askeri ve politik alanda birbirlerini takip etmek için kullandıkları istihbarat örgütlerini de yeni çıkarlar doğrultusunda ekonomik alana yönlendirmişlerdir. Bununla birlikte kapatılan ya da küçültülen istihbarat personelinin çok uluslu şirketlerin bünyesinde kendilerine yeni bir yer edindikleri görülmektedir. Sadece devletler değil şirketler de istihbaratı haksız da olsa rekabetin bir aracı olarak kullanmak istemektedir. İstihbaratın bilgi çağındaki hedefinde ekonomik değeri yüksek olan fikri mülkiyet ve ticari sırlar yer almaktadır.

Günümüzde ekonomik istihbaratın hem saldırı hem de savunma maksatlı kullanıldığı görülmektedir. Makro seviyede ekonomik istihbaratı uygulayan bir devlet gizli yollardan elde ettiği veriler ile faiz oranlarını ne zaman artırıp azaltması gerektiği veya çekişmeli ticari görüşmelerde nasıl pozisyon alması gerektiği bilgisini karar vericilerine sunabilir. Gizli ve açık kaynaklardan elde edilen ekonomik veriler ile gelişmekte olan pazarlar önceden tespit edilebilir. Diğer yandan ülke içinde

TASNİF DIŐI

retilen ticari sırların korunmasına ynelik karŐı istihbarat tedbirleri iin de ekonomik istihbarattan faydalanılabilir.

Endstriyel casusluk, ekonomik istihbaratın bir alt dalı olarak karŐımıza ıkmaktadır. Genel olarak bakıldıėında siber suları da ieren beyaz yakalıların iŐlediėi yeni bir su dalı olarak tanımlanmaktadır. Endstriyel casuslukla ilgili lkelerin farklı hukuki mevzuatlara sahip olması, ticari sır hırsızlıėı, beyaz yakalı suu, endstriyel casusluk, ekonomik casusluk gibi farklı kavramların kullanılmasına yol amaktadır. rneėin ABD hukuk sistematıėında ticari sır hırsızlıėı “endstriyel casusluk” ve “ekonomik casusluk” olmak zere iki baŐlık altında incelenmektedir. Trkiye, Fransa, Almanya ve diėer pek ok devlet endstriyel casusluėu ceza hukukunun meselesi olarak kabul etmektedir.

Endstriyel casusluėun pek ok nedeni bulunmaktadır. Bu nedenler arasında; rekabet avantajı saėlamak, know-how alıŐması iin yeterli zaman ve imkânın bulunmaması, yenilik iin kaynak yokluėu, bilginin gcnn anlaŐılması, kreselleŐmenin etkisi ve ticari sırların gn getike artan deėerinin anlaŐılması yer almaktadır. Kullanılan yntemler teknolojinin geliŐmesine paralel olarak eŐitlilik gstermektedir. Bilinen temel yntemler:

- Ticari bilgiler iin yapılan beklenmedik istekler,
- İŐ ziyareti boyunca karŐılaŐılan sıra dıŐı olaylar,
- Őpheli İŐ teklifleri,
- Uluslararası sergi, seminer ve toplantıların kullanılması,
- Ortak giriŐim ve araŐtırmaların istismar edilmesi,
- Őirketlerin veya teknolojinin satın alınması,
- Eski alıŐanların kullanılması,
- Kltrel benzerliklerin kullanılması,
- p KarıŐtırma,

- Sızdırma (Toplum Mhendisliėi), őeklinde sıralanabilir. Bu yntemlerden etkili olanların eski veya hâlihazırda alıŐmaya devam eden personel tarafından icra edilen casusluk faaliyeti olduėu belirtilmektedir.

TASNİF DIŐI

Ekonomik değeri olan hassas bilgilerin ele geçirilmesinde devletlerin kendilerine ait istihbarat örgütleri ile çeşitli kurumlarını kullanmaktan çekinmedikleri gözlenmiştir. UKUSA Anlaşması çerçevesinde ABD, Kanada, İngiltere, Yeni Zelanda ve Avustralya'nın ortaklığında yürütölen ECHELON küresel dinleme sistemi diğer devletlerin tepkisi ile karşılaşmaktadır. Elde edilen bilgilerin beş devlet arasında paylaşılması, BM veya NATO gibi hiçbir uluslararası kurumun sistem üzerinde söz sahibi olmaması bu konuda duyulan endişeleri haklı kılmaktadır. Bununla birlikte ECHELON benzeri küresel dinleme ve takip sistemlerine Almanya, Fransa ve Rusya'nın da sahip olduđu belirtilmektedir. Dünyanın çeşitli bölgelerinde yer istasyonlarına sahip olan bu üç ölkenin de dinleme kapasiteleri hakkında yeterli bilgi bulunmamaktadır. Bu bağlamda medyada yer alan haberlerde veya açıklanan raporlarda kendilerini endüstriyel casusluk konusunda mağdur gösteren gelişmiş devletlerin bu beyanlarında gerçeđi olduđu gibi yansıtmadıkları değerlendirilmektedir. Ekonomik çıkarlar söz konusu olduđuunda tüm devletler sahip oldukları teknolojik kapasitelerini ve istihbarat yeteneklerini doğrudan kullanmaktadır.

İstihbarat örgütlerinin endüstriyel casusluk konusunda yöntem olarak ağırlıklı İnsan İstihbaratı (HUMINT) ile Sinyal İstihbaratını (SIGINT) kullandığı anlaşılmaktadır. Bu noktada bağlı oldukları ölkelere de önemli kazançlar sağlamaktadırlar. Örneđin CIA tarafından sağlanan istihbarat sayesinde imzalanan ticari anlaşmaların ABD sanayiine yıllık 7 milyar dolarlık bir kazanç sağladığı ifade edilmektedir. Buna ek CIA'nın Nisan 1994'ten 17 ay önce Amerikan şirketlerinin dezavantajlı konuma düştüğü ve toplam değeri 30 milyar doları bulan ihalelerde de karar alıcıları 72 kez ikaz ettiđi belirtilmektedir.

Yapılan çalışma sonucu çeşitli devletlere ait istihbarat örgütleri ile çeşitli kurumların endüstriyel casusluk faaliyetlerine karıştığı görölmektedir. İsrail İstihbarat örgütü MOSSAD ve Lakam, Çin istihbarat servisi Guoanbu, Fransız istihbarat örgütü DGSE, Amerikan İstihbarat örgütü CIA, NSA ve Advocacy Center, İngiltere'de GHCQ, Japonya'da MITI ve JETRO, Rusya'da FSB, GRU ve SVR adları geçen örgütlerdir. Adı geçen ölkelere bakıldığında bunların gelişmiş ölkeler grubunda yer aldıkları görölmektedir. Az gelişmiş ya da gelişmekte olan ölkeler ancak kendi teknolojilerinin yetebileceđi ürünleri taklit etmek adına ticari sırları ele geçirmeye çalışırken, gelişmiş ölkeler küresel rekabette öne geçmek maksadıyla daha yüksek ve gelişmiş teknolojileri kullanarak fikri mülkiyet haklarını ele geçirmeye çalışmaktadır.

TASNİF DIŞI

İstihbarat örgütleri tarafından endüstriyel casusluk faaliyetinde bulunulması beraberinde bazı sorunları da gündeme getirmektedir. İstihbarat örgütlerinin imkânları ulusal sanayii desteklemek maksadıyla kullanılacaksa kuşkusuz bazı şirketler aynı alanda ülke içinde faaliyet gösteren diğer rakiplerine göre bu durumdan daha fazla faydalanacaktır. İstihbarat örgütlerinin desteğini alan şirketlerin bir anlamda piyasaları düzenleyen “görünmez ele” sahip olduğu söylenebilir. Bu durum devlet içinde rüşvetle birlikte çeşitli yolsuzluk türlerine neden olabilir. Günümüzde pek çok bürokratin emekliliklerinde şirketlerin yönetim kademelerinde görev aldığı görülmektedir. Şirketler, emekli olan istihbarat kurumu yöneticilerinin eski kurumları ile olan samimi ilişkilerini bu doğrultuda kullanmak isteyebilirler. Aynı zamanda hâlihazırda istihbarat kurumlarında çalışan idarecilerin çalışmayı planladıkları şirketlere ayrımcılık yapmaları da ihtimal dâhilinde olan bir durumdur. . İstihbarat örgütleri ile şirketler arasında meydana gelebilecek bu tarz bir ilişkinin kötüye kullanılma ihtimali oldukça açıktır.

Endüstriyel casusluğun gerek işletme gerekse ülke ekonomisine verdiği zararlara yönelik araştırmalara bakıldığında birbirinden çok farklı sonuçlara ulaşıldığı görülmektedir. Zararın tam olarak bilinmemesi, hesaplamalarda standart bir yöntemin kullanılmaması değişken sonuçlara yol açmaktadır. Sahip olunan bir ticari sırrın ekonomik değerinin belirlenmesinde pazar, maliyet ve gelir yaklaşımı olmak üzere üç çeşit klasik yöntem uygulanmaktadır. Kanaatimizce kayıplarla ilgili sorular net olarak cevaplanmadığı müddetçe gerçek maliyeti ortaya çıkarmak mümkün olmayacaktır.

Endüstriyel casuslukla mücadele ülke genelinde topyekûn yapılması gereken bir faaliyettir. Endüstriyel casuslukla mücadele ve bilgi güvenliği konusu ayrı bir çalışmanın konusu olmakla birlikte bu konuda alınacak tedbirleri işletme ve devlet seviyesi olmak üzere iki gruba ayırmak mümkündür. İşletme seviyesinde alınması gereken tedbirler genel olarak personel güvenliği, fiziksel güvenlik, siber güvenlik, çalışanların eğitimi ve kurumsal farkındalık ile rekabet istihbaratından oluşmaktadır. Endüstriyel casusluk olaylarına bakıldığında, bilgi kaybı konusunda çalışanların ve yöneticilerin kusuru bulunduğu halde bazı durumlarda da personelin dikkati ve kurumuna olan bağlılığı sayesinde yapılmak istenen saldırının ortaya çıktığı görülmektedir. Bu nedenle işletme seviyesinde personelin eğitilerek kurumsal farkındalık yaratılması son derece önemlidir. Çalışanlar ve yöneticiler, ticari sır ve bilgi güvenliği konusunda eğitilmeli, olası problemlerde ne şekilde hareket etmeleri gerektiğini bilmelidirler. Bununla birlikte işletme içerisinde bir bilgi güvenliği politikası oluşturulmalı, bilmesi gereken (need to know) kuralı çerçevesinde yetkisiz kişilerin

TASNİF DIŐI

ekonomik deęer taşıyan ve kendileri ile ilgisiz bilgiye erişimi engellenmelidir. İşletmenin alacağı tüm önlemler faydalı olmakla birlikte, bilginin takipçisi olanlar başka bir ülkenin istihbarat örgütü ise alınacak tedbirlerin yetersiz kalması kaçınılmazdır. Fikri mülkiyet haklarının ve ticari sırların korunması sadece işletmelerin sorumlu olduğu bir alan değildir. Devletlerin de ekonomiyi destekleyen ve istihdam sağlayan özel sektörün gelişimini koruma adına ulusal güvenlik çerçevesinde endüstriyel casusluğu önleyici tedbirler alması gerekmektedir. Bağlı oldukları ülkenin kaynakları ile donatılan istihbarat örgütlerinin bilgi toplama konusundaki imkân ve kabiliyetleri ile tek başına bir işletmenin mücadele etmesi mümkün gözükmemektedir. Bu nedenle endüstriyel casuslukla mücadele konusunda ulusal istihbarat örgütlerinin aktif olarak görev yapması, bilgi üreten tüm kurumları bu konuda yönlendirmesi gerektięi değerlendirilmektedir. Bununla birlikte endüstriyel casusluk konusu basit bir ticari sır hırsızlığı olarak ele alınmamalı, ABD'deki Ekonomik Casusluk Kanunu (EEA)'na benzer şekilde yasal tedbirler alınarak bu konudaki caydırıcılık güçlendirilmelidir.

KAYNAKÇA

- Acar, M. (2004). Küreselleşme mi, Küreselleştirme mi? *Piyasa Dergisi* (3) sayı 12, s.1-14.
- Adıgüzel, M. (2011). *Bilgi Toplumu ve Küreselleşme Bağlamında Küresel Rekabet Ortamı*. Ankara: Nobel Yayıncılık.
- Akın, B. (2001). *Yeni Ekonomi*. Konya: Çizgi Kitabevi.
- Akpınar, H. ve Edin, İ. (2007). Rekabet İstihbaratı. *Marmara Üniversitesi Sosyal Bilimler Enstitüsü Öneri Dergisi*, cilt.7, sayı.28, s.1-8.
- Aktan, Ç.C. (1999). *Türkiye Dünya'nın Neresinde?* Ankara:EGİAD Yayını.
- Alper, D. (2011). Patent Değerlemesi ve Reel Opsiyonlar. *Business and Economics Research Journal*. vol.2, no.1, s.153-172.
- Anderson, S. ve Cavanagh, J. (2000). *Top 200: The Rise of Corporate Global Power*. 16 Mart 2012 tarihinde IPS Bilgi Portalı: http://www.ips-dc.org/reports/top_200_the_rise_of_corporate_global_power adresinden alındı.
- Ararat, M. ve Yurtoğlu, B. (2006). Yönetişim ve Küresel Rekabet. *Yönetim Araştırmaları Dergisi*, cilt 6, sayı 1-2, s.5-44.
- ASIS (2007). Trends in Proprietary Information Loss. *Survey Report August 2007*. 30 Nisan 2012 tarihinde ASIS International Bilgi Portalı: <https://www.asisonline.org/newsroom/surveys/spi2.pdf> adresinden alındı.
- Avar, B. (2012). *Kaçın Demokrasi Geliyor*. İstanbul: Remzi Kitabevi.
- Aviatia Site (2012). IAI Kfir Savaş Uçağı, resmi 25 Nisan 2012 tarihinde Aviatia Site Bilgi Portalı: <http://www.aviatia.net/other/jet-aircraft/israel/iai-kfir/> adresinden alındı.
- Avşar, Z. ve Öngören, G. (2010). *Bilişim Hukuku*. İstanbul: Türkiye Bankalar Birliği.
- Aydın, S. (2009). Küreselleşme Sürecinde Türkiye'nin Ekonomik Güvenliği. *Akademik Araştırmalar Dergisi*, Sayı. 42, s.39-52.
- Ayhan, A. (2002). *Dünden Bugüne Türkiye'de Bilim ve Teknoloji*. İstanbul:Beta Yayınları.
- Bank Systems Technology (2005). "Keyloggers Foiled In Attempted \$423 Million Bank Heist" haberi, 24 Ocak 2012 tarihinde Bank Systems & Technology Bilgi Portalı: <http://www.banktech.com/articles/159902118> adresinden alınmıştır.
- Barutçu, E. (2006). Bilgi Toplumunda İnsan Kaynakları ve İnsan Kaynaklarının Etkinliğini Sağlamada Yetkinlikler. N. Kargı (Ed). *Bilgi Ekonomisi*, içinde (s.145-165). Başak Matbaacılık.
- Barutçugil, İ. (2002). *Bilgi Yönetimi*. İstanbul: Kariyer Yayıncılık.
- Bayamlıoğlu, İ. E. (2008). *Fikir ve Sanat Eserleri Hukukunda Teknolojik Koruma*. İstanbul: On İki Levha Yayıncılık.
- BBC (2011). "US Spy for China Noshir Gowadia Jailed for 32 Years" haberi 29 Nisan 2012 tarihinde BBC Bilgi Portalı: <http://www.bbc.co.uk/news/world-asia-pacific-12272941> adresinden alındı.

TASNİF DIŞI

Betz, F. (2010). *Teknolojik Yenilik Yönetimi: Değişimle Gelen Rekabet Avantajı*. Ankara: TÜBİTAK Popüler Bilim Kitapları.

Beydağlı, E.(2010). Ortak Kriterler (ISO/IEC 15408) Standardı ve Ülkemizdeki Uygulaması. 29 Ocak 2012 tarihinde TUBİTAK BİLGEM Bilgi Portalı: <http://www.bilgiguvenligi.gov.tr/bt-guv.-standartlari/ortak-kriterler-iso-iec-15408-standardi-ve-ulkemizdeki-uygulamasi.html> adresinden alınmıştır.

Bilge, M. E. (2005). *Ticari Sırların Korunması*. Ankara:Asil Yayın Dağıtım.

Blood, C. G. (2002). Holding Foreign Nations Civilly Accountable for their Economic Espionage Practices. *IDEA-The Journal of Law and Technology*, vol. 42, no.2, s.227-247.

Boulanger, A. (2010). Unauthorized Intrusions and Denial of Service, içinde, Ghosh, S. ve Turrini, E (Ed.). *Cybercrimes: A Multidisciplinary Analysis*. Berlin:Springer, s.27-44.

Brenner, S.W. ve Crescenzi, A.C.(2006). State-Sponsored Crime. The Futility of the Economic Espionage Act. *28 Houston Journal of International Law (Winter)*, s.389-465.

Burgess, C. ve Power R.(2008). *Secrets Stolen, Fortunes Lost:Preventing Intellectual Property Theft and Economic Espionage in the 21st Century*. Burlington:Syngress Publishing.

Buzan, B. (1997). Rethinking Security after the Cold War. *Cooperation and Conflict* vol. 32 (1), s. 5-28,

Bülbül, Y. ve Özbay, R.D. (2010). Sanayi Devrimi'nin Tartışmalı Bir Kurumu Olarak Patent ve Osmanlı'da İhtira Beratı Kanunu. *Marmara Üniversitesi İ.İ.B.F Dergisi*. cilt.XXVIII, sayı.1, s.37-55.

Campbell, D. (October 1999). *Development of Surveillance Technology and Risk of Abuse of Economic Information*. Working document for the STOA Panel. Luxemburg: European Parliament Directorate General for Research Directorate A. The STOA Programme.

Canbek. G. ve Sağiroğlu, Ş. (2006). *Bilgi ve Bilgisayar Güvenliği: Casus Yazılımlar ve Korunma Yöntemleri*. Ankara.

Canbek. G. ve Sağiroğlu, Ş. (2007). Bilgisayar Sistemlerine Yapılan Saldırıları ve Türleri: Bir İnceleme. *Erciyes Üniversitesi Fen Bilimleri Enstitüsü Dergisi* 23 (1-2) 1 - 12 (2007).

Canbek. G. ve Sağiroğlu, Ş. (2008). Casus Yazılımlar: Bulaşma Yöntemleri ve Önlemler. Gazi Üniv. Müh. Mim. Fak. Der. cilt.23, no.1, s.165-180.

Castells, M. (2008). *Enformasyon Çağı: Ekonomi, Toplum ve Kültür. Birinci Cilt Ağ Toplumunun Yükselişi*. İstanbul: Bilgi Üniversitesi Yayınları.

Choo, K.K.R. (2010). High Tech Criminal Threats to The National Information Infrastructure. *Information Security Technical Report* 15.s.104-111.

Ciprian, B. (2011). Scada Security in the Context of Corporate Network Integration. *Constanta Maritime University Annals*. year.XII, vol.15, s.159-164.

TASNİF DIŞI

Clark, D. ve Johnston, R. (1998). Economic Espionage and Interallied Strategic Cooperation. *Thunderbird International Business Review*, vol. 40(4), s.413-431.

Clerc, P. (1997). *Economic Intelligence*. UNESCO Press

CNNMoney (2005) Çin’li Şirketlerin 2005 yılına ait verileri, 21 Mart 2012 tarihinde CNNMoney Bilgi Portalı: <http://money.cnn.com/magazines/fortune/global500/2005/countries/C.html> adresinden alındı.

CNNMoney (2011). “Dünyanın En Büyük İlk On Şirketi” sıralaması 21 Mart 2012 tarihinde CNNMoney Bilgi Portalı: http://money.cnn.com/magazines/fortune/global500/2011/full_list/index.html adresinden alındı.

Cowell, A. (10 March 1997). “Bonn Said to Expel U.S. Envoy Accused of Economic Spying” haberi, 26 Nisan 2012 tarihinde The New York Times Bilgi Portalı: <http://www.nytimes.com/1997/03/10/world/bonn-said-to-expel-us-envoy-accused-of-economic-spying.html> adresinden alındı.

Crane, A. (2005). In the Company of Spies: When Competitive Intelligence Gathering Becomes Industrial Espionage. *Business Horizons*, sayı 48, s.233-240.

CSIS (2011). Methods Used in Economic Espionage. 18 Kasım 2011 tarihinde Bilgi Portalı: <http://www.csis.gc.ca/prtrts/spng/mthds-eng.asp> adresinden alındı.

Çağlar, H. (2006). Patent Hukukunda Ön Kullanım Hakkı. *Gazi Üniversitesi Hukuk Fakültesi Dergisi*. c. X, s.1,2 , ss.77-92.

Çiftçi, H. (2004). *İktisadi Gelişmede Uluslararası Rekabet ve Ulusal Kurumlar Dinamiği*. Ankara: Seçkin Yayıncılık.

Damodaram, V. ve Valarmathi, M. L.(2010). Security Measures of Randvul Keyboard. *International Journal on Computer Science and Engineering*. vol. 02, no.3, s. 619-625.

Danielson, M.E.A. (2009). Economic Espionage: A Framework for a Workable Solution. *MINN. J.L. SCI. & TECH.* 10(2), s.503-548.

Demirci, C. (2009). *Sınai Haklarda Rüçhan Hakkı*. Yayınlanmamış Yüksek Lisans Tez.

Denk, D. (2000). *21. Yüzyıla Girerken Türkiye’nin Jeopolitik Durumu ve Jeostratejik Öneminin Yeniden Belirlenmesi*. İstanbul: Harp Akademileri Basımevi

Department of Justice, Canada (2011). Economic Espionage. 18 Kasım 2011 tarihinde Bilgi Portalı: <http://laws-lois.justice.gc.ca/eng/acts/O-5/page-8.html> adresinden alındı.

Dexter, D.A. ve Beckett-McWalter, J. (2006). Protecting Trade Secrets: Best Practices from Hiring to Terminating and Everything in Between. *Licensing Journal*, vol. 26 Issue 1, s.1-5.

Dindar, İ. (2004). *21.Yüzyılda Teknoloji ve İstihbarat Savaşları*. İstanbul: IQ Kültür Sanat Yayıncılık.

Dlamini, M.T. , Eloff, J.H.P. ve Eloff, M.M. (2009). Information Security: The Moving Target. *Computers & Security*. vol.28, issues 3-4, ss.189-198.

Donay, S. (1978). *Meslek Sırrının Açıklanması Suçu*. İstanbul.

TASNİF DIŞI

Dugdale-Pointon, T. (22 August 2001). The Israeli Intelligence Services; Deception and Covert Action Operations. 25 Nisan 2012 tarihinde Military History Encyclopedia Bilgi Portalı: http://www.historyofwar.org/articles/concepts_israeli_covert.html adresinden alındı.

Dünya Geneline İnternet Kullanıcı Sayısı. 11 Ocak 2012 tarihinde International Telecommunication Union Bilgi Portalı: <http://www.itu.int/ITU-D/ict/statistics/> adresinden alındı.

Edin, İ. (2008). Rekabet İstihbaratı Sürecinde Anahtar İstihbarat Konularının Belirlenmesi. *Marmara Üniversitesi İ.İ.B.F Dergisi*, yıl.2008, cilt. XXV, sayı.2, s.589-600.

Ekonomik Güvenlik (2003). Milli Güvenlik Akademisi Yayın No:5. Ankara.

Elbahadır, H. (2011). *Hacking Interface*. İstanbul:KODLAB Yayın.

Erbay, İ. (2002). Know-How Sözleşmesi. Ankara:Yetkin Yayınları.

Encyclopaedia Britannica (2012). "Industrial Espionage" tanımı 09 Mayıs 2012 tarihinde Encyclopaedia Britannica Bilgi Portalı: <http://www.britannica.com/EBchecked/topic/287033/industrial-espionage> adresinden alındı.

Erdem, B.B. (2002). 22.11.2001 Tarihli ve 4721 Sayılı Türk Medeni Kanunu'nda Düzenlenen Türk Mahkemelerinin Yetkisine İlişkin Kurallar ve Bu Mahkemelerin Milletlerarası Yetkisi. *MHB, Prof. Dr. Engin NOMER'e Armağan*, y.22.

Erdem, B.B. (2003). *Fikri Hukukta Türk Mahkemelerinin Milletlerarası Yetkisi*. İstanbul: Beta.

Erkal, N. (2004). Policy Forum: Intellectual Property Rights. On the Interaction between Patent Policy and Trade Secret Policy. *The Australian Economic Review*. Vol.37, no.4, s.427-435.

Eurostat (2012). AB'in Toplam GSYH Miktarı, 21 Mart 2012 tarihinde Eurostat Bilgi Portalı: http://epp.eurostat.ec.europa.eu/statistics_explained/index.php/National_accounts_%E2%80%93_GDP adresinden alındı.

Falliere, N. , Murchu, L. O. ve Chien, E. (February 2011). *W32.Stuxnet Dossier*. Symantec Security Response.

FAS (2012). Russian Federation Federal Law No. 5 Adopted by the State Duma on 8 December 1995. 05 Mayıs 2012 tarihinde Federation of American Scientists Bilgi Portalı: http://www.fas.org/irp/world/russia/docs/law_960110.htm adresinden alındı.

Fink, S. (2002). *Sticky Fingers, Managing The Global Risk of Economic Espionage*. USA: Dearborn Trade Publishing.

Fitzpatrick, W.M. , DiLullo, S.A. ve Burke, D.R. (2004). Trade Secret Piracy and Protection: Corporate Espionage, Corporate Security and the Law. *Advances in Competitiveness Research*, vol.12, no.1, s.57-71.

FM 2-22.3 (FM 34-52) *Human Intelligence Collector Operations*. Headquarters, Department Of The Army, September 2006. 30 Nisan 2012 tarihinde Federation of American Scientists Bilgi Portalı: www.fas.org/irp/doddir/army/fm2-22-3.pdf adresinden alındı.

TASNİF DIŞI

Fraumann, E. (1997). Economic Espionage: Security Missions Redefined. *Public Administration Review*, vol.57, no.4,s.303-308.

Gallino, L. (2007). *Küreselleşme ve Eşitsizlik*. Ankara: Dost Kitapevi.

Garnaut, J. ve Liu, S. (2010). Stern Sentenced to 10 Years by Chinese Court. 30 Nisan 2012 tarihinde The Age Bilgi Portalı: <http://www.theage.com.au/business/stern-sentenced-to-10-years-by-chinese-court-20100329-r7x0.html> adresinden alındı.

Garrie, D.B. , Griver, Y. ve Joller, M.(February 2010). Regulating Spyware: Challenges and Solutions. *Journal of Internet Law*. vol.13, no.8, s.3-13.

Ghosh, S. ve Turrini, E. (2010). *Cybercrimes: A Multidisciplinary Analysis*. New York:Springer.

Gilad, B. (1995). Competitive intelligence: What has gone wrong? *Across the Board*, cilt 32, sayı 9. 04 Nisan 2012 tarihinde Ebsco Host Bilgi Portalı: <http://web.ebscohost.com/ehost/detail?sid=ea182436-e428-46dd-a16c-7704ec01fea7%40sessionmgr14&vid=1&hid=13&bdata=Jmxhbm9dHlmc2l0ZT1laG9zdC1saXZl#db=bth&AN=9510130877> adresinden alındı.

Girgin, K. (2003). *Uluslararası İlişkiler Modern İstihbarat ve Türkiye*. İstanbul: Okumuş Adam Yayınları.

Global Aircraft (2012).Dassault Mirage III Savaş Uçağı, resmi 25 Nisan 2012 tarihinde Global Aircraft Bilgi Portalı: http://www.globalaircraft.org/planes/dassault_mirage_iii.pl adresinden alındı.

Global Issues (2012). "World Military Spending" bilgisi, 03 Nisan 2012 tarihinde Global Issues Bilgi Portalı: <http://www.globalissues.org/article/75/world-military-spending> adresinden alındı.

Gordon, L. A. , Loeb, M. P. , Lucyshn, W. ve Richardson, R. (2005). CSI/FBI Computer Crime and Security Survey. 24 Nisan 2012 tarihinde www.cpppe.umd.edu/Bookstore/Documents/2005CSISurvey.pdf adresinden alındı.

Gozzi, R. (2000). The Trojan Horse Metaphor. 24 Ocak 2012 tarihinde <http://www.thefreelibrary.com/THE+TROJAN+HORSE+METAPHOR.-a062891163> adresinden alındı.

Gregory, S. (1997). Economic Intelligence in the Post-Cold War Era:Issues for Reform. 21 Mart 2012 tarihinde <http://www.fas.org/irp/eprint/snyder/economic.htm> adresinden alındı.

Güldiken, N. (2006). Bilginin Elde Edilmesi ve Korunmasında Ekonomik İstihbarat Sistemlerinin Rolü. *Cumhuriyet Üniversitesi İktisadi ve İdari Bilimler Dergisi* , 178-179. 28 Kasım 2011 tarihinde Bilgi Portalı: <http://eskidergi.cumhuriyet.edu.tr/dergi.php?name1=iibffakultesi&yil=2006&cilt=7&sayi=2> adresinden alındı.

Halligan, R.M. ve Weyand, R.F. (2006). The Economic Valuation of Trade Secret Assets. *Journal of Internet Law*, vol.9, issue. 8, s.19-24. 27 Nisan 2012 tarihinde EbscohostBilgiPortalı:<http://web.ebscohost.com/ehost/pdfviewer/pdfviewer?sid=a553f8f7-7d43-4d51-b2ab-b69c73414962%40sessionmgr12&vid=1&hid=12> adresinden alındı.

TASNİF DIŞI

Hemphill, T.A. (2002). Oracle vs. Microsoft: Corporate Espionage or Competitive Intelligence? *Business & Society Review* (00453609), vol. 107, issue 4, s.501-511.

Internet Archive (1996). Economic Espionage: Joint Hearing before the Select Committee on Intelligence, United States Senate, and the Subcommittee on Terrorism, Technology, and Government Information of the Committee on the Judiciary, United States Senate, One Hundred Fourth Congress, second session, February 28, 1996 (1996). 26 Nisan 2012 tarihinde Internet Archive Bilgi Portalı: http://www.archive.org/stream/economicespionag00unit/economicespionag00unit_djvu.txt adresinden alındı.

IOSS (1996). *Intelligence Threat Handbook*. Pennsylvania: DIANE Publishing Company.

ISIS (2011). Stuxnet Malware and Natanz: Update of ISIS December 22, 2010 Report, haberi 25 Ocak 2012 tarihinde ISIS Bilgi Portalı: <http://isis-online.org/isis-reports/detail/stuxnet-malware-and-natanz-update-of-isis-december-22-2010-reportsupa-href1/8> adresinden alınmıştır.

İyibozkurt, E. (1995). *Uluslararası İktisat Teori ve Politika*. Bursa.Ezgi Kitapevi.

Jain, S. , Kaur, G. ve Jain, V.K. (2010). Intellectual Property and Intellectual Property Rights. *Journal of Pharmaceutical Sciences & Research*. vol.2(5), s.314-316.

Kara, M. (2012). Elektrik Üretim ve Dağıtım Sistemleri SCADA Güvenliği. 30 Ocak 2012 tarihinde TUBİTAK BİLGEM Bilgi Portalı: <http://www.bilgiguvenligi.gov.tr/siber-savunma/elektrik-uretim-ve-dagitim-sistemleri-scada-guvenligi.html> adresinden alındı.

Karadeli, C. (2003). Küreselleşme ve Dünya Düzenleri. C. Karadeli (Ed). *Küreselleşme ve Alternatif Küreselleşme*, içinde (s.3-23). Ankara: Phoenix Yayınevi.

Kaplan, İ. (1990). Banka Gizliliği-Bankanın Sır Saklama Borcu. *BATİDER* c.XV s.3–22.

Karahan, S. , Suluk, C. , Saraç, T. ve Nal T. (2011). *Fikri Mülkiyet Hukukunun Esasları*. Ankara:Seçkin Yayıncılık.

Kırca, Ç. (1998). Know-How Sözleşmesinin Hukuki Niteliği Prof. Dr. Ali Bozer'e Armağan, Ankara 1998, s. 243- 268.

Kobler, S. (1992). The CIA As Economic Spy: The Misuse of U.S. Intelligence After the Cold War. 27 Nisan 2012 tarihinde CATO Institute Bilgi Portalı: <http://www.cato.org/pubs/pas/pa-185.html> adresinden alındı.

Köni, H. (1999). Soğuk Savaş ve Sonuçları. *Avrasya Dosyası Uluslararası İlişkiler ve Stratejik Araştırmalar Dergisi*, cilt.5, sayı.4, s.76-88.

Krotoski, M. L. (November 2009). Common Issues and Challenges in Prosecuting Trade Secret and Economic Espionage Act Cases. *United States Attorneys' Bulletin*. vol 57, no.5, ss.2-23.

Kumbasar, A.H.(2010). TEMPEST. *TÜBİTAK UEKAE Dergisi*, cilt.2,sayı.3, s.21-27.

Lall, S. (2003). Foreign Direct Investment, Technology Development and Competitiveness: Issues and Evidence. Lall, S ve Urato S. (2003) *Competitiveness*,

TASNİF DIŞI

FDI and Technological Activity in East Asia, içinde s.12-56. Northampton: Edward Elgar Publishing.

Larson, J. S. (2010). Enforcing Intellectual Property Rights to Deter Phishing. *Intellectual Property & Technology*. vol.22, no.1, s.1-7.

Loganathan, M. ve Kirubakaran, E. (2011). A Study on Cyber Crimes and Protection. *International Journal of Computer Science Issues*. Vol.8, Issue.5, No.1, s.388-393.

Los Angeles Times (17 January 1991). "Alfred Frauenknecht; Convicted of Selling Jet Secrets to Israel" haberi, 25 Nisan 2012 tarihinde Los Angeles Times Bilgi Portalı: http://articles.latimes.com/1991-01-17/news/mn-489_1_alfred-frauenknecht adresinden alındı

Macrakis, K. (2010). Technophilic Hubris and Espionage Styles During Cold War. *Isis*. Vol. 101, no.2, ss. 375-385. 08 Ağustos 2011 tarihinde JSTOR Bilgi Portalı: <http://www.jstor.org/stable/10.1086/653104> sitesinden alındı.

Manning, M.J. (2012). Economic Espionage. 04 Nisan 2012 tarihinde <http://www.faqs.org/espionage/Ec-Ep/Economic-Intelligence.html> adresinden alındı.

McAfee (2004). Anti-Phishing: Best Practices for Institutions and Consumers. 18 Ocak 2012 tarihinde Bilgi Portalı: <http://www.antiphishing.org/resources.html> adresinden alındı.

Mijalkovic, S. ve Milosevic G. (2011). Correlation Between Economic Corporate and National Security. *Megatrend Review*, vol.8 (2), s.437-454.

MİT (2012). İKK ve Koruyucu Güvenlik Birimleri. 26 Nisan 2012 tarihinde MİT Bilgi Portalı:http://www.mit.gov.tr/ikk_seminer.html adresinden alındı.

Mitnick, K.(2009). *Aldatma Sanatı*. Ankara: ODTÜ Yayıncılık.

Moore, T. (2010). The Economics of Cybersecurity: Principles and Policy Options. *International Journal of Critical Infrastructure Protection*, 3 (2010), ss.103-117.

Mosier, M. (2001). Causes of Action for Foreign Victims of Economic Espionage abroad by U.S.. Intelligence. *Duke Journal of Comperative & International Law*, vol.11, no.2, s.427-450.

Nabbali, T. ve Perry, M. (2004). Surveillance Systems. Going fort he Throat: Carnivore in an ECHELON World-Part II. *Computer Law & Security Report*. vol.20, no.2, s.84-96.

Naisbitt, J. ve Aburdene P. (2000). *Megatrends 2000: Ten New Directions for the 1990's*. New York: Avon Books.

Nart, S. (2009). Rekabetin Korunması Kapsamında Fikri ve Sınai Hakların Korunması. *Dokuz Eylül Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*. cilt.11, sayı.1, s.113-146.

Nasheri, H. (2005). *Economic Espionage and Industrial Spying*. New York: Cambridge University Press.

NCC (1995). Annual Report To Congress On Foreign Economic Collection And Industrial Espionage

TASNİF DIŞI

NCC (1997). Annual Report To Congress On Foreign Economic Collection And Industrial Espionage.

Nebioğlu, H. (2001). *Tekstil ve Hazır Giyim Ticareti*. Ankara: DTM

NTVMSNBC (2010). "İran Santraline Siber-Saldırı" haberi 25 Ocak 2012 tarihinde NTVMSNBC Bilgi Portalı: <http://www.ntvmsnbc.com/id/25135114/> adresinden alınmıştır.

ODTÜ Bilgisayar Topluluğu Elektronik Dergisi (2007).Toplum Mühendisliği, makalesi 13 Aralık 2011 tarihinde Bilgi Portalı: <http://e-bergi.com/2007/Haziran/Toplum-Muhendisligi> adresinden alındı.

OECD (2008). *Malicious Software (Malware): A Security Threat to the Internet Economy*. Ministerial Background Report. DSTI/ICCP/REG(2007)5/FINAL.

ONCIX (2001). Annual Report To Congress On Foreign Economic Collection And Industrial Espionage.

ONCIX (2002). Annual Report To Congress On Foreign Economic Collection And Industrial Espionage.

ONCIX (2003). Annual Report To Congress On Foreign Economic Collection And Industrial Espionage.

ONCIX (2009-2011). *Foreign Spies Stealing US Economic Secrets In Cyberspace*. Report to Congress on Foreign Economic Collection and Industrial Espionage.

Oran, B. (2002). *Türk Dış Politikası, Kurtuluş Savaşından Bugüne Olgular, Belgeler, Yorumlar Cilt II:1980-2001*. İstanbul: İletişim Yayınları.

Osborn, A. (2002). "Sweden Expels Russian Jet 'Spies'" haberi, 29 Nisan 2012 tarihinde The Guardian Bilgi Portalı: <http://www.guardian.co.uk/world/2002/nov/12/russia.andrewosborn> adresinden alındı.

Ottekin, F. (2008). Bilgi Güvenliğinde ISO 27000 Standartlarının Yeri ve Öncelikli ISO 27002 Kontrolleri. 30 Ocak 2012 tarihinde TUBİTAK BİLGEM Bilgi Portalı: <http://www.bilgiguvenligi.gov.tr/teknik-yazilar-kategorisi/bilgi-guvenliginde-iso-27000-standartlarinin-yeri-ve-oncelikli-iso-27002-kontrolleri.html> adresinden alındı.

Owens, A. W. , Dam, K. W. ve Lin H. S. (2009). *Technology, Policy, Law and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*. Washington: The National Academies Press.

Önel, D. ve Dinçkan, A. (2007). Bilgi Güvenliği Yönetim Sistemi Kurulumu. TUBİTAK UEKAE Doküman Kodu: BGYS-0001. 30 Ocak 2012 tarihinde TUBİTAK Bilgi Portalı: <http://www.bilgiguvenligi.gov.tr/bilgi-guvenligi-yonetimi-dokumanlari/uekae-bgys-0001-bilgi-guvenligi-yonetim-sistemi-kurulum-kilavuzu.html> adresinden alınmıştır.

Özdağ, Ü. (2009). *İstihbarat Teorisi*. Ankara: Kripto Yayıncılık.

Özdemir, E. (2010). Rekabet İstihbaratı Toplama ve Etik: Bir Alan Araştırması. *İ.Ü. Siyasal Bilgiler Fakültesi Dergisi*, no.43, s.67-95.

Öztürk, G. (2008). Bilgi Güvenliği Politikası Oluşturma Kılavuzu. TUBİTAK UEKAE Doküman Kodu: BGYS-0005. 29 Ocak 2012 tarihinde TUBİTAK Bilgi Portalı:

TASNİF DIŞI

<http://www.bilgiguvenligi.gov.tr/bilgi-guvenligi-yonetimi-dokumanlari/uekae-bgys-0005-bilgi-guvenligi-politikasi-olusturma-kilavuzu.html> adresinden alındı.

Paallysaho, S. ve Kuusisto, J.(2011). Informal Ways to Protect Intellectual Property (IP) in KIBS Business. *Innovation: Management, Policy & Practice*, vol.13, issue.1, s.62-76.

Poltorak, A. ve Lerner, P. (2002). *Essentials of Intellectual Property*. New York: John Wiley & Sons.

Porteous, S. (1995). Archived: Commentary No. 59: Economic / Commercial Interests and Intelligence Services, makalesi 04 Nisan 2011 tarihinde CSIS Bilgi Portalı: <http://www.csis-scrs.gc.ca/pblctns/cmmntr/cm59-eng.asp> adresinden alındı.

Porter, M.E. (1990). The Competitive Advantage of Nations. *Harvard Business Review*, March-April, s.71-91.

Porter, M.E. (2007). *Rekabet Stratejisi: Sektör ve Rakip Analizi Teknikleri*. İzmir: Sistem Yayıncılık.

Quinto, D.W. ve Singer, S.H. (2009). *Trade Secrets.Law and Practice*. New York: Oxford University Press.

Ramcharan, R. (2005). Intellectual Property and Security. *Contemporary Security Policy*. vol.26, no.1, s.126-159.

Reilly, T. (November 2009). Economic Espionage Charges Under Title 18 U.S.C. § 1831: Getting Charges Approved and The “Foreign Instrumentality” Element. *United States Attorneys’ Bulletin*. vol 57, no.5, ss.24-26.

Richardson, L. ve Luchsinger, V. (Summer 2007). Strategic Marketing Implications in Competitive Intelligence and Economic Act Of 1996. *The Journal Of Global Business Issues*, vol.1, issue.2, ss.41-45.

Rivero, O. D. (2003). *The Myth of Development: Non-Viable Economies of the 21st Century*. London: Zed Books.

Roche, E. M. (2007). *Corporate Spy: Industrial Espionage and Counterintelligence in the Multinational Enterprise*. New York: Barraclough Ltd.

“Saldırı Gelişmişliği-Saldırgan Bilgi Düzeyi”. 31 Ocak 2012 tarihinde Bilgi Portalı: <ftp://ftp.dtm.gov.tr/Etik/sunular/uekae.pdf> adresinden alınarak düzenlendi.

Samli, A. C. ve Jacobs L. (2003). Counteracting Global Industrial Espionage: A Damage Control Strategy. *Business and Society Review*. 108:1 ss.95-113.

Sapancalı, F. (2001). Yeni Dünya Düzeni ve Küresel Yoksulluk. *Dokuz Eylül Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*. cilt 3, sayı:2, s.115-140.

Saraç, U. (2010). TEMPEST’in Keşfi ve Sinyal Analizi. *TÜBİTAK UEKAE Dergisi*, cilt.2,sayı.3, s.29-34.

Sauver, J. S. (2008). Bots, Malware, and What We Need From Uncle Sam. 31 Ocak 2012 tarihinde University of Oregon Bilgi Portalı: <http://www.uoregon.edu/~joe/unclesam/> adresinden alındı.

Schweizer, P. (1996). The Growth of Economic Espionage: America is Target Number One. *Foreign Affairs*.vol.75, no.1, ss.9-14.

TASNİF DIŞI

Scheffer, G. ve Zieger, M. (2005). Methods for Patent Valuation. *International Conference on "IP as an Economic Asset: Key Issues in Exploitation and Valuation"* 28 Nisan 2012 tarihinde OECD Bilgi Portalı: <http://www.oecd.org/dataoecd/34/63/35428822.pdf> adresinden alındı.

SCIP (2012). How large is the CI market? 04 Nisan 2012 tarihinde SCIP Bilgi Portalı: <http://www.scip.org/resources/content.cfm?itemnumber=601&navItemNumber=533> adresinden alındı.

Scott, R. D. (1999). Territorially Intrusive Intelligence Collection and International Law. *Air Force Law Review*, 1999, Cilt 46. 25 Nisan 2012 tarihinde EBSCOhost Bilgi Portalı: <http://web.ebscohost.com/ehost/detail?vid=5&hid=111&sid=544432ea-23f1-4ce7-ba8b-a6b614089b96%40sessionmgr110&bdata=Jmxhbm9dHlmc2l0ZT1l aG9zdC1saXZl#db=lgh&AN=12601647> adresinden alındı.

Shearer, R. (2007). *Business Power: Creating New Wealth from IP Assets*. New Jersey: John Wiley & Sons Inc.

SIPRI (2012). "Dünya Geneline Askeri Harcamalar". 16 mart 2012 tarihinde SIPRI Bilgi Portalı: <http://milexdata.sipri.org/files/download/?key=49d7f01921ce1b27a62c2709af532d7f&file=SIPRI+milex+data+1988-2010.xls> adresinden alınarak düzenlendi.

Sloan, L. D. (2001). ECHELON and the Legal Restraints on Signals Intelligence: A Need for Reevaluation. *Duke Law Journal*, vol.50, no.5, s.1467-1510.

Sommer, P. ve Brown, I. (2011). *Reducing Systemic Cybersecurity Risk*. OECD/IFP Project on "Future Global Shocks". IFP/WKP/FGS(2011)3.

Soyak, A. (2005). Fikri Ve Sınâî Mülkiyet Hakları: Tanımı, Tarihsel Gelişimi ve GOÜ'ler Açısından Önemi. *Legal Fikri ve Sınâî Haklar Dergisi*, Yıl:1, Sayı:1, s.11–30

Sönmezoğlu, F. (2000). *Uluslararası İlişkiler Sözlüğü*. İstanbul: Der Yayınları.

Stanley, R. (2010). *Information Security*. Ghosh, S. ve Turrini, E (Ed.). *Cybercrimes: A Multidisciplinary Analysis*, içinde, s.95-126. Berlin: Springer

Stewart, P. (1994). *Role of the U.S. Government in Industrial Espionage*. Washington: National Defense University.

Stiblar, F. (2005). *Preservation of National Identity and Interests in the Enlarged EU, Discussion Paper*. Bonn: Center for European Integration Studies.

Süel, S. (2007). *Türk ve Avrupa Birliği Hukukunda Patent Hakkının Tükenmesi*. Yayınlanmamış Yüksek Lisans Tezi.

Symantec (2008). Report on the Underground Economy July 07- June 08. 11 Ocak 2012 tarihinde Symantec Bilgi Portalı: <http://www.symantec.com/business/threatreport/archive.jsp> adresinden alındı

Symantec (2011). Intelligence Report: November 2011, s.5. 11 Ocak 2012 tarihinde Symantec Bilgi Portalı: http://www.symanteccloud.com/globalthreats/overview/r_mli_reports?om_ext_cid=biz_socmed_twitter_facebook_marketwire_linkedin_2011Nov_worldwide_intelligencer_eportnov2011 adresinden alındı.

Syngress (2009). *Securing Intellectual Property. Protecting Trade Secrets and Other Information Assets*. Burlington: Syngress Publishing.

TASNİF DIŞI

Tekinalp, G. ve Tekinalp, Ü.(2000). *Avrupa Birliği Hukuku* İstanbul: Beta.

Temporary Committee on the ECHELON Interception System (11 July 2001). Report on the Existence of a Global System for the Inteception of Private and Commercial Communications, Part I. European Parliament Session Document A5-0264/2001

The Guardian (2005). London Couple Remanded in Israel's Biggest Industrial Espionage Case, haberi 10 Ocak 2012 tarihinde Bilgi Portalı: <http://www.guardian.co.uk/world/2005/may/31/israel> adresinden alındı.

The Japan Times Online (2005). Russian Trade Official Accused of Buying Toshiba Chip Secrets” haberi 29 Kasım 2011 tarihinde Bilgi Portalı: <http://www.japantimes.co.jp/text/nn20051021a2.html> adresinden alındı.

The New York Times (2010) Hilton and Starwood Settle Dispute, haberi 10 Ocak 2012 tarihinde Bilgi Portalı:<http://dealbook.nytimes.com/2010/12/22/hilton-and-starwood-settle-dispute/> adresinden alındı.

The Phoenix Journal (2000). ECHELON Exposed-Proof of No Privacy haberi 05 Nisan 2012 tarihinde <http://www.phoenixsourcedistributors.com/000228.pdf> adresinden alındı.

The Silver Lake Editors (2004). *The Value of a Good Idea: Protecting Intellectual Economy in an Information Economy*. Los Angeles: Silver Lake Publishing.

The White House (July 1994). A National Security Strategy of Engagement and Enlargement. 19 Nisan 2012 tarihinde ABD Savunma Bakanlığı Bilgi Portalı: <http://history.defense.gov/resources/nss1994.pdf> adresinden alınmıştır.

The World Bank (2012). Dünya GSYH Sıralamasında İlk Beş Ülke (2010). 21 Mart 2012 tarihinde The World Bank Bilgi Portalı: <http://data.worldbank.org/indicator/NY.GDP.MKTP.CD> adresinden alınarak düzenlendi.

TOBB. Teknoloji Geliştirme ve Yenilik Destekleri Rehberi. 29 Şubat 2012 tarihinde TOBB Bilgi Portalı: http://www.tobb.org.tr/Documents/yayinlar/Teknoloji_Gelistirme_ve_Yenilik_Destekleri_Rehberi_.zip adresinden alındı.

Todd, P. ve Bloch, J. (2004). *Global Intelligence: The World's Secret Service Today*. London: Zed Books.

Toffler, A. (1981). *Üçüncü Dalga*. İstanbul: Altın Kitaplar Yayınevi.

Toffler, A. ve Toffler, H. (1994). 21. *Yüzyılın Şafağında Savaş ve Savaş Karşısı Mücadele*. İstanbul: Sabah Kitapları.

Topçu, D. (2007). *Sınai Mülkiyet Hakları Aleyhine İşlenen Suçlar*. Ankara:Seçkin Yayıncılık.

Trabelsi, Z. (2005). Switched Network Sniffers Detection Technique Based on IP Packet Routing. *Telecommunications, Network and Internet Security*, vol.14, issue.4, s.51-60.

Tsang, R.(2009). Cyberthreats, Vulnerabilities and Attacks on SCADA Networks. 30 Ocak 2012 tarihinde University of California, Berkeley Bilgi Portalı: http://gspp.berkeley.edu/iths/working_papers.html adresinden alındı.

TASNİF DIŐI

TPE (Ekim 2011). Endüstriyel Tasarımlar Tescili Kullanıcı Rehberi ve Başvuru Kılavuzu. 05 Mart 2012 tarihinde TPE Bilgi Portalı: http://www.turkpatent.gov.tr/dosyalar/yayinlar/basvuru_kilavuz/TASARIM_BK.pdf adresinden alındı.

TPE (2012a). Fikri Haklar Dünyanız. 29 Şubat 2012 tarihinde TPE Bilgi Portalı: <http://www.turkpatent.gov.tr/dosyalar/yayinlar/bilgikitapcıkları/fikrihaklardunyaniz.pdf> adresinden alındı.

TPE (2012b). Rüçhan Hakkı Nedir? 01 Mart 2012 tarihinde TPE Bilgi Portalı: <http://www.tpe.gov.tr/portal/default2.jsp?sayfa=125&konu=18> adresinden alındı.

TSE (2012). Ortak Kriterler Belgelendirilen Ürünler. 30 Ocak 2012 tarihinde TSE Bilgi Portalı: <http://bilisim.tse.org.tr/standartlar/ortakkriterler/urunler> adresinden alınmıştır.

TÜBİTAK UEKAE (2011). “Açıklık” ve “İstenmeyen e-posta (spam)” terimlerinin anlamı, 28 Aralık 2011 tarihinde, TÜBİTAK UEKAE Bilgi Portalı: <https://www.bilgiguvenligi.gov.tr/olay-sozlugu.html> adresinden alındı.

TÜBİTAK (2012). Ortak Kriterler. 29 Ocak 2012 tarihinde TÜBİTAK Bilgi Portalı: http://www.bilgiguvenligi.gov.tr/index.php?option=com_easyfaq&task=cat&catid=63&Itemid=99999999#faq39 adresinden alınmıştır.

TÜBİTAK (2012b). “Biz Kimiz?”, 27 Nisan 2012 tarihinde TÜBİTAK Bilgi Portalı: <http://www.uekae.tubitak.gov.tr/home.do?sessionId=87E2A93D02E7C4207CF2619247736A23?ot=1&sid=2> adresinden alındı.

Tzu, S. (1996). *Savaş Sanatı*. İstanbul: Anahtar Kitaplar.

Ulukan, H. (2007). Klasik Bitki Islahı ve Genetik Mühendisliği ile Oluşturulan Değişimlere Genel Bakış. *Uludağ Üniversitesi Ziraat Fakültesi Dergisi*, 2007, Cilt 21, Sayı 2, 27-40.

UNICEF (2011). *Global Inequality: Beyond the Bottom Billion a Rapid Review of Income Distribution in 141 Countries*. Social and Economic Policy Working Paper

Usluel, A.G. (2009). *Türk Özel Hukukunda Özellikle Anonim Şirketlerde Ticari Sırrın Korunması*. İstanbul: Vedat Kitapçılık.

Uşan, F. (2003). *İş Hukukunda İş Sırrının Korunması (Sır Saklama ve Rekabet Yasağı)*. Ankara: Vedat Kitapçılık.

Ünsal, Ş.(1993). *Free Trade Agreements and North American Free Trade Agreement*. Maliye Araştırma Merkezi Konferansları Otuzbeşinci Seri-Yıl 1991/1992, Prof. Dr. Bedî N. Feyzioğlu'na Armağan, içinde s.284-295. İstanbul: İstanbul Üniversitesi İktisat Fakültesi.

Ünsal, Ş. (2003). *Uluslararası İlişkilerin Asya ve Uzak Doğudaki Boyutları ve Japonların Yeni Rolü*. İstanbul: Set Yayınları.

Whittaker, J. (2004). *The Cyberspace Handbook*. London:Routledge.

WND (2004). “French Economic Spies Target U.S.” haberi 27 Nisan 2012 tarihinde WND Bilgi Portalı: <http://www.wnd.com/2004/12/27966/> adresinden alındı.

Yakın, A. (1969). *İstihbarat, Casusluk ve Casuslukla Mücadele*. Ankara: Dış İşleri Akademisi Yayını.

TASNİF DIŐI

Yılmaz, S. (2007). 21. Yüzyılda Güvenlik ve İstihbarat. İstanbul:Milenyum Yayınları.

Yılmaz, M.A. (2008). "The New World Order": An Outline of the Post-Cold War Era. *Alternatives*. vol.7, no.4, s.44-58.

Yılmaz, S. ve Salcan, O. (2008). *Siber Uzay'da Güvenlik ve Türkiye*. İstanbul: Milenyum Yayınları.

WIPO (2011a). IP Facts and Figures. 27 Şubat 2012 tarihinde WIPO Bilgi Portalı: http://www.wipo.int/pressroom/en/articles/2011/article_0021.html adresinden alındı.

WIPO (2011b). *World Intellectual Property Indicators*. WIPO Economics & Statistics Series.

WIPO (2012a). Understanding Industrial Property. 27 Şubat 2012 tarihinde WIPO Bilgi Portalı: <http://www.wipo.int/about-ip/en/> adresinden alındı.

WIPO (2012b). Total number of Contracting Parties: 174. 12 Mart 2012 tarihinde WIPO Bilgi Portalı: http://www.wipo.int/treaties/en/statistics/StatsResults.jsp?treaty_id=2 adresinden alındı.

ÖZGEÇMİŐ

Bölent Sungur, 1977 yılında Ankara’da doğmuştur. 1997 yılında Maltepe Askeri Lisesi’nden, 2002 yılında Kara Harp Okulu’ndan Jandarma Teğmen rütbesi ile mezun olmuştur. 2004-2005 yılları arasında Mardin/Nusaybin Jandarma Asayiş Komando Bölüğü’nde Tim Komutanı, 2005-2007 yılları arasında Mardin/Dargeçit Jandarma Asayiş Komando Bölük Komutanı, 2007-2010 yılları arasında Manisa/Kırağaç 6’ncı Jandarma Komando Eğitim Alayı’nda Bölük Komutanlığı görevinde bulunmuştur. 2010 yılında Harp Akademileri Stratejik Araştırmalar Enstitüsü Uluslararası İlişkiler Ana Bilim Dalı’nda başladığı İstihbarat Yüksek Lisans Eğitimi’ne devam etmektedir. Bölent Sungur, evli ve bir çocuk sahibi olup, İngilizce bilmektedir.

(BU SAYFA BOŞ BIRAKILMIŞTIR.)