

T.C.

GEBZE YÜKSEK TEKNOLOJİ ENSTİTÜSÜ

SOSYAL BİLİMLER ENSTİTÜSÜ

137322

BİLGİ SAVAŞI NEDİR?
BİLGİ SAVAŞLARININ TÜRKİYE'NİN BİLİM
TEKNOLOJİ POLİTİKALARI VE SAVUNMA
STRATEJİLERİNE ETKİLERİ

T.C. YÜKSEKÖĞRETİM KURULU
DOKÜMANTASYON MERKEZİ

Eşref ÖZDEMİR
YÜKSEK LİSANS TEZİ
STRATEJİ BİLİMİ ANABİLİM DALI

TEZ DANIŞMANI
Prof.Dr.Abdülkadir AKÇİN

GEBZE

2003



Eşref ÖZDEMİR'in tez çalışması, G.Y.T.E. Sosyal Bilimler Enstitüsü Yönetim Kurulu'nun **14/01/2003** tarih ve **2003/1** sayılı kararıyla oluşturulan jüri tarafından Strateji Bilimi Bölümü .Anabilim Dalında YÜKSEK LİSANS tezi olarak kabul edilmiştir.

JÜRI

ÜYE (Tez Danışmanı) : Prof.Dr. Abdülkadir AKÇİN

ÜYE

Prof.Dr. Yavuz SEZEN

ÜYE

: Yard.Doç.Dr.Halit KESKİN

ONAY

GYTE Sosyal Bilimler Enstitüsü Yönetim Kurulu'nun **23/01/2003** tarih ve **2003/2** sayılı kararı.

ÖZET

Bu çalışmanın amacı bilgi savaşının konseptini tanımlamak ve bilgi savaşının Türkiye'nin savunma stratejileri ve bilim teknoloji politikalarına olan etkilerini araştırmaktır.

Çalışmada, tanımlardan yola çıkılarak, konsept üzerindeki etkiler sistematik olarak incelenmiştir. Özellikle savunma stratejileri ve bilim teknoloji politikalarına olan etkiler geleceğe ilişkin öngörülerle birlikte araştırılmıştır.

Tanımlar, uygulamalar, hedefler, bilgi güvenliği ve kriptoloji ile olan ilişkiler ve bilgi sistemleri düzeyinde etkiler incelenmiş ve bilgi savaşının savaş dışı hareket kavramı içerisinde uygulanabilirliği ortaya konulmuştur.

Teknolojik gelişmeler ve küreselleşmenin bir sonucu olarak bilginin silah olarak kullanıldığı yeni bir boyut ortaya çıkmıştır. Çalışmada gelişmiş ülkelerin stratejileri bu yeni tür savaş kapsamında analiz edilmiştir. Bu stratejiler Türkiye'nin savunma stratejileri ve bilim teknoloji politikalarına yönelik olarak da incelenmiştir. Sonuçların yardımıyla yeni bir bilgi yapılanması stratejisine ulaşmak hedeflenmiştir.

Bilgi toplumuna ulaşmak maksadıyla tasarlanan stratejiler kapsamında alınması gerekli önlemler sonuç olarak ifade edilmiştir. Herşeyin ötesinde de bu çalışma bilgi savaşının bir akademik kavram olarak sunulmasından dolayı önemlidir.

SUMMARY

The aim of this study is to describe the concept of information warfare and figure out the impacts of information warfare on Turkey's defense strategies and Science and Technology Policies.

At the first steps of the study, stemming from the definitions, the impacts that affect the concept were investigated systemically. Especially the impacts of defense strategies and Science and Technology Policies were investigated with expectations in detail

The impacts which are at the level of definition, appliances, targets, relationships with information security and cryptology and information systems were searched and applicability of infowar in the content of operations other than war is exposed.

As a result of technological improvements and globalism, a new dimension were appeared which was used information as a weapon. In the study the strategies of developed societies were analyzed with the concept of a new kind of war. These strategies were investigated with the approaching of Turkey's defense strategies and Science and technology policies It was aimed to reach a new structural information strategy with the help of the conclusions.

In the content of strategy which was designated for the aim of reaching the information society, the requisitions that must be taken were presented finally.

Beyond these issues this study is important because of the presentation of infowar as an academic term.

TEŞEKKÜR

Bu çalışmanın seçim aşamasından tamamlanma aşamasına değin her türlü yönlendirme ve desteğini esirgemeyen danışmanım Prof.Dr. Abdülkadir AKÇİN başta olmak üzere; manevi desteklerinden dolayı eşim Zeynep İlknur ÖZDEMİR'e ve gelecekte bilim yolunda ilerlemesini istediğim oğlum L.Egehan ÖZDEMİR'e, yardımlarından dolayı Lv.Yzb.Hakan EMANET'e, ayrıca beni teşvik ettiklerinden dolayı Lv.Yb.Mehmet COŞKUN ve Lv.Alb.Turgut KOÇ'un şahsında tüm Levazım Okulu personeline teşekkürlerimi sunarım.



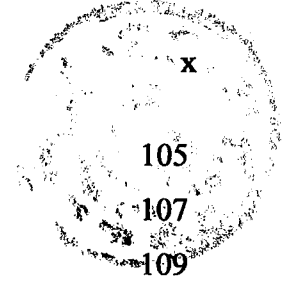
İÇİNDEKİLER DİZİNİ

Sayfa

ÖZET	iv
SUMMARY	v
TEŞEKKÜR	vi
İÇİNDEKİLER DİZİNİ	vii
SİMGELER VE KISALTMALAR DİZİNİ	xi
ŞEKİLLER DİZİNİ	xiii
1. GİRİŞ	1
1.1 Bilgi Toplumuna Geçiş	3
1.1.1. Eğitim ve Araştırma	4
1.1.2. Üretim ve Ticaret	5
1.1.3. Kamu Hizmetleri	5
1.1.4. Sağlık Hizmetleri	6
1.1.5. Yasama ve Yargıya Yönelik Hizmetler	6
1.1.6. Evlere Hizmet	6
1.1.7. Topluma Yönelik Diğer İletişim ve Bilgi Hizmetleri	7
1.1.8. Akıllı Evler	8
1.2. E-Devlet	11
2. SAVAŞ KAVRAMI	20
2.1. Geleceğin Savaşları	20
2.2. Bilgi Savaşının Hedefleri	27
2.2.1 Politik Hedefler	27
2.2.2.Yapısal Hedefler	27
2.2.3. Askeri Kuvvetler	28
2.3. Senaryo	28
2.2. Bilgi Savaşlarına Uzanan Yol	30
3. BİLGİ SAVAŞI NEDİR?	32
3.1. Bilgi Savaşının Tanımı	32
3.1.1. Bireysel Bilgi Savaşı	32
3.1.2. Şirketlerarası Bilgi Savaşı	34
3.1.3. Küresel Bilgi Savaşları	35

3.2. Bilgi Savaşının Bölümleri	37
3.2.1. Komuta Kontrol Savaşı	37
3.2.2. İstihbarat Temelli Savaş	38
3.2.3. Elektronik Harp	38
3.2.4. Bilgisayar Korsan Savaşı	38
3.2.5. Ekonomik Bilgi Savaşı	38
3.2.6. Kültür Empozesi	39
3.2.7. Beyin Göçü	39
3.2.8. Propaganda/Psikolojik Savaş	39
3.2.9. Siber Savaş	39
3.3. Bilgi Savaşının Özellikleri ve Araçları	40
3.3.1. Bilgisayar Virüsleri	42
3.3.2. Kurtlar	42
3.3.3. Truva Atları	42
3.3.4. Mantık Bombaları	43
3.3.5. Tuzak Kapılar	43
3.3.6. Chipping	43
3.3.7. Nano-Mekanikler ve Mikroplar	43
3.3.8. High Energy Radio Frequency (HERF)	44
3.3.9. Uzaktan Nöral Denetim	45
3.4. Bilgi Savaşının Yöntemleri	48
3.4.1. Warden Modeli	48
3.4.2. Sayısal Bilgi Harekatı	50
3.4.2.1. Devre Dışı Bırakma	51
3.4.2.2. Zayıflatma	51
3.4.2.3. Aldatma	51
3.4.2.4. İstismar Etme	52
3.4.3. Stratejik Felç	54
3.4.4. Dünyanın Gözleri ve Kulakları (ECHELON)	55
3.4.5. Çift Kullanımlı Teknolojiler (GPS)	56
4. TÜRKİYE’NİN BİLGİ SAVAŞINA YÖNELİK KONSEPTİNİN BELİRLENMESİ	58
4.1. Ekonomik, Politik, Sosyal ve Kültürel Yapıda Gelişmeler	59
4.2. Jeopolitik Değerlendirme	63

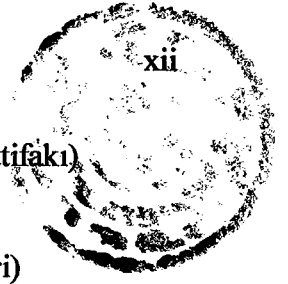
4.2.1. Milli Güvenlik Kavramı	64
4.2.2. İç Tehditler	66
4.2.3. Dış Tehditler	68
4.2.3.1. Yunanistan	69
4.2.3.2. Bulgaristan	70
4.2.3.3. Rusya Federasyonu	70
4.2.3.4. Ermenistan	71
4.2.3.5. Irak	71
4.2.3.6. Suriye	72
4.2.3.7. İran	73
4.3. Türkiye'nin Savunma Stratejisinde Değişiklikler	74
4.4. Türkiye'nin Bilim ve Teknoloji Politikaları	77
4.5. Dünya Devletlerinin Bilgi Savaşı Potansiyeli	83
4.5.1. Amerika Birleşik Devletleri	84
4.5.2. Çin	86
4.5.3. İngiltere	86
4.5.4. Fransa	87
4.5.5. Almanya	87
4.5.6. Rusya Federasyonu	88
4.5.7. Yunanistan	89
4.5.8. İsrail	90
4.6. Türkiye'de Bilgi Savaşı Konusunda Mevcut Durum	91
4.6.1. Savunma Güvenliği	91
4.6.2. Haberleşme Güvenliği	94
4.6.2.1. Radyo Televizyon Yüksek Kurulu (RTÜK)	95
4.6.2.2. Haberleşme Yüksek Kurulu (HYK)	97
4.6.2.3. Telsiz Genel Müdürlüğü (TGM)	97
4.6.2.4. Haberleşme Genel Müdürlüğü (HGM)	98
4.6.2.5. Tr-Net Bürosu	99
4.6.2.6 Kurumsallaşma Çabaları	99
4.7. Bilgi Güvenliğine Stratejik Yaklaşım	100
4.7.1. Savunma ve Saldırı Politikası	101
4.7.2. Yasal Çerçeve ve Toplumsal Mutabakat	102
4.7.3. Kritik Altyapılar	104



4.7.4. Sivil ve Askeri Sanal Güçler	105
4.7.5. Stratejik Sektör ve Ürünler	107
4.8. Bilgi Savaşı Projeleri	109
4.8.1. TAFICS (Turkish Armed Forces Integrated Communication System)	109
4.8.2. Taktik Saha Muharebe Sistemleri (TASMUS) Projesi	109
4.8.3. Türk Silahlı Kuvvetleri Uydu Muharebe Sistemi Projesi	110
4.8.4. Uzun Ufuk Projesi	110
4.9. Konseptin İfadesi	111
5. SONUÇ VE ÖNERİLER	112
KAYNAKLAR	121
ÖZGEÇMİŞ	124
EKLER	
EK-1. Ulusal Bilgi Güvenliği Teşkilatı ve Görevleri Hakkında Kanun Tasarısı Taslağı	

SİMGELER VE KISALTMALAR DİZİNİ

AB	Avrupa Birliđi
AGİT	Avrupa Güvenlik ve İşbirliđi Teşkilatı
ABD	Amerika Birleşik Devletleri
ARGE	Araştırma Geliştirme
BTYK	Bilim ve Teknoloji Yüksek Kurulu
CIA	Central Intelligence Agency (Merkezi Haberalma Ajansı)
C2	Command and Control (Komuta Kontrol)
COMSEC	Communication Security (İletişim Güvenliđi)
COMPUSEC	Computer Security (Bilgisayar Güvenliđi)
CB	Citizen Band (Halk Bandı)
CD	Compact Disc (Kompakt Disk)
DPT	Devlet Planlama Teşkilatı
EDT	Elektronik Destek Tedbirleri
EKT	Elektronik Karşı Tedbirler
EKOT	Elektronik Koruyucu Tedbirleri
EMP	Electro Magnetic Pulse (Elektromanyetik Dalga)
GSMH	Gayri Safi Milli Hasıla
GPS	Global Positioning System (Küresel Yerbulma Sistemi)
GW	Giga Watt (Enerji Birimi)
GHz	Giga Hertz (Frekans Birimi)
HGM	Haberleşme Genel Müdürlüğü
HYK	Haberleşme Yüksek Kurulu
HERF	High Energy Radio Frequency (Yüksek Enerji Radyo Frekansı)
ISDN	Integrated Seviles Digital Network
IMF	International Money Fund (Uluslar arası Para Fonu)
INFOSEC	Information Security (Bilgi Güvenliđi)
MGK	Milli Güvenlik Kurulu
MOSSAD	İsrail Milli İstihbarat Örgütü
MİT	Milli İstihbarat Teşkilatı
MSB	Milli Savunma Bakanlığı
Mİ5	Military Intelligence 5 (İngiltere Askeri İstihbarat Örgütü)



NATO	North Atlantic Treaty Organization (Kuzey Atlantik İttifakı)
NSA	National Security Agency (Milli Güvenlik Ajansı)
NEV	National Elements of Value (Milli Değer Parametreleri)
ODTÜ	Ortadoğu Teknik Üniversitesi
ÖSYM	Öğrenci Seçme ve Yerleştirme Merkezi
PKK	Sözde Kürdistan İşçi Partisi
PTT	Posta Telgraf Telefon İdaresi
RTÜK	Radyo Televizyon Üst Kurulu
TTGV	Türkiye Teknoloji Geliştirme Vakfı
TSK	Türk Silahlı Kuvvetleri
TÜBİTAK	Türkiye Bilimsel ve Teknik Araştırma Kurumu
TÜBA	Türkiye Bilimler Akademisi
TUENA	Türkiye Ulusal Enformasyon Altyapısı
TESİD	Türk Elektronik Sanayicileri Derneği
TÜBİSAD	Türkiye Bilgi İşlem Hizmetleri Derneği
TÜBA	Türkiye Bilimler Akademisi
TBMM	Türkiye Büyük Millet Meclisi
TEMPEST	Temporary Emanations and Spurious Transmission (Elektromanyetik Sızıntı)
TGM	Telsiz Genel Müdürlüğü
TAFICS	Taktik Saha Muhabere Sistemleri
TASMUS	Turkish Armed Forces Integrated Communication System
ULAKNET	Ulusal Akademik Ağ ve Bilgi Merkezi
UEKAE	Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü
YÖK	Yüksek Öğrenim Kurumu

ŞEKİLLER DİZİNİ

Sekil

3.1. Nöromanyetik Silahların Etkileri

3.2. 5 Halkalı Warden Modeli

Sayfa

47

49



1. GİRİŞ

Yirmi birinci yüzyıla girdiğimiz şu günlerde dünyamız, bilgi teknolojisindeki gelişmeler nedeniyle inanılmaz hızda bir değişime sahne olmaktadır. Elektronik ve bilgi sistemleri alanındaki gelişmeler dünyamızı adeta küresel bir köy haline getirmiştir. Bu küresel köyde meydana gelen olaylar, içinde yaşayan birer fert olarak bizleri her yönüyle etkilemekte ve küresel boyutlu etkinliklere yön vermektedir. Günlük işlerimizi yürütürken İnternette girdiğimiz herhangi bir web sayfası, küresel köy olgusunu güçlü bir biçimde ortaya koymakta; yanımızdan ayırmadığımız wap sistemli cep telefonları iletişimin ne derece inanılmaz sürat ve boyutlarda dünyanın bir ucundan diğer ucuna sağlandığının en büyük kanıtı olmaktadır. İçinde bulunduğumuz akıl almaz bir hızla gelişmekte ve değişmekte olan bu dönemi en iyi ifade eden tanımlama “Bilgi Çağı” tanımlaması olmaktadır. Bilgi devrimi cep telefonları, entegre devreler, ATM’ler, barkodlu yazar kasalar, televizyon ve bilgisayar gibi ürünleri günlük hayata sokmuş ve “Bilgi Toplumu” diye adlandırılan yeni bir toplum yapısı ortaya çıkmıştır (TSK Bilgi Harbine Nasıl Hazırlanmalıdır?, 1999, s. 3).

Bilgisayar, bireylerin günlük yaşantısına oldukça fazla miktarda girmiş, bankacılık, borsa, eğitim, ulaştırma, iletişim, medya, enerji ve savunma sektörleri gibi en hayati sektörler, bilgi sistemleri olmaksızın işleyemez hale gelmiştir. Bilgisayar, uydu ve telefon, mesafeleri ortadan kaldırmış, bilgi çağı ile birlikte küreselleşme kavramı da ortaya çıkmıştır. Küreselleşen dünyamızda sadece bireyler ve toplumlar değil, devletler de birbirleriyle bilgi sistemleri vasıtasıyla etkileşim içine girmişlerdir. Henüz gelişmekte olan ve bu teknolojik gelişmenin gerisinde kalan devletler, sözü edilen teknolojik devrimde başı çeken ülkelere rekabet güçlerinin olmayışından dolayı gittikçe artan bir oranda bağımlı olmaya başlamışlardır. Bu bağımlılık, ekonomik, psiko-sosyal, kültürel, bilimsel ve teknolojik güç gibi milli güç unsurlarından her birini etkiler durumda iken, askeri güç söz konusu olduğunda daha da büyük bir önem arz etmektedir. Geçmişte ülkelerin milli stratejileri kullandıkları ya da kullanacakları teknolojiyi belirlerken, günümüzde teknolojinin stratejiyi belirlediği fikri tartışılır olmuştur (TSK Bilgi Harbine Nasıl Hazırlanmalıdır?, 1999, s. 4).

Yirminci yüzyılın son çeyreğinden itibaren teknolojinin üretim sistemlerine olan etkisiyle teknoloji-lider ülkelerde ürün çeşitlemesi artmış otomasyon sistemlerinin de etkisiyle özellikle sanayide yığınsal üretime geçilmiştir. Kendi iç pazar taleplerini kolaylıkla karşılayan bu ülkeler ürünlerini pazarlayacak yeni alanların arayışına girmiştir. Ekonomik amaçlarını politik amaçlarına paralel kılarak, bu pazar mücadelesinde yer kapmak için kendi ülkelerinin bütün dinamiklerini (milli güç unsurları) harekete geçirmişlerdir. Ürünlerini pazarlayabilmek için askeri güç dahil her türlü yöntemi deneyen teknoloji-lider ülkeler emperyalizmin yeni bir boyutuyla karşımıza çıkmışlardır. Nüfuz alanlarındaki mücadele siyasi, ekonomik, kültürel, psiko-sosyal ve askeri faaliyetlerde yoğunluk kazanmıştır. Hem mücadelenin alanı genişlemiş hem de şiddeti artmıştır. Bilgi teknolojilerindeki gelişim paralelinde, savaş kavramı da değişmeye başlamıştır. Artık savaş bir milli devletin veya devletler grubunun ordularının birbirleriyle çarpışması olarak düşünemeyiz. Milli devletin savaş yapma üzerindeki tekeli kalmamıştır. Bir takım diğer unsurlar, örneğin, şirketler, dini gruplar, terörist organizasyonlar, uyuşturucu kartelleri, bilgisayar korsanları (hackerler) yeni tehdit kapsamına girmişlerdir.

Genel anlamda bilginin artık küresel bir mahiyet göstermesine karşılık, bilimsel bilgi; küresel ticari rekabette ve nüfuz mücadelesinde kritik hüviyeti nedeniyle stratejik bir özellik ve önem kazanmış, küresel güçlerin adeta odak noktası olmuştur. (Ayhan, 2002, s. 308)

Günümüzde ülkeler; bilgi teknolojilerinin nimetlerinden en üst düzeyde faydalanabileceği gibi, aynı zamanda, teknoloji tabanlı yeni bir mücadelenin yani bilgi savaşının hedeflerinden biri haline de gelmiştir.

Sonuç olarak bilginin gittikçe daha değerli bir hale geldiği günümüzde, alt yapısında bilgi sistemleri bulunan her sahayı hedef alan yeni bir savaş türü olan Bilgi Savaşları ortaya çıkmıştır. Bu araştırmada bu savaş türü hakkında bilgi verilmekte, gelecekte bu mücadelenin nasıl şekilleneceği ve bir milli devlet olarak Türkiye'nin nasıl hazırlanması gerektiği ortaya konmakta; bu maksatla hayata geçirilen projeler incelenmekte ve asker-sivil toplumun her kesiminin sorumlulukları irdelenmektedir.

1.1 Bilgi Toplumuna Geçiş

Sanayi devriminin toplumsal yaşamımıza getirdiği değişikliklere benzer bir süreç günümüzde de yaşanmaktadır. Ancak farklı olan bu sürecin daha kısa zamanda ve daha yoğun yaşanmasıdır. Teknolojik gelişimin üretim tekniklerini ve metotlarını etkilemesi sonucunda 1970'lerden sonra hızlı bir değişim başlamıştır. Yirminci yüzyılın son çeyreğinde bilgi teknolojisi popüler hale gelmiş ve bilgi dördüncü üretim faktörü olarak ekonomik sisteme dahil edilmiştir. Yirminci yüzyılın başlarında, tarım toplumundan sanayi toplumuna dönüşüm gerçekleşmiştir. Sanayi toplumundan bilgi toplumuna geçiş aşaması ise bilgi teknolojisi alanında lider sayılan ülkelerde, yirminci yüzyılın son çeyreğinde başlamıştır. Bilgisayar donanım ve yazılım alanındaki gelişmeler, bu ülkelerde bilginin toplanması, saklanması, işlenmesi ve yeniden saklanması alanlarında teknolojik imkanlar yaratmış; telekomünikasyon alanındaki gelişmelerle bilgi alışveriş süreci başlamış özellikle İnternet ortamından yararlanılarak uluslararası bilgi edinme ve kullanım olanakları üst seviyeye çıkartılmıştır. Sanal ortamda oluşturulan bilgi süper otoyolu (information superhighway) ile toplumların bilgi çağına geçiş süreci daha da hızlandırılmıştır (İlyasoğlu, 1997, s. 3).

Her ekonomik-tarihsel dönemde bir endüstri kolu, o döneme damgasını vurmuş ve ekonomik gelişmelerin hızlanmasına yol açarak; bu gelişmelerden faydalanan ülkeleri, diğerlerinden daha önce refaha ulaştırmıştır (İlyasoğlu, 1997, s. 5). Dikkatli incelendiğinde ekonomik gelişmelerin hep bir süreç sonrasında ortaya çıktığını ve toplumsal bir değişime (transformation) eşzamanlı olarak yürüdüğünü görmekteyiz. Genellikle bilgi üretimiyle başlayan bu değişim, üretim metotlarını etkileyerek, nihayetinde kitlesel üretimlerle mal ve hizmetlerin yaygın olarak kullanıma sunulmasıyla sonuçlanmaktadır.

İnsanlık tarihini yakından incelediğimizde buna benzer değişim-dönüşüm süreçlerinin genellikle uzun bir zamana yayıldığı görülmektedir. Örneğin sanayi toplumunun oluşması yüz yıla yakın bir zaman almıştır ve hala dünyanın pek çok bölgesinde bu süreci hatta sanayi öncesi süreci yaşayan toplumlar bulunmaktadır. Bilgi toplumuna geçişin en belirgin özelliği ise bu sürecin çok kısa bir sürede gerçekleşmesi ve süratle genelleşmesidir. Bunun sebebi ise günümüz insanının teknolojik gelişmelere olan uyum hızının yüksek olmasındandır. Her geçen gün daha

fazla eğitim ve iletişim imkanı bulabilen günümüz insanının teknolojik yenilikler konusunda bilinç düzeyi daha yüksektir. Bu durumdan insan oğlunun bilgi toplumuna geçişinin daha hızlı olacağı ve sanayi toplumunun getirdiği değişikliklerden daha köklü ve daha derin bir değişim ve dönüşümle karşılaşacağı sonucuna ulaşılabilir.

Sanayi toplumundan bilgi toplumuna geçiş döneminin analizini yapılması ve kendisinin bu sürecin neresinde olduğunun tespiti, kurulmakta olan yeni dünyada etkin ve saygın bir konuma sahip olmak isteyen toplumların temel yaklaşımı olmalıdır. Teknolojik değişimin hızı ve jenerik teknolojilere etkisi değerlendirildiğinde önümüzdeki dönem içerisinde günlük yaşantıyı etkileyen pek çok olayın, teknolojiyle bağlantılı olarak, farklı boyutlarda algılanmaya başlanacağı ve bilgi toplumunun en temel özelliklerinin dijital devlet/toplum şeklinde karşımıza çıkacağı tahmin edilmektedir. Bir fikir oluşturması bakımından günlük yaşamımızı büyük ölçüde etkileyecek teknolojik gelişmelerin hangi alanlarda nasıl kullanılacağına yönelik bir yenilik listesi aşağıda sunulmuştur (Enformatik Çalışma Grubu Raporu, 1995, s. 2-7):

1.1.1. Eğitim ve Araştırma

- Uluslararası Elektronik Üniversiteler: Üniversite ve yüksek okulların, bilgi teknolojilerinin bütün disiplinlerdeki eğitim, araştırma ve geliştirmede en yetkin biçimde nasıl kullanılabileceğinin ortaya konduğu odaklara dönüşmesi, yalnızca ulusal bilgi ağları ile sınırlı kalmayıp küreselleşmek ve Küresel Enformasyon Altyapısı üzerinden uluslararası dersliklerin oluşması.

- Etkileşimli Uzaktan Eğitim: Orta ve yüksek eğitim kurumlarında etkileşimli uzaktan eğitim vermesi aracılığıyla, giderlerin önemli ölçüde azalması; verilen hizmetin, kaliteden ödün vermeksizin, küçük yerleşim alanlarına dek yaygınlaştırılması.

- Kütüphanelere Erişim: Bu altyapıyı kullanarak yerel ya da herhangi bir uzak kütüphaneye erişim, istenen bilginin taranması ve elde edilmesinde hız ve ucuzluk sağlanması.

1.1.2. Üretim ve Ticaret

- Bilgisayar Destekli Tasarım ve Üretim: Sanayi toplumunun bir niteliği olan büyük ölçeklerde kitlesel üretim yerini geniş bir çeşitlilik yelpazesi içinde esnek üretime bırakmaktadır. Esnek üretimin; ürünün tarif edilmesi, ürünün modellenmesi, üretim mühendisliği, üretim kontrol ve lojistik destek aşamalarında enformasyon teknolojilerinin kullanılması, üretimdeki yaygın standartlar.

- Video-konferans: Gerekli an, kişilerin bulundukları yerden bağımsız olarak ve ulaşım gideri ödemeksizin iş toplantıları gerçekleştirilmesi.

- Elektronik Ticaret: Gerek pazar bilgileri, gerekse bu pazara sunulacak ürüne ilişkin tüm para transferleri elektronik olarak anında yapılabilmesi. Örneğin; pazarlamadan gelen bir bilginin, anında ne tür bir ürünün üretilmesi gerektiğini söyleyerek, bu üretim için neyin nereden ve kaçta alınacağı bilgilerinin elde bulundurulması, gerekli satıcıların stok durumunun anında bilinmesi, sipariş verilirken ilgili firmaların çalıştıkları bankalar arası para transferlerinin anında yapılması.

- Satış Sonrası Uzaktan Etkileşimli Eğitim: Profesyonel ürün satan firmaların sattıkları ürüne ilişkin eğitimi, müşterilere enformasyon teknolojilerini kullanarak vermesi.

- Süper Bilgisayar Ağları ile Bağlantı: Süper bilgisayarlar gibi büyük yatırımların küçük işletmeler tarafından ortak satın alınması, kullanılması.

1.1.3. Kamu Hizmetleri

- Elektronik Belgeler: Bireylerin devletten almak zorunda olduğu ve devletin tuttuğu diğer kayıtlarda (nüfus kağıdı, pasaport, tapu ve kadastro, nüfus, adli kayıt ve sicil, askerlik, ithalat/ihracat v.b.) enformasyon teknolojilerinin kullanılması.

- Ödemeler: Vergi, harç v.b. ödemelerin enformasyon altyapısı üzerinden yapılması.

- Veri Aktarımı: Devlet içi yazışmaların, belge ve veri aktarımların, enformasyon altyapısı üzerinden sağlanması.

- Video-konferans: Kamu görevlilerinin toplantılarının zaman ve mekandan bağımsız enformasyon altyapısı üzerinden yapılması.

- Elektronik Oylama: Elektronik oylama ya da referandum ile bireylerin yönetime katılımının etkinleştirilerek daha çoğulcu bir demokratik düzene geçilmesi.

1.1.4. Sağlık Hizmetleri

- Uzaktan Tarama: Röntgen, ultrason, tomografi gibi sağlık taramalarının her hangi bir yerde yapılıp, uzaktaki bir uzman hekimin incelemesine enformasyon altyapısı üzerinden sunulması.
- Video-konsültasyon: Uzmanların her hangi bir yerdeki hastaya, bulunduğu yerden bağımsız olarak uzmanların enformasyon altyapısı aracılığıyla uzaktan konsültasyon yapması.
- Sağlıkla İlgili Veri Bankaları: Bireylerin sağlıkları ile ilgili tüm verilerin düzenli bir biçimde veri bankalarında saklanması.
- Koruyucu Sağlık Hizmetlerinin Uzaktan Sunulması: Bireylerin koruyucu sağlık hizmetlerini, evlerinde enformasyon altyapısı üzerinden, akıllı terminaller aracılığıyla yapabilmesi.

1.1.5. Yaşama ve Yargıya Yönelik Hizmetler

- Hukuk Düzeninin Çelişkilerden Arındırılması: Enformasyon teknolojilerinin Kullanımıyla, hukuk düzeninin yeniden gözden geçirilmesi, çelişkili uygulamaların ortadan kaldırılması.
- Bireyin Parlamenteoya Katılımı: Bireylerin parlamentodaki çalışmaları yakından izleyebilmesi, çıkartılmakta olan yasalar hakkında daha geniş bilgi sahibi olabilmesi.
- Bireyin Yasal Uygulamaya Etkin Katılımı: Bireyin kendisi ile ilgili yasal verilere erişebilmesi, durumunu (örneğin her hangi bir yasaya olan karşı davranışı gibi) tüm açıklığı ile görebilmesi, bir suç oluşmadan gereken önlemleri ve düzeltmeleri uygulamasına yönelik hizmetler.

1.1.6. Evlere Hizmet

- Evde Çalışma (Tele-İş): Bireylerin işe gidip gelmek için harcadıkları zamanı azaltacak, çalışma ortamının ev olmasını sağlayacak uygulamalar.
- Güvenlik Hizmetleri ve Sayaçların Uzaktan Okunması (Telemetre): Elektrik, su, gaz gibi hizmetlerde, idareler bireyin konutuna gelmeden sayaçların okuması ve bu şebekelerdeki güvenliğin, hizmetin sürekliliğinin enformasyon teknolojileri aracılığıyla denetlenmesi.



- Evden Alışveriş ve Banka Hizmetleri: Etkileşimli çoklu-ortam ve sanal gerçeklik uygulamaları yardımıyla insanların alacakları giysileri üzerlerinde nasıl duracağına bakması, ev eşyalarının yerlerini değiştirmesi, alışveriş sonucunda ücreti elektronik olarak ödemesi.

- Bilgi Alma Hizmetleri: Bireylerin yasa, yönetmelik konularında güncel bilgilere ulaşabilmesi, coğrafi bilgi sistemlerine erişim kolaylıkları, sanat, spor, ulaşım alanlarında rezervasyon v.b. gibi hizmetlere ulaşabilme.

- Video Postası ve Video Telefon: Görüntülü posta ve telefon hizmetlerinin enformasyon altyapısı aracılığıyla sunulması.

- İsmarlama Video (video on demand): Bireyin evinde ayrı bir video göstericisi ve video kaset koleksiyonu olmadan, evindeki uç biriminden merkezi bir bilgi bankasına erişerek dilediği video filmini izleyebilmesi, gerektiğinde durdurup geri sardırabilmesi.

- Etkileşimli Çoklu Ortam ve Video Oyunları: Bireyin eğlenme isteklerine yeni ve yaratıcı çözümler sunabilecek etkileşimli, yaratıcılık yeteneği kazandıran oyunların enformasyon altyapısı aracılığıyla sunulması.

1.1.7. Topluma Yönelik Diğer İletişim ve Bilgi Hizmetleri

- Elektronik Gazete ve Kaynak Bilgiler: Elektronik gazete ve kaynak bilgilerin derli bir biçimde sunulması, aranan bilgiye erişimin kolaylaşması.

- Toplumu İlgilendiren Bilgi Hizmetleri: Toplumu ilgilendiren bilgilerin zamanında ve periyodik olarak bireylere ulaşması.

- Elektronik Duyuru Hizmetleri: Enformasyon Altyapısının ivedi duyuruların topluma anında iletilmesini için kullanılması.

- Hizmetleri Tanıtan Rehberler ve Sınıflandırılmış Reklamlar: Bilgileri ve hizmetleri tanıtan, sınıflandıran sistemlerin kullanılması.

- Elektronik Müzeler ve Kütüphaneler: Bireyin yaşadığı çevre ve kültür birikimi ile yakınlaşmasını sağlamasına yönelik Elektronik Müzeler ve Kütüphaneler gibi uygulamalar.

1.1.8. Akıllı Evler

- Telefonlar; her oda yerine sadece insanların bulunduğu yerde çalacaktır; ısı sensörleri ve kameralar aynı şekilde sadece insanların bulunduğu mahallerde elektrikleri yakacaklardır.

- Bilgisayar komutları ile odalar otomatik olarak havalandırılacaktır, perdeler kapatılacaktır.

- Ev robotları yaygınlaşacak; odalardaki çiçekleri sulayacak, kirli çamaşırları çamaşır makinelerine atacaktır, ancak anında suyun kimyasal bileşiminin analizi yapılacağından çamaşırın kirliliği biter bitmez makine durdurularak su, kimyasal madde ve elektrik tasarrufu sağlanacaktır.

- Ev robotları mutfak işleri ve bahçe işlerini yapacaklardır.

- Ev dışında bir tehlike belirlendiğinde; tehlike, anında görüntülü olarak bildirilecekti; kepenkler otomatik olarak kapanacak, eve hırsız girdiğinde polis ikaz edilecektir.

- Ev televizyon ekranlarının büyümelerine karşılık, kalınlıkları azalacaktır ve duvarlara asılacaklardır.

- Mutfaklardaki buzdolapları; işyerlerindeki kişilere eksik gıdaları bildirecektir; ayrıca gıda paketi üzerindeki barkod bilgileri sayesinde, o gıdanın kalorileri verilerek diyet uygulamalarına yeni bir boyut kazandırılacaktır; buzdolabı kapağından İnternete girilecek, yemek tariflerine kolayca ulaşılabilecektir (Ayhan, 2002, s. 374,375).

Günümüzde, bilgi teknolojilerinin öneminin büyük bir hızla artmasının elle tutulur gözle görülür sebepleri vardır. Bu sebepler bazı ileri ülkeler için çok açık bir şekilde bilinmekte, bu yüzden bu ülkeler bilgi teknolojilerinde daha fazla araştırma, geliştirme ve üretim yaparak daha büyük ekonomik güce sahip olmaya, bireylerinin ve kurumlarının geleceğini emniyet altına almaya çalışmaktadır. Gelecekte bilgi teknolojilerinin tüm ekonomik faaliyet alanlarının altyapısını oluşturması ve ekonomik gücün büyüklüğünü tayin edici nitelikte olması beklenmektedir.

Bilginin kişi, kurum ve toplum yararına, araştırılması, geliştirilmesi, üretilmesi ve etkin bir şekilde kullanılması faaliyetlerinin tümünü bilgi teknolojileri olarak tanımlanmaktadır. Bu tanımda bilgi ve bilgi teknolojilerinden ne anlaşıldığını tekrar etmekte yarar var.

Bilgi, ya da enformasyon, İngilizce ya da Fransızca "information" kelimesinin karşılığı olarak, metin, konuşma, resim, kaliteli ses, hareketli görüntü ve benzeri biçimlerde bulunmakta ve insanlar için bir anlam içermektedir. Bilgi teknolojileri, bilgi iletişimi, işlenmesi ve saklanması teknolojilerini kapsamakta ve altyapılarını bugünün elektronik, optik, haberleşme, bilgisayar vb teknolojileri oluşturmaktadır. Bilişim ve bilgi teknolojileri ile ilgili olarak bilgi devrimi, bilgi çağı, bilgi toplumu, bilişim toplumu vb terimler de bulunmaktadır. Sanayi devrimi ve sanayi toplumu terimlerinden esinlenerek kullanılmakta olan bu terimler ile ileri toplumların yakın gelecekteki farklı bir sosyo-ekonomik ve politik düzene ve teknolojik altyapıya geçiş sürecini adlandırılmaktadır. Bilgi devrimi süreci Kuzey Amerika, Pasifik ve Avrupa'daki ileri ülkelerde 80'li yıllarda başladı. Bilgi devrimi sanayi devriminden çok daha hızlı bir şekilde ilerlemekte ve dünyayı şimdiden değiştirmeye başlamış bulunmaktadır.

Bilgi teknolojilerinin amaç mı araç mı olduğu, bileşenlerinin ya da farklı boyutlarının neler olduğuna değinmekte fayda vardır. Yeni teknolojilerin bir kaç boyutundan en önemlisi, varolan, devamlı değişen ve geleceği beklenen fakat geldiğinde ne şekil alacağı tam olarak da bilinemeyen bilgi teknolojileridir. Bunların arasında bilgisayar donanımı (işlemciler, bellek v.b.), yazılım, iletişim ve ağ teknolojileri (yerel ağlar, ethernet, modemler, fiber optik, telsiz iletişim, v.b.), uygulama mimarileri ve prosedürlerini (açık sistemler, kullanıcı arayüzleri, v.b.) saymak olasıdır. Teknoloji alanında her gün yeni sürprizlerle karşılaşmaktadır. Hergün teknolojik bir ürünün yeni sürümünün ne kadar daha işlevsel, ne kadar daha hızlı, ne kadar daha küçük, ne kadar daha yüksek başarımlı, ne kadar daha güvenilir ve ne kadar daha ucuz olarak sunulduğu duyurulmaktadır.

Diğer bir boyut, araştırma geliştirme (AR-GE), üretim ve pazarlama, satış üçlüsü içinde bilgi teknolojilerini arz eden kurumların bakış açısıdır. Buna bilgi teknolojisinin arz boyutu denilebilir. Arz kurumlarının bir bölümü serbest piyasanın rekabet kuralları çerçevesinde daha çok kar etmek amacıyla, yukarıda sıralanan daha işlevsel, daha hızlı, daha küçük, daha yüksek başarımlı, daha güvenilir ve daha ucuzu araştırıyorlar, geliştiriyorlar, üretiyorlar ve kullanıcılara sunuyorlar. Üretim süreci, toplumsal ve kültürel konumuna bağlı olarak çeşitli kurum ve sınıflar farklı davranış karakteristikleri göstermektedir. Arz boyutunda, kar amacı gütmeyen bu boyutta rol



alan üniversiteler, araştırma kurumları, vakıflar, şirketlerin bir araya gelmesinden oluşan organizasyonlar, dernekler de bulunmaktadır.

Arz boyutunu tamamlayan bir de talep boyutu var. Talep boyutu bilgi teknolojilerinin yararları ve günlük hayatta kullanımı olarak da tanımlanabilir. Günlük hayat derken, kişi ve kurumların eğitim, sağlık, v.b. kamu hizmetlerinden etkin bir şekilde yararlanmasında, demokrasinin uygulanmasında ya da başka bir deyişle kişi ve kurumların kendi geleceklerini kararlaştırmada söz sahibi olmasında, kısaca insanların daha az acı çekerek daha uzun ve mutlu yaşamaları için bilgi teknolojilerinin kullanılması olarak anlaşılmaktadır. Talep boyutunda da çok farklı oyuncular vardır. Bunların bir tanesi çok önemlidir: Devlet.

Devlet tüm diğer konularda olduğu gibi bilgi teknolojilerinde de en büyük alıcı ve kullanıcı, aynı zamanda kanunlar, yönetmelikler, politikalar aracılığı ile kimin neyi araştıracağı, üreteceği ve kullanacağı konularında söz sahibidir. Talep boyutunda talep ağırlıklı özel sektör (turizm, imalat, servis v.b.) diğer kamu kuruluşları, üniversiteler, sivil toplum örgütleri ve sokaktaki adamın bilgi teknolojilerine farklı bakış açıları vardır. Kısaca açmak gerekirse, kamu kuruluşları sokaktaki adama daha etkin hizmetler sunmak, üniversiteler daha çok insana daha kaliteli eğitim sağlamak ve araştırma yapmak, sokaktaki adam da daha önce belirttiğimiz gibi daha az emek vererek, daha uzun ve mutlu yaşamak için bilgi teknolojilerini kullanmak istemektedir.

Acaba bilgi toplumu olmanın, göstergeleri nelerdir? Örneğin, "Acaba Almanya bir sanayi toplumu mudur?" sorusuna herhalde hemen hemen herkes evet cevabı verir, burada da Almanya'nın adam başına ürettiği demir çelik, elektrik, otomobil, TV, buzdolabı v.b. gibi sanayi ürünlerini dikkate alınır.

Bilgi toplumu olmanın, göstergeleri olarak;. bir toplumdaki adam başına telefon, faks, cep telefonu, radyo, televizyon, modem, ISDN ucu, bilgisayar, İnternet bağlantısı sayıları ile kullanılmakta olan yazılım paketleri, varolan bilgisayarların bir ağ içinde yer alıp almadığı, kablo televizyon ve varolan televizyon kanallarının sayısı v.b. oldukça iyi göstergelerdir. Ek olarak bilgi teknolojileri alanlarında çalışanların toplam çalışanlara oranı, bunların ürettikleri ürün ve servislerin toplam üretim içindeki payı, üniversite ya da yüksek okul mezunlarının toplam yetişkinlere oranı



gibi göstergeler de kullanılabilir. Diğer taraftan adam başına üretilen/tüketilen kitap, dergi ve gazete sayıları, örgütlenme, basın özgürlüğü, demokrasi gibi konulardaki ölçütler de iyi göstergeler olarak sayılabilir.

1.2. E-Devlet

İnsanoğlunun kas gücüyle yaptığı işleri makinelere bıraktığı Endüstri çağında sırasıyla mekanik, hidrolik, optik, kimyasal, nükleer ve elektronik sistemler geliştirilmiştir. Bu aşamada üniteler ve tezgahlar yerine sistemler ortaya çıktı. Daha sonra elektrooptik, hidromekanik, mekatronik gibi birleşik sistemlere yönelindi. Elektroniğin hakim olduğu teçhizat hem belirli karmaşık fonksiyonları yerine getirirken hem de kontrol görevini üstlendi. Sistemler ise ana görevi yerine getirdiler. Bigi toplumuna geçişin ilk adımı bilgisayarlarla atıldı. İnsanlar bulundukları yerden, iletişim kanalları vasıtasıyla, istedikleri bilgilere erişme imkanına kavuştular. Bu ilerleme toplumların da yapısını değiştirmeye başladı. Yirminci yüzyılın son çeyreğinde toplumlar iletişim imkanlarının sınırsızlığına paralel olarak sosyal, kültürel ve ekonomik etkilere maruz kaldılar. Teknolojik yeterlilik ve bilgiyi ticari olarak kullanma yeteneği ekonomik gelişimin temelini oluşturdu. Bilgi ve iletişim teknolojileri dünya pazarlarına egemen olmaya başladı. Günümüzde rakamsal olarak 2 trilyon Amerika Birleşik Devletleri (ABD) doları tutarında bir pazarın varlığı söz konusudur. Bilgi ve iletişim teknolojileri doğurgan yani geliştirilebilen teknolojilerdir. Bilgisayar donanım ve telekom hizmetleri bugünkü pazar ihtiyaçlarının ancak yüzde 60'ını karşılayabilmektedir. Bu pazarda pay elde etmek için ülkeler arasında da büyük bir ticari rekabet yaşanmaktadır (Orün, 2000, s. 84).

Bilgi teknolojisinde asıl olan bilgilerin yüklenmesi ve depolanarak sınıflandırılmasıdır. Daha sonra isteğe uygun olarak bu bilgiler geri çağrılabilir. Basit anlamda; bilgilerin toplanması ve iletişim imkanlarıyla istenen yerlere ulaştırılmasını sağlayan model yapı (infrastructure) olarak isimlendirilir. Bilgi çağına ulaşmak isteyen her toplumun bu anlamda bilgi yapılanmalarına ihtiyacı vardır. Stratejik seviyede bu yapıların oluşturulması ise devletlerin görevi olarak algılanmaktadır.

Devletin bilgi teknolojileri ile ilgili faaliyetlerine geçmişten başlayarak bakmakta yarar vardır. Bilgisayar sistemlerinin nasıl alınacağını tam olarak bilinmediği devirlerde, devlet hangi bilgisayar sistemlerinin satın alınıp tesis edilebileceğini

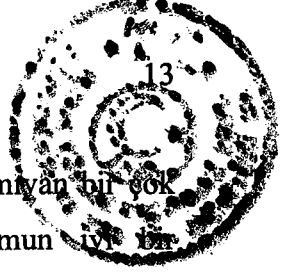


Ortadoğu Teknik Üniversitesi (ODTÜ)'ne sorardı. Daha sonra, kimin neyi aldığı ve kurduğu, serbestleşen ithalat rejimi ile birlikte kurumlara bırakıldı. 80'li yıllarda eğitimde bir milyon bilgisayar projesi ortaya atıldı. Çeşitli boyutları yeterince düşünülmeyen bu proje; bazı okullarımıza kapalı laboratuvarlarda, beyaz örtüler altında saklanan müzelik bilgisayarları miras bıraktı. Yazılım, kitap, insangücü eğitimi anlamında bir birikim sağlanamadı. Ne devlet ne de Türk bilişim sektörü benzeri hataları tekrarlamamak için gerekli değerlendirmeyi bugüne kadar yapmadı.

Türk toplumunun bilgi teknolojileri açısından modernleşmesinde Dünya Bankası projeleri önemli bir rol almış durumdadır. Hemen hemen tüm büyük bilişim projelerinin Dünya Bankası destekli oluşu göze çarpmaktadır. Türk bilişim sektörünün, hemen hemen sorgusuz sualsiz bu projeleri sahiplenmesi, projelerin sadece Dünya Bankası'ndan kaynaklanması ve sonuçlarının hiç irdelenmemesi ilginç ve acı bir gerçek olarak yüzümüze çarpmaktadır.

Toplumuzda büyük ölçüde eksik olan araştırma ve geliştirme faaliyetleri, son yıllarda Türk Teknoloji Geliştirme Vakfı (TTGV) ve Türkiye Bilimsel ve Teknik Araştırma Kurumu (TÜBİTAK) tarafından bilişim sektörünü de kapsayacak şekilde desteklenmektedir. Bu destek çok olumlu olmakla birlikte henüz bilgi teknolojilerinin gelişiminde ciddi değişiklikler yapacak parasal boyutlarda değildir. Devletin ekonomik krizler ile ilgili olarak ara sıra duyurduğu tasarruf tedbirleri içinde bilgi teknolojileri ürünlerinin satın alınmasının belki de lüks ya da gereksiz alımlar sayılarak durdurulması, devletin kendi kurumlarında bilgi teknolojilerine önem vermediğini göstermekte, aynı zamanda bilgi teknolojilerinin henüz kamuda verimliliği artırıcı bir şekilde kullanılamadığını da yansıtmaktadır.

İnternet'in 1993 yılının Nisan ayında Türkiye'ye gelişinden bu güne kadar olan gelişmeler Türkiye bilişim sektörünün içinde bulunduğu kaos, kafa karışıklığı ve yaşadığı problemler çok iyi örneklerdir. Devletin Türk Telekom'dan, Öğrenci Seçme ve Yerleştirme Merkezi (ÖSYM), Yüksek Öğrenim Kurumu (YÖK)'na, DPT'na kadar İnternet'in önemini kavramada, kullanmada ve önünü açmada gösterdiği direnç; özel sektör, kamu ve bilişim örgütlerinin İnterneti kullanmada gösterdiği yavaşlık, kendi aralarında diyalog eksikliği, örgütlenmede geç kalışımız aslında tipik sorunlarımızın da yansımasıdır. Sektör olarak bir masa etrafında oturup konuşup, çözüm üretme ve bunu hayata geçirmede başarılı olunamamıştır. İnternetin

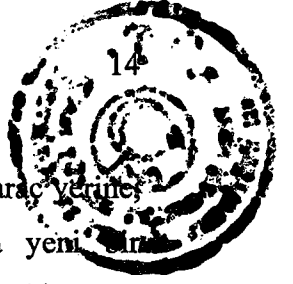


Türkiye'ye geç gelişinden sonra bile İnternete kurumsal bağlantısı olmayan bir çok üniversite, holding ve kamu kuruluşunun olması mevcut durumun iyi bir göstergesidir. Bilgi teknolojileri sektörünün Türk ekonomisi içinde önemli bir yerinin olmadığı da önemli bir gerçektir. Kamuda genel bir sahipsizlik, koordinasyon eksikliği, plansızlık, hesap verme ve denetim eksikliği kendini göstermektedir. Büyük çaplı projeler göze çarpıcı bir şekilde duyurulmakta, ama projenin başarısını sağlamak için denetleme mekanizmaları kurulmamakta ve projenin süresi bittiğinde kamuyu bilgilendirici değerlendirmeler yapılmamaktadır. Bu projelerin bitmediği ya da istenen amaçlara ulaşmadığı zamanlar sorunlar üzerinde durulup, sorunların çözülememesinden ders alınıp, ortaya çıkan engeller konusunda bir açıklama bile yapılmamaktadır. Yılan hikayesine dönen Mernis projesi, çeşitli Dünya Bankası projeleri bu durumdadır.

Kamu sektöründe adacıklar halinde bilişim teknolojilerinin etkin kullanımı konusunda bazı çabalar da sözkonusudur. Ama değişik birimler arasında üretime yönelik ciddi atılımlar henüz başlayabilmiş değildir.

Bilgi teknolojileri sektörünün Türkiye'deki önemli gücü uluslararası bilgisayar firmaları, onların Türkiye'deki temsilcileri ve çözüm ortaklarıdır. Bu firmalar, genelde, Türkiye'de araştırma yapmamakta, ürün geliştirmemekte, sadece pazarlama, satış ve satışın bir parçası olan destek faaliyetlerinde bulunmaktadırlar. Geliştirme olarak en fazla yaptıkları; yabancı kaynaklı ürünlerin Türkçeleştirilmesidir. Ayrıca tüm dünya ile birlikte, ürünlerin Türkçe sürümünü de duyurabiliyorlarsa, bunu da büyük başarı olarak sunmaktadırlar. Bu firmaların Türkiye için sorumlulukları, yukarıda sıralanan faaliyetlerle sınırlı gözükmektedir. İnternet boyutunda da durum aynıdır. Sözkonusu firmaların, TR alanı altında İnternet alan adı kaydı, web sunucuları kurma, Türkçe içerikli web sayfaları üretme, Türkiye İnternetinin parçası olma gibi bir endişelerinin olmadığı bilinmektedir.

Bilgisayar donanım ve yazılımı ithalat, satış, servis ve bakım olarak bilgi teknolojileri pazarının toplam parasal değerinin Gayri Safi Milli Hasıla (GSMH) içinde çok yüksek miktarlara ulaşmadığı da bir gerçektir. İleri ülkelerin harcamaları ile karşılaştırıldığında ve kişi başına harcamalar dikkate alındığında bu rakamların çok düşük kaldığı görülmektedir.



Türkiye özel sektöründe bilgi teknolojileri, üretim için kullanılan bir araçtır. Bir kurumda yeni bir teknolojinin; belirli bir plan kapsamında, eğitim ve uyarlamalarla birlikte, bir süreç içinde hayata geçirilmesi gerekirken, ülkemizde yeni teknoloji projelerinin plansız ve programsız, statü ve gösteriş ağırlıklı yapıldığına ilişkin pek çok örnek göze çarpmaktadır. Öğrenmenin ve iyileştirmenin bir süreklilik arzettiği ve bunun bir felsefe olarak sürekli eğitim, toplam kalite kavramları, bir kaç kısıtlı örnek dışında, ülkemiz pratiğinin epey yabancı olduğu konulardır.

Üretim meselesine değinmişken, bilgi teknolojilerinin en önemli ve ana konularından biri olan yazılım üretiminin ancak son dönemde devlet tarafından bir sanayi kolu olarak tanındığını belirtmekte de yarar vardır.

Üniversiteler de geniş bir yelpazede farklılıklar ortaya çıkmaktadır. Boğaziçi, ODTÜ ve Bilkent dahil olmak üzere henüz hiç bir üniversitemizde, o üniversitenin tüm faaliyetlerini kapsayan bir yönetim bilişim sistemi maalesef hala bulunmamaktadır. Genellikle üniversitelerin farklı birimleri kendi gereksinimleri için özel uygulamalar geliştirmişlerdir. Personel, muhasebe, öğrenci işleri ve kütüphane uygulamalarının birbirinden bağımsız ortamlarda, bir ağ bütünlüğünden uzak bir yapıda oluşu olağan bir uygulama olarak görülmektedir. Gelişmiş üniversitelerden başlayarak, kütüphane ve öğrenci işlerinin etkileşimli ortamlara ve giderek web ortamına doğru kaydırma eğilimi vardır. Bazı üniversitelerde bilgi işlem birimlerinin varlığı bile tartışılacak bir durumdadır. Öğrenci ve öğretim üyelerine İnternet ve temel bilgisayar hizmetlerini verebilecek bir altyapı planının olmadığı kurumlar çoğunluktadır 70'li ve 80'li yıllarda önemli dünya üniversiteleri İnternet'e bağlanırken, en atılgıncı kurumlar olması gereken üniversitelerimiz İnternet'in farkına ancak 1993 yılında vardılar. Bu arada İnternet'in Türkiye'ye gelmesinden sonra konunun öneminin kavranmasının ve ULAKNET projesinin biraz da plansız, programsız başlatıldığını da belirtmek gereklidir. Hala üniversitelerin bilgi teknolojilerini eğitim ve araştırmanın her alanında yaygın olarak kullanabilmesi için belirlenen hedeflerin ya da bir stratejik planının olmadığını da söylenebilir.

Bilgi teknolojilerine sahip çıkacak, ilgili birimler arasında koordinasyonu sağlayacak örgütler yetersizdir. Kamu ve özel sektörde kurum boyutunda

koordinasyon eksikliğini vardır. Sivil toplum örgütleri sayı ve etkinlik açısından yetersizdir, katılımcı mekanizmalar hemen hemen yok denilebilir.

Türkiye tüm çabalara rağmen bilgi teknolojisi kullanımında neden bu düzeydedir ve niçin hala istenen düzeye çıkartılamamakta? Bu soruların cevabı tam olarak verilebilirse, sorunun çözümünde önemli bir yol almış olunur.

Çok genel bir tespit ile, çalışan, devamlı gelişen, katılımcı süreçler yerine hep tepeden gelen, ben yaptım oldu mantığı ile, hızlı bir şekilde karar verilen ama çoğunlukla hayata geçirilmesi çok geciken süreçlerin görülmesidir. Öğrenen sistemler yerine değişimi zor esnekliği az sistemler kurulmaktadır.

Sorunun kökünde ülkenin koşullarından kaynaklanan nesnel nedenlerle, kültürden, çalışma alışkanlıklarından, örgütlenme ve bilinç düzeyinden kaynaklanan öznel nedenler yatmaktadır. Nesnel engelleri aşmanın yolu, öznel sorunları çözüp, toplumsal gücü harekete geçirerek, oluşacak sinerjiden yararlanmaktır. Öznel sorunları çözmek, yöntem sorunun da çözülmesini sağlayacaktır. Yanlış yöntemlerle sorunların çözülemeyeceği açıktır.

Bilgi teknolojilerini etkin, yaygın ve üretim için, toplumsal yaşamın çeşitli boyutlarında kullanmak Türkiye için hayati bir konudur. Bilgi teknolojisi, çağdaş, gelişmiş bir ülke olmak için olmazsa olmaz koşulların başında gelmektedir.

Bunu başarabilmek için stratejik ve taktik düzeylerde, ulusal uzlaşma içinde partiler üstü politikaların belirlenip, bunları ısrarla gündemde tutmak, gerekli kaynakları ayırarak ve ortak çabalarla hayata geçirmek zorunluluğu vardır.

Türkiye'de özellikle eksikliği hissedilen katılımcı mekanizmalardır. Karar alma ve bunları hayata geçirmede toplumdaki bilgi ve deneyim etkin bir şekilde işbirliği içinde kullanılabilmelidir.

Bilgi teknolojileri ancak öğrenen, katılımcı mekanizmalarla hızlı bir şekilde hayata geçirilebilir. Önemli olan doğru ilkeler ve mekanizmalarla, esnek önlü açık sistemleri hep beraber hayata geçirebilmektir.

Bilgi teknolojileri ve onun öncüsü, taşıyıcısı olan İnternet, Türk toplumuna özlediği sıçrama için katalizör görevi yapabilecektir. Bu potansiyeli harekete

geçirmekte doğru mekanizmaları kurmak, devlete ve bilgi teknolojileri sektöründeki kurumlara düşmektedir.

Türkiye’de bilgi yapılanlamasının oluşturulmasına yönelik ilk stratejik adım Temmuz 1997’de Ulaştırma Bakanlığına tarafından Türkiye Ulusal Enformasyon Altyapısı (TUENA) Anaplanı yayınlanarak atılmıştır (Orün, 2000, s. 84).

Milli enformasyon altyapısının yaşamsal önemi Bilim ve Teknolojide Atılım Projesi kapsamında 1995 yılında vurgulanmıştır. Türkiye Bilimler Akademisi (TÜBA), TÜBİTAK, TTGV tarafından oluşturulan ve ilgililerin katılımına açık olan “Bilim Teknoloji Sanayi Politikaları Platformu” çalışmaları çerçevesinde kurulan “Enformatik Çalışma Grubu” raporunda da, Türkiye’nin karşı karşıya bulunduğu tehditlere dikkat çekilerek ana plan çalışmasının yapılması istenmiştir. Konu ile ilgili 2000’e yakın kişi ve kuruluşa gönderilen raporda, enformatik sektörünün kazandığı stratejik önem vurgulanarak enformasyon altyapısının oluşturulmasına bir ana plan çerçevesinde yaklaşılması gereği tekrarlanmıştır. Bu öneri ve rapor, TÜBİTAK tarafından kilit konumdaki bütün kişi ve kurumlara gönderilmiştir. Bu aşamadan sonra Milli Güvenlik Kurulu Genel Sekreterliği, konunun önemi nedeniyle, 23 Ocak 1996’da çeşitli kamu kuruluşlarını toplantıya çağırmıştır. Bu toplantıda Master Planın milli yararın en çoğa çıkartılması ve hedeflenen yetenek düzlemlerine erişilebilmesi için kaçınılmaz olduğu belirtilmiş ve şu görüşler saptanmıştır (TUENA Sonuç Raporu, 1999, s. 3):

- Yeni teknolojik olanakların getireceği yasal sorunlardan kurtulmanın yolunun elbette bu teknolojilerin ülkeye girmesi ve yaygınlaşmasını engellemek olmadığı,
- Dünya nimetlerinden alınacak payın belirlenmesinde en büyük rolü oynayan teknolojinin, benzer rolü yasaların ve uluslararası hukukun biçimlenmesinde de oynadığının, göz ardı edilmemesi gerektiği,
- Enformasyon teknolojisi üzerinde etkinliğini artıranların, geleceğin enformasyon toplumunun ekonomisine olduğu kadar hukukunda da hakim olacakları,
- Bu nedenle yapılacak düzenlemelerin zaten kullanılması kaçınılmaz olan bu teknolojilerin önünü açması ve bunu yaparken de milli çıkarları gözetmesi gerekliliği,
- İnternetin milli enformasyon altyapısının başlangıcı olarak değerlendirilmesi;

bu bağlamda milli enformasyon altyapısı ve bunun üzerinde geliştirilecek telematik hizmetlere ilişkin ek altyapıların inşası konusunun bir master plan çerçevesinde ele alınması gerekliliği.

Toplantı sonrasında, Başbakanlık, 5 Şubat 1996'daki bir yazısıyla Enformasyon teknolojilerinin geliştirilmesi ve bilgi toplumuna geçişin sağlanması maksadıyla enformasyon alanında kamu güvenliği ve menfaatleri, sosyo-ekonomik, yasal, kurumsal ve düşünülebilecek diğer hususları da kapsayan bir enformasyon (İnternet dahil) politikasının geliştirilmesine duyulan ihtiyaç nedeniyle Ulaştırma Bakanlığı sorumluluk ve koordinatörlüğünde, sekreteryaya hizmetlerini TÜBİTAK Başkanlığı'nın yürüteceği Türkiye'de Enformasyon Politikası ve Enformasyon Altyapısı Master Planının oluşturulmasını istemiştir. Başbakanlığın direktifleri gereğince Ulaştırma Bakanlığı koordinatörlüğü ve TÜBİTAK Başkanlığı'nın sekreteryasında 1996'da başlayan çalışmalarda dört kez toplanılmıştır. Bu toplantılar sonucunda şu ilkeler oluşmuştur (TUENA Sonuç Raporu, 1999, s. 3):

- Enformasyon teknolojileri alanının bir bütün olarak değerlendirilmesi gerektiği, İnternetin Ulusal Enformasyon Altyapısının yalnızca bir başlangıç ögesi olduğu,
- Dünya üzerinde İnterneti milli enformasyon şebekelerine çevirme yolunda gelişmiş ve gelişmekte olan ülkelerin planlarını hazırlayıp eyleme geçtikleri,
- Türkiye'nin entegrasyonu hedeflediği Avrupa Birliği'nde yaşanan bu gelişmeler karşısında kayıtsız kalamayacağı,
- Bu nedenle, İnternetin Türkiye uzantısının milli enformasyon altyapısının ilk adımı olarak değerlendirilmesi,
- Milli güvenlik tanımının gerçekte milli menfaatlerin bir bütün olarak korunması geniş çerçevesinde ele alınması durumunda konunun kavranmasının kolaylaşacaktır.

Bu toplantılarda Milli Güvenlik Kurulu (MGK) Genel Sekreterliği, Genelkurmay Başkanlığı, Ulaştırma Bakanlığı, DPT, YÖK Başkanlığı, TÜBİTAK Başkanlığı ve özel sektör şemsiye kuruluşlarının temsilcilerinden oluşan bir çalışma grubunun oluşturulmasına ve bu grubun Enformasyon Altyapısı Anaplanı Yürütme Grubu adıyla anılmasına karar verilmiştir. TÜBİTAK tarafından hazırlanan Ulusal Enformasyon Altyapısı Anaplanı Hazırlama Önerisi, Yürütme Grubu'nun

değerlendirmesine sunulmuş ve özel sektörü temsilen Türk Elektronik Sanayicileri Derneği (TESİD) ve Türkiye Bilgi İşlem Hizmetleri Derneği'nin (TÜBİSAD) birer temsilciyle katılmalarının sağlanmasına karar verilmiştir.

Çalışmanın finansmanı ile ilgili sorunların giderilmesi konusunda yapılan çeşitli toplantılar sonucunda Türkiye Teknoloji Geliştirme Vakfı (TTGV), Türk Telekom ve Türk Elektronik Sanayicileri Derneği (TESİD)'in ve Ulaştırma Bakanlığı'nın kaynaklarının biraraya getirilmesi sağlanmıştır. 31 Mart 1997 tarihli toplantıda, Ulaştırma Bakanlığı, TÜBİTAK, TTGV, Türk Telekom ve TESİD arasında imzalanması için hazırlanan çerçeve protokol ve ikili sözleşmeler kabul görmüş ve gerekli yasal süreç başlatılmıştır. 30 Haziran 1997 tarihi itibarıyla Maliye Bakanlığı ve Sayıştay'ın olumlu görüşleri alınmış ve çalışma başlatılmıştır. TÜBİTAK çatısı altında oluşturulmaya başlanan proje ofisi Ulusal Enformasyon Altyapısı Anaplanı Yürütme Grubu'nun üzerinde anlaşmaya vardığı Teknik Şartname'de tanımlanan, sorulara yanıt aranmasıyla sürdürmüştür. Çalışmaların her aşaması Ulaştırma Bakanlığı başkanlığında oluşturulan, Genel Kurmay Başkanlığı, MGK Genel Sekreterliği, DPT Müsteşarlığı, YÖK Başkanlığı, TESİD, TÜBİSAD, TTGV ve Türk Telekom yetkililerinin katıldığı yürütme kurulunca izlenmiş ve denetlenmiştir. TÜBİTAK bünyesinde oluşturulan proje ekibi, yine TÜBİTAK bünyesinde oluşturulan ve bu alandaki özel ve kamu sektöründeki uzmanlardan oluşan teknik yönlendirme komitesi tarafından TÜBİTAK içi kalite denetimi yapılarak yönlendirilmiştir. Başbakanlık direktifi üzerine başlatılan çalışma, Ulaştırma Bakanlığı koordinatörlüğü ve TÜBİTAK Başkanlığı'nın sekreteryaya hizmetlerini yürüttüğü bir kapsamda sürdürülmüştür (TUENA Sonuç Raporu, 1999, s. 4).

Çalışmalarda; çeşitli ülkelerin kurumsal yapıları incelenmiş ve bu ülkelerin kendilerine hedef seçtikleri enformasyon ve iletişim teknolojileri, üretim alanları dahil incelenerek, geniş bir çalışma başlatılmıştır. Araştırma sonucunda ülkelerin büyük çoğunluğunun donanım imalatı yapmakta oldukları tespit edilmiştir. Türkiye'de, evlerdeki iletişim araçlarıyla ilgili olarak yapılan ankette;

- % 81.8 Telefon sahibi
- % 5.8 Telesekreter sahibi,
- % 6.5 Bigisayar sahibi,
- % 1.2 İnternet sahibi
- % 1.5 Faks sahibi olduğu belirlenmiştir.

Halkın telefon, su, elektrik, vergi borçlarını öğrenmek ve ödemek, yazdığı dilekçelere cevap almak, rezervasyon yaptırmak, iş başvurusu benzeri işlerle ilgili beklentilerinin yoğun olduğu da bu anket sonucunda ortaya çıkmıştır. Ancak halkın bu hususta bilgilendirmesi zorunlulu da vardır. Hane halkının iletişim araçları sahipliği düşüncesiyle yola çıkılmıştır. Yapılan planda 2010 yılına kadar nüfusu 20 000'den fazla olan yerleşim birimlerinin yüzde 75'inin bir iletişim ağı oluşturması hedeflenmiştir. Bu nüfusun altındaki yerleşim birimlerinde de hedef yüzde 25'tir. Türkiye için güvenlik teknolojileri ve ağ ve ağ üzerindeki uygulamalara ilişkin izleme ve yönetim teknolojileri kritik teknolojiler olarak benimsenmiştir.

Bilgi toplumunu genel yapılanması ise Bilim ve Teknoloji Yüksek Kurulu yöneticiliğinde, Bilgi Toplumu Fonu oluşturularak, yeni kurulacak bir Bilgi ve Teknoloji Bakanlığı ile sistemin organize edilmesi olarak ifade edilmektedir (Orün, 2000, s. 84).

Türkiye'de halihazırda e-devlete geçişin altyapısını oluşturacak milli bilgi yapılanması kapsamında, devlet kurumları ve kamu hizmeti sağlayan diğer kuruluşlar tarafından sistem projeleri yürütülmektedir.

2. SAVAŞ KAVRAMI:

Savaş, genel olarak bir milletin milli güç unsurlarının (ekonomik, psiko-sosyal, kültürel, bilimsel ve teknolojik, askeri güç) bir sorunun çözümünde topyekün kullanılması durumunu ifade etmektedir. Günümüzün savaş kavramı özellikle bilgi teknolojilerinde gelişime paralel olarak değişime uğramış, sadece askeri güçlerin kullanıldığı savaş alanı boyutundan çıkarak, terörist organizasyonlardan, uyuşturucu kaçakçılığına, psikolojik harekattan, sistematik ve bilinçli bilgisayar saldırılarına (hack) kadar geniş bir boyuta yayılmıştır. Böylece Savaş Harici Harekat (Operations Other Than War) kavramı ortaya çıkmıştır (Field Manual 100-5 Operations, 1993, s. 14). Bu çalışmada ele aldığımız savaş kavramı hem savaş hem de savaş harici harekat kavramlarının toplamının ifadesidir.

2.1. Geleceğin Savaşları

Özellikle yirminci yüzyılın son çeyreğinde ortaya çıkan gelişmeler, dünya üzerindeki mevcut iki kutuplu düzenin sona ermesiyle birlikte, geleneksel tehdit anlayışının da değişmesine sebebiyet vermiş ve sadece askeri güç çerçevesinde şekillenen tehdit anlayışı günümüzde yerini;

- Bölgesel krizler ve etnik çatışmalar
- Çeşitli radikal akımlar
- Ülkelerdeki siyasi ve ekonomik istikrarsızlıklar ve belirsizlikler
- Kitle imha silahları ve uzun menzilli füzelerin yayılması
- Köktendincilik
- Uyuşturucu ve her türlü silah kaçakçılığı
- Uluslararası terörizm gibi yeniden tanımlanan tehdit ve risklere bırakmıştır

(Şenoğlu, 1999, s. 22).

Tehdit anlayışındaki değişim; güvenlik anlayışının askeri güç kavramının ötesinde ekonomik, kültürel, siyasi ve teknolojik bir boyut kazanmasına yol açmıştır. Güvenlik ortamının barıştan itibaren şekillendirilmesine yönelik ortaya çıkan ihtiyaç; savaş ortamında sayısal ve coğrafyaya yönelik üstünlük anlayışının yerine bilgi, teknoloji ve etki üstünlüğünü getirmiştir. Klasik savaş anlayışı terkedilmiş, yerine güvenlik ortamının barış zamanında şekillendirilmesi, savaş dışı hareketler, kriz

yönetimi ve sınırlı güç kullanımı gibi öncelikle caydırıcı etkiye sahip olan; en son aşamada kesin sonuçlu konvansiyonel savaşı devreye sokan bir mücadele stratejisi geliştirilmiştir.

Bilgi teknolojilerindeki gelişim paralelinde, ülkeler güvenlik stratejilerini teknoloji tabanlı bir savaşa dayandırma arayışına girmişlerdir. Teknolojik Savaş ya da diğer bir deyişle Bilgi Savaşı (Information Warfare) bilgisayar mikroişlemcilerinde ve iletişimde modern sensör ve röle devrelerinin üretilmesiyle fiilen başlamıştır (TSK Bilgi Harbine Nasıl Hazırlanmalıdır?, s. 62).

Gelişen teknolojinin baskın tesirini arttırması; teknolojik bilgiye dayalı yeni sistemlerin Silahlı kuvvetlerin her kademesinde kullanılması gerekliliğini kaçınılmaz hale getirmiştir. ABD’nde yapılan çalışmalara göre 2010 Yılına kadar savaş alanı elektronikleşecektir. Her asker ve her silah sistemi elektronik iletişim şebekesine bağlanacaktır. ABD Ordu Araştırma ve Geliştirme Laboratuvarı (Natick-Massachusetts) 21 nci yüzyıl askerinin savaş giysisini tasarlamıştır. Helmette (koruyucu başlık) mikrofon ve kulaklık olacak, gece görüş dürbünü ve termal görüntüleme sensörü ile arazi üzerinde nerede bulunduğunu gösteren ve devamlı, güncel hedef bilgilerini içeren göz-vizörü takacaktır. Mikro işlemcilerdeki yenilikler silah sistemlerinin daha küçük boyutta üretilebilirliğini sağlayacaktır. Uzaktan kontrollü insansız hava araçları yer hedeflerinin tam doğrulukla saptayabilecektir. Geleceğin savaşlarında uçaklar yerlerini insansız hava araçlarına bırakacaktır (TSK Bilgi Harbine Nasıl Hazırlanmalıdır?, s. 64).

John Hopkins Üniversitesi Uygulamalı Fizik Laboratuvarında bilim adamları Super Elit Bilgisayarı üzerinde çalışmalarını yoğunlaştırmıştır. Bu bilgisayar radar sinyallerini alarak, işleyip grafik haline getirebilir ve ekranda üç boyutlu savaş alanı modeline dönüştürebilir özelliktedir. Komutan harita veya arazi modelindeki semboller yerine ekranda üç boyutlu model üzerinde dost ve düşman savaş araçlarının grafik resimlerini ve özelliklerini görerek yerleri, hareketleri ve imkan kabiliyetleri üzerinde muhakeme yapabilir. Bilgisayar ekran başında kimse olmaksızın vurulacak hedefi seçip ikaz edebilir. Bilgisayar bir tehdit sinyali aldığında ikaz düzeniyle ilgilileri ekran başına çağırabilir.

Günümüzde ileri memleketlerin orduları geleceğin bilgi savaşları için yoğun hazırlıklar yapmaktadır. Gelecekte ABD; müttefiklerinin Körfez Savaşı'nda olduğu gibi saldırıya uğraması durumunda, askerlerle ve savaş gemileriyle yardım göndermek yerine, saldırgan tarafa mouse, video ekranları ve klavyelerle müdahale etmeyi planlamaktadır.

Önce saldırgan ülkenin telefon şebekesine, bütün telefon sistemini çökertecek bir bilgisayar virüsü sokulacaktır. Daha sonra, önceden belirlenmiş bir zamanda harekete geçmesi için programlanmış olan bilgisayar mantık bombaları demiryolu hatlarını ve askeri konvoyları kontrol eden elektronik yönlendiricileri işlemez hale getirecektir. Bu sırada düşman kuvvetlerinin komutanları, telsizlerinden aldıkları emirleri sahte olduklarını bilmeden uygulayacaktır.

Özellikle psikolojik hareket için donatılmış olan ABD uçakları, halkı ülkenin başındaki yöneticiye karşı ayaklandıracak propaganda mesajları ile düşmanın televizyon yayınlarını altüst edecektir. Bütün bunların tek kurşun atılmadan yapılacağı kabul edilmektedir. Virginia'da ve Pentagon'da Bilgi Savaşının konsept çalışmaları ve diğer hazırlıklar yapılmaktadır. Bilginin savaş hedefi olarak kullanılması savaşın şeklini değiştirecektir.

Amaç, 20. yüzyılın sonlarındaki teknolojik mucizeleri, düşmanın askeri ve sivil altyapısına hızlı, gizli, yaygın ve yıkıcı saldırılar başlatmak için kullanmaktır. TIME dergisinin yaptığı röportajlar sonucunda, Pentagon'un savaş alanını bilgi teknolojisi ile yenileyip, tankların I. Dünya Savaşı'ndaki ve atom bombasının II. Dünya Savaşı'ndaki etkinliği gibi bir etkinliği, gelecek savaşlarda bilgiyi kullanarak, yapmayı planladığı anlaşılmaktadır.

Amerikan ordusunda, donanmasında ve hava kuvvetlerinde bilgi savaşı karargahları oluşturulmaktadır. Geçtiğimiz Haziran ayında Washington'daki National Defence University, bilgisayar saldırılarına karşı savunmadan, savaş manevralarının sanal gerçeklikle planlanmasına kadar birçok alanda özel olarak yetiştirilmiş 16 bilgi savaşı subayını mezun etmiştir. Temmuz ayında da Newport'taki Deniz Harp Okulu'nda bilgi savaşı uzmanları tarafından, düşmanın bilgisayar sistemlerini felce uğratan küresel bir savaş oyunu oynanmıştır. Bu yıl sonunda Pentagon subayları, son iki yılda gerçekleştirilen bir düzine gizli bilgi savaşı oyunundan alınan sonuçları,

gelecekte askeri taktiklerin nasıl değiştirilmesi gerektiğini belirlemek için inceleyecektir.

ABD Milli İstihbarat Örgütü (The National Security Agency-NSA); ordu, donanma ve hava kuvvetlerindeki çok gizli istihbarat birlikleri ile birlikte, halihazırda ev ve işyerlerindeki bilgisayarlara bulaşan virüs tipleri ile düşmanın bilgisayar sistemlerine zarar verme yollarını araştırmaktadır. "Mantık bombası" adı verilen bir başka virüs de, düşman sistemine yerleştirildikten sonra, önceden belirlenmiş bir zamana kadar cansız ve hareketsiz kalıp, harekete geçtiğinde verileri yok etmeye başlayacaktır. Bu tip bombalar ile bir ülkenin hava savunma sistemine ya da merkez bankası bilgisayar sistemine saldırılabilir. ABD Merkezi İstihbarat Örgütü (Central Intelligence Agency-CIA)'nın, bir silah üreticisinin, potansiyel bir düşman ülkeye sevk edeceği silah sistemlerinin içerisine bubi tuzaklı bilgisayar çipleri yerleştirecek gizli bir programı vardır. Bu teknik chipping olarak adlandırılmaktadır. Bir diğer programda ise ABD Milli İstihbarat Örgütü, silah sistemlerine yazılım hazırlamaları için silah üreticileri tarafından sözleşmeye bağlanan bağımsız müteahhit firmalarının, hazırladıkları yazılımlara virüs bulaştırmanın nasıl sağlanacağını yollarını aramaktadır.

Bilgi teknolojisi uzmanı olan bir CIA kaynağı şöyle söylemektedir:

"Silah satıcısının şebekesine giriyorsunuz. Silah üreticisinin ikmal sistemine girerek virüs yerleştirilecek parçayı seçersiniz, parçayı ele geçirip içine virüsü yerleştirirsiniz. Silah üreticisi silahı tamamlayıp yabancı ülkeye yolladığında, silahın içinde aktif olmayan virüs vardır. Silahı alan ülke ileride hasım konumuna geçerse uzaktan göndereceğiniz bir kodla silahı işlemez hale getirirsiniz. Her şey çalışıyor gibi görünse de, örneğin savaş başlığı patlamaz."

Bilgi savaşı silahları, bilgisayar virüslerinden çok daha değişik, alışılmamış olabilir. New Mexico' daki Los Alamos Milli Laboratuvarında yüksek güçlü elektromanyetik puls (EMP) üretebilen çanta büyüklüğünde bir aygıt geliştirilmiştir. Komandolar yabancı bir başkente gizlice girebilir, EMP çantasını bir bankanın yanına yerleştirebilir ve sistemi çalıştırabilirler. Sonuçta ortaya çıkan pulslar binadaki bütün elektronik parçaları yakacaktır. Diğer öneriler, biyoloji ile elektroniği birleştirmektir. Örneğin, Pentagon görevlileri, mikroorganizmaların çöpleri yok

etmesi gibi, mikropların da bilgisayarların içindeki elektroniği ve yalıtkan malzemeyi yok etmek için yetiştirilebileceklerine inanmaktadır.

Bilgi savaşları haber alma tekniklerinin geliştirilmesini teşvik etmektedir. Pentagon halihazırda uydulara, ajan uçaklara ve yerdeki düşmanı izlemek için içine kameralar yerleştirilmiş insansız uçaklara sahiptir. Gelecekte binlerce minik sensör havaya gönderilebilir. Massachussetts Teknoloji Enstitüsü Lincoln Laboratuvarı'nda, fotoğraf çekebilen, sigara paketi büyüklüğünde bir insansız hava aracı yapılmaya çalışılmaktadır.

Bilgi savaşı, sıcak savaş muhtemelen önleyebilir. Bunun yanı sıra, kullanılan teknikler ve teknoloji gerçek bir sıcak savaşın yönetimini kolaylaştırabilir ve konvansiyonel silahlı kuvvetlerdeki eksikleri telafi edebilir. Yüksek rütbeli subaylar, gelecekteki savaşlarda savaşabilmek için bilgi işleme ve iletişim konularında Amerika'nın teknolojik önderliğinden yararlanmaları gerektiğine inanmaktadır.

Geçen Mayıs ayında Kansas, Fort Leavenworth'de yapılan bir savaş tatbikatında, bilgi işlem cihazları ve 2010 yılına kadar Amerikan ordusunun hizmete almayı planladığı yüksek teknoloji silahlarla donatılmış olan 20 000 kişilik bir Amerikan piyade tümeni, üç misli büyüklüğündeki Kuzey Kore ordusuyla karşılaştırılmıştır. Savaş emirlerini hızla ileten bilgisayarlar ve savaş alanında düşmanı çok daha iyi gösteren sensörler sayesinde Amerikan ordusu üstünlük sağlamıştır.

Johns Hopkins Üniversitesi Uygulamalı Fizik Laboratuvarı'ndaki bilim adamları Force Threat Evaluation and Weapon Assignment adı verilen, her şeyi bilen bir bilgisayar sistemi üzerinde testler yapmaktadır. Bu sistem, bir donanma grubunun radar sinyallerini alıp, bunları amiralin ekranda izleyebileceği şekilde üç boyutlu görüntü haline çevirir. Amiral, ekranda karmaşık semboller yerine düşman ve dost uçakların grafiklerini görür. Bir mouse kullanarak, tehdide herhangi başka bir açıdan bakmak için görüntüye müdahale edebilir. Bilgisayar, saldırılması gereken hedefleri gösterir ve hatta ekranın başından uzaklaşıldığı sırada dahi gökyüzünü taramaya devam eder.

Amerika, 2010 yılına kadar, her askerin ve silah sisteminin elektronik olarak birbirine bağlanmasıyla savaş alanlarını sayısallaştırmayı hedeflemektedir.

Geleceğin savaşlarının, günümüzün bilim kurgu gerilim filmlerine benzeme ihtimali vardır. Günün birinde liderler, gerçek bir savaşa girmeye karar vermeden önce, aralarında sanal savaş yapacaklardır. Bazı bilimkurgucular, kimin kazanacağına karar vermek için ülkelerin, gerçek savaş yapmak yerine bilgisayar savaşlarına yöneleceğini söylemektedir.

Bütün bunlar, askeri kuvvetlerin büyük çapta yeniden yapılanmasını gerektirebilir. İçlerine yerleştirilmiş mikroişlemciler sayesinde elektronik olarak kumanda edilebilen insansız uçak ve gemilerle, hedefleri takip ederek isabet kaydeden küçük boyutlu akıllı silah sistemlerinin kullanılmasıyla, uçak gemileri ve insanlı bomba uçakları gelecekteki savaşlarda kullanılmaz hale gelebilirler (Waller, 1995, s. 26-34).

Enformasyon teknolojileri silahlı kuvvetleri her seviyede ve her fonksiyonel sahada etkilemekte ve değiştirmektedir. Yazılımın ön plana çıkmasıyla devrim niteliğinde sayılan bu değişimin etkilediği sahaların başında, kuvvetlerin tertiplenmesi (stratejik tertiplenme) ve muharebe sahası taktikleri gelmektedir (TSK Bilgi Harbine Nasıl Hazırlanmalıdır?, s. 69).

Dünyada savunma sanayinin gelecekte kavuşacağı yapının esasını bilgi tabanlı teknolojilerin oluşturacağı fikrinden hareketle; yirmi birinci yüzyılın savaş alanlarında hangi sistemlerin kullanılabileceği öngörülebilir (Ayhan, 2002, s. 159) :

- Geleceğin piyade askeri ABD'nin Raytheon firması tarafından "Land Warrior prototipiyle tasarlanmıştır. Bu sistemde; entegre miğfer, yazılım, bilgisayar/telsiz, silah, koruyucu üniforma ve bireysel teçhizat grubu yer almaktadır.

- 2000'li yıllarda savaşan birlikler pek çok sayıda karmaşık bilgisayar sistemleri kullanma durumunda olacaktır. Bunlar silahlar içerisine yerleştirilmiş küçük mikro işlemciden, mobil komuta kontrol merkezlerine kadar geniş bir alana yayılmış bilgisayar sistemleridir.

- Yirmi birinci yüzyılda gelişmiş sensörler ve mikro işlemcilerle teçhiz edilmiş, yapay zeka ile yön bulup ilerleyebilen, hedef tespit edebilen, muharebe cihazlarını kullanabilen robot araçlara sahip olacaktır. Bu araçlar; bağımsız olarak, ya da yüksekten uçan bir hava aracı ile takviyeli olarak çalışabileceklerdir.

- Robotlar özellikle cebri keşif yaparak, düşman yerleşimi ve muharebe hasar tespit görevlerini rahatlıkla yerine getirebileceklerdir.

- Silah sanayindeki gelişmeler, boyut ve ağırlıkları arttırmadan, çok daha etkili atış yapabilen silahların ortaya çıkmasına yol açmaktadır. Yirmi birinci yüzyılda elektrik ya da elektro kimyasal tahrip ile çalışan 200 milimetrelilik bir sahra topunun tesirli menzili 300 mil, mermi hızı ise şu andakinin üç katı olacaktır. Yine aynı şekilde, bir antitank silahı 2.5 mil/saniye namlu ağzı hızı ile 2.5 mil uzaktan etkili olabilecektir.

- Lazer kullanan yönlü enerji silahları, elektronik karşı tedbirlerden tahrip etkisine kadar her yerde kullanılabileceklerdir.

- Mikro işlemci, sensör ve yapay zeka teknolojilerinin gelişmesiyle; yapımı son derece basit ve ucuza mal olacak akıllı cephaneler zırhlı, topçu, ulaşım araçları, komuta karargahları ve köprüler gibi hedefler için rahatlıkla kullanılabileceklerdir. Bu cephaneler ilgili bölgelere herhangi bir araçla serpilip burada bırakılacaklardır. Kendi sensörleri ve yapay zeka yetenekleri ile, düşman hareketini sezdiklerinde derhal harekete geçeceklerdir.

- Bilgisayarlar sayesinde muharebe ortamının tam bir coğrafik simülasyonu gerçekleştirilecek, muharebe eş zamanlı olarak gerçek zaman harp oyunları her seviyedeki komutanların kullanabilecekleri bir simülasyon şeklinde oynanabilecektir.

- Sözel ya da formlar şeklinde verilen direktifleri kararlara dönüştüren yazılım paketleri kullanılacaktır. Bu paketler, tıpkı insan gibi aldığı direktifleri kararlara dönüştüreceklerdir.

- Yeni teknolojik imkanlara dayanan yeni yöntemlerden biri de "Zayıatsız Savunma"dır. Zayıatsız savunma elektromanyetik, akustik, kinetik v.b. gibi silahlarla, düşmanın insan gücünü öldürmeden, malzeme ve teçhizatını etkisiz kılan, tahrip eden ve fonksiyonsuz hale getiren silahlarla icra edilecektir.

- İnsansız taktik uçaklar kullanılacak, ulaştırma uçaklarının menzili ve taşıma kapasitesi muhtemelen 15 kat artacaktır. Hipersonik füzeler, taktik balistik füzeler korumalı yer hedeflerinin tahribi için etkili olacaklardır (Ayhan, 2002, s. 160).

2.2. Bilgi Savaşının Hedefleri

Günümüzde Milli Kritik Hedefler Listesi altında askeri hedefler üç bölüme ayrılmakta; politik hedefler, yapısal hedefler ve askeri kuvvetler başlıkları altında incelenmektedir. Bu hedefler öncelik sırasına göre aşağıdaki gibi sıralanmaktadır (Campen et al, 1996, s. 192).

2.2.1 Politik Hedefler

- Milli Hükümet Aygıtları ve Merkezleri,
- Bakanlıklar, Ana Karargahlar ve İdari Ofisler,
- Stratejik Komuta Kontrol Sistemini Destekleyen Birimler,
- Stratejik Komuta Yerleri (Mobil, Daimi, Hava, Deniz, Kara),
- Polis ve İç Emniyet Unsurları (Sivil Savunma, Jandarma v.b.),
- Karargahlar, İstihbarat Toplama Merkezleri,
- Destekleyici Birimler,
- Propaganda Sistemleri (Milli ve Uluslar Arası),
- Halkla İlişkiler, Kamuoyu Oluşturma, Psikolojik Harekat Birimleri,
- Kültür Merkezleri, Ağları,
- İletişim Ağları (Giriş Noktaları).

2.2.2.Yapısal Hedefler

- Bilgi Altyapısı,
- Açık ve Gizli İletişim Merkezleri,
- Telsiz Parkları ve Telefon Merkezleri,
- Fiber Optik Ağlar, Toplama Merkezleri ve Tekrar İstasyonları,
- Bilgisayar ve Bilgi İşlem Merkezleri,
- Milli C2 Merkezleri ve Uydu Bağlantıları,
- Enerji ve Güç Kaynakları,
- Enerji Üretim, Dönüşüm, Dağıtım ve Kontrol Merkezleri
- Pompalama ve Geri Dönüşüm Sistemleri,
- Ulaştırma,
- Yer Trafik Kontrol Merkezleri,
- Hava Trafik Kontrol Merkezleri,
- Destekleyici Bilgisayar ve Elektronik Sistemler,

- Mali Merkezler ve Ağlar,
- Bankalar, Ticaret Merkezleri ve Finansal Kuruluşlar,
- Nakit Akış Kontrol Merkezleri, Nakit Toplanan Yerler ve Destekleyici Birimler,
- Toplumsal Denge,
- Yiyecek ve Su Dağıtım Sistemleri ve Kontrol Noktaları.

2.2.3. Askeri Kuvvetler

- Stratejik Milli Savunma Unsurları,
- Erken Uyarı Sensörleri,
- Savunma Komuta ve Kontrol Merkezleri,
- Uydu Bağlantıları ve Uzay Tabanlı Sistemler,
- Muharebe Alanındaki Birlikler,
- Stratejik Saldırı Gücü Oluşturma Merkezleri,
- Klasik Askeri Güç Görevlendirme Sistemi,
- Klasik Olmayan Silah Sistemleri,
- Kontrol Merkezleri, Mobil Komuta Yerleri AR-GE Merkezleri.

Bu liste incelendiğinde; klasik savaşlardaki hedef kavramının tamamıyla değiştiği fark edilmektedir. Savaşlarda hedefin eskiden olduğu gibi sadece savaş alanındaki birlikler olmadığı, düşman ülkenin özellikle komuta, kontrol, haberleşme ve yönetim merkezlerinin öncelikli hedefler olarak tespit edildiği ortaya çıkmaktadır.

2.3. Senaryo

Aşağıda sunulan senaryo sınırlı güç kullanımına dayalı bir yirmi birinci yüzyıl savaşının basit olarak nasıl icra edilebileceğine yönelik olarak hazırlanmıştır:

Türk Silahlı Kuvvetlerinin Ankara'dan yönlendirilen uzaydaki TURKMILSAT uydusundaki sanal komuta yerinde; Türkiye'nin halen uzayda mevcut 12 adet haberleşme ve hedef tesbit uydusundan sağlanan istihbarat bilgilerinin ışığında hedef ülke için önceden tesbit edilmiş olası durum senaryolarından bir tanesinin uygulamaya geçirilmesi yolunda hazırlık kararı alınmış ve faaliyet başlatılmıştır. Hedef ülkeden elde edilen bilgiler eşzamanlı olarak bu karargaha ulaşmakta ve sürekli durum değerlendirmeleri yapılmaktadır. Olası durum senaryosunun uygulanmasını, elde edilen bu bilgilerdeki; hedef ülkenin askeri faaliyetlerindeki,

diğer zamanlardan farklı olarak meydana gelen artışın derecesi belirleyecektir. Sanal Komuta Yeri şimdilik hard killing silahların kullanılmasını gerektirecek bir durumun olmadığı; Kara, Deniz ve Hava Kuvvetlerinin “Görevin Gerektirdiği Hazırlık Derecesi-I” seviyesinde bulunmasının yeterli olacağını birlik komuta yerlerine bildirmiştir. Birliklerinin dışında bulunan askeri personele üzerlerinde taşıdıkları iletişim aygıtları vasıtasıyla birliklerine katılmaları mesajı ulaştırılmıştı.

Olası durum senaryosuna göre; öncelikle hedef ülkenin telekomünikasyon hatlarının bağ yerlerine bir virüs sızdırılacak, virüs içerisindeki mantık bombaları önceden belirlenmiş zamanlarda başlamak üzere patlatılarak, hedef ülkenin haberleşme, ulaştırma ve komuta kontrol sistemlerini tahrip edecektir. Bu sayede askeri konvoylar, havaalanları ve demiryolları ulaşımını düzenleyen elektronik sinyalizasyon sistemleri devre dışı kalarak askeri birliklerin stratejik intikalleri tam bir kaos ortamına döndürülecektir. Aynı anda düşman komuta kontrol sistemleri içerisine bırakılan mesajlar, hedef ülkenin alt seviyedeki birliklerine düzmece emirler olarak gönderilecektir. Bu birlikler haberleşme cihazlarından kendilerine ulaşan hatalı emirleri uygulama telaşına düşecekler, asılsız emirlerle yanlış istikametlere yöneltileceklerdir. Haberleşme sistemi tek taraflı çalıştığından en yakınlarındaki birliklerden bile gerçek durumun ne olduğunu öğrenemeyeceklerdir.

Bir sonraki safhada psikolojik hareket için düzenlenmiş program devreye girecek, hedef ülkenin televizyon, radyo ve İnternet kanalları propaganda mesajları ile karıştırılacaktır. Hedef ülkenin tüm dünya finans piyasalarındaki ekonomik göstergelerinin karşısında anlaşılmasız sayısal ifadeler görülmeye başlanacak, bu durum ülke içerisinde büyük bir huzursuzluk ve karışıklığa yol açacaktır.

İlerleyen saatlerde hedef ülkenin askeri faaliyetlerindeki yoğunluk hızla artmaya başlamıştır. Sanal Karargahtan beklenen emir de gelmiştir: “Görevin Gerektirdiği Durum-II seviyesine geçilsin ve senaryo uygulanmaya başlansın.” Daha ilk aşamada hedef ülkenin haberleşme ve ulaşım sistemlerindeki kargaşayı fark etmemek mümkün değildir. Hedef ülkenin yöneticileri ve askeri yetkilileri bir savaşın içerisinde olduklarını anlamaya başlamıştır. Askeri faaliyetlerini barış seviyesine çekmek için çok az zamanları vardır. Hedef ülkenin dışişleri yetkilileri iletişim imkanı olan tek hatlarını, Birleşmiş Milletler hattını, kullanarak, acilen, Türk dışişlerini sanal barış görüşmelerine davet etmişlerdir. Görüşmeler neticesinde hedef

ülkeye verilen kısıtlı iletişim imkanı, onlara barış durumuna geçmek için gerekli ortamı sağlamıştır. Böylece tek bir mermi atılmadan, tek bir kişinin burnu kanamadan elde edilen sonuç Türkiye'nin teknolojik savaş gücünün yeni bir göstergesi olmuştur.

Aslında hedef ülkenin askeri istihbaratı, iki ay önce Türkiye'nin kendi sınır bölgelerinde yaptığı tatbikatı izlemişlerdi. Akıllı mühimmatların nasıl kullanıldığını, robot bölümünün savaş ortamındaki başarısını, arazide yaratılan lazer perdesinden Türk savaş uçakları ve taarruz helikopterlerinin nasıl geçtiklerini görmüşlerdi ve bu konulardaki ayrıntılı raporlarını göndermişlerdi. Nasıl olmuştu da kendi yöneticileri ve askeri yetkilileri bir savaş hazırlığına girmişlerdi?

2.2. Bilgi Savaşlarına Uzanan Yol

Bilgi aktarım miktarı Birinci Dünya savaşında telgraf üzerinden 30 kelime/dakika, İkinci Dünya Savaşında telem üzerinden 66 kelime/dakika, 1991'de Körfez Savaşında bilgisayar üzerinden 192 000 kelime/dakika olmuştur. Yapılan çalışmalarla bu miktarın 2010 yılında bir buçuk trilyon kelime/dakikaya ulaşması hedeflenmektedir. Bilgi akış hızına paralel olarak Amerikan İç Savaşında General Grant kararını bir haftalık bir sürede verirken, 1944 yılında General Patton aynı işi birkaç günlük sürede yapıyordu. 1991 yılında General Schwarzkopt ise saatlerle belirlenen sürelerde kararını veriyor ve uygulamaya geçiyordu. Aslında bilginin önemi yeni ortaya çıkmış bir kavram değildir. M.Ö 5 nci yüzyıldan itibaren ünlü savaş teorisyeni Sun-Tzu'dan başlayarak yirminci yüzyılda Liddell Hart'a kadar pek çok düşünür bilginin stratejik önemi hakkında bir çok söz söylemiştir (Komuta ve Kontrol, 1997, s. 43). Ancak Alvin Toffler'in şu sözleri bilginin stratejik öneminin sadece askeri boyutta düşünülmemesi gerektiğini ortaya koymaktadır.

” Bilgiyi diğer güç kaynaklarından ayıran hususlar; tükenmez olması, aynı anda karşılıklı olarak hem olumlu hem de olumsuz kullanılabilmesi ve en önemlisi, kuvvetin ve servetin aksine zayıfların ve yoksulların da sahip olabileceği bir unsur olmasıdır. Bilginin kontrolü, yarının tüm kurumlarında yer alacak, dünya çapındaki güç mücadelesinin özünü oluşturmaktadır” (Toffler, 1995, s. 69).

1980'lerden bu yana süratle gelişen bu yeni konseptin uygulamalarının ortaya konulması ilk defa Körfez Savaşında anlam kazanmış, bilgi savaşı ayrı bir konuma gelmiş, bilgi stratejik ve taktik bir güç olarak kullanılmış ve ABD, teknoloji ve bilgi gücünü askeri stratejisinin bir unsuru olarak kullanarak politik isteklerini Irak hükümetine kabul ettirmiştir. Sonuç almada bu kadar etkili bir güce sahip olduğunu Körfez Savaşında fark eden ABD ordusu 1994 yılında Bilgi Harbi Konsepti ve doktrininin geliştirilmesi ve tesbiti için çalışmalar başlatmıştır. ABD Savunma Bakanlığı bünyesinde teşkil edilen bir kurul Ocak 1995'ten itibaren uygulama çalışmaları da yapmakta ve bu çalışmalar bir seri tatbikatlarla analiz edilmektedir. Sivil alandaki uygulamalar ise 1996'dan itibaren başlatılmıştır. Kuzey Atlantik İttifakı (North Atlantic Treaty Organization-NATO) 1998 yılında Bilgi Harbi Konseptini kabul etmiştir. Fransa, Almanya ve İngiltere gibi ülkeler bu konuyla ilgili özel çalışmalarının yanı sıra NATO içerisindeki çalışmalara da destek vermektedir. Diğer taraftan Rusya, Kanada ve Çin'inde bilgi harbinin temel kavramlarına yönelik çalışmalar yaptığı ve projeler planladığı bilinmektedir.

Belki de en önemlisi Yunanistan ve İsrail'in Bilgi Savaşı kapsamında bilinçli çalışmalar yapmasıdır. Bilgi güvenliği hususunda bir hayli mesafe alan bu iki ülkenin çalışmaları konunun Türkiye açısından önemi bakımından oldukça dikkat çekicidir.

3. BİLGİ SAVAŞI NEDİR?

3.1. Bilgi Savaşının Tanımı

Bilgi Savaşı ile ilgili problemlerden birisi hala müşterek bir tanımının yapılmayıpıdır. Bunun başlıca sebebi bilgi savaşlarının göreceli olarak yeni bir konu olması ve değişik anlamlar içermesidir. Bir tarafta konunun askeri içeriği varken, diğer taraftan bilgi savaşları kavramı İnternet üzerinde yapılan mücadeleyi tanımlamak için kullanılmaktadır.

Bilgi Savaşları ile ilgili teknik bir tanım ilk kez konuyla ilgili bir seminerde Dr. John Alger tarafından verilmiştir:

Bu tanımda bilgi savaşı; “sahip olduğumuz bilgilerimizi, bilgi sistemlerimizi ve bilgi tabanlı yapılanmalarımızı korurken; rakibin bilgilerini, bilgi sistemlerini ve bilgi tabanlı yapılanmalarını etkileyerek bilgi üstünlüğünü sağlamamıza yarayacak her türlü faaliyetlerdir” şeklinde ifade edilmektedir (Libicki, 1996, s. 17).

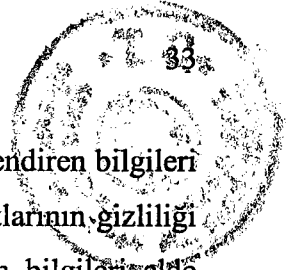
Bu tanım hem sivil hem de askeri tanımlamalar için kullanabilir. Nitekim Amerikan Hava Kuvvetleri Komutanlığı da bu tanıma benzer bir tanımla bilgi savaşının askeri tanımını yapmak için kullanmaktadır.

Bu tanımlamaya göre bilgi savaşı; "Düşmanın sahip olduğu bilgi ve onun fonksiyonlarını engellemek, imha etmek, bozmak ve kendi çıkarımız doğrultusunda kullanmak için yapılan hareketlerle, düşmanın bu faaliyetimize karşı önlem almasını engellemek ve benzeri hareketine karşı koymaktır" (Tatar, 2001, s.74).

Diğer yandan Winn Schwartau bilgi savaşını tek bir tanımda her seviyeyi içerecek şekilde tanımlamak yerine üçe bölerek daha ayrıntılı bir tanım önermiştir. Schwartau bilgi savaşlarını hedeflerine göre üçe ayırmıştır (Libicki, 1996, s. 63).

3.1.1. Bireysel Bilgi Savaşı

Bu tanım şahsi elektronik özel hayata yönelen saldırıları ifade etmektedir. Bilginin depolandığı yerlerdeki bilgi tabanına yapılan girişleri ve dijital kayıtların ortaya çıkarılmasını içermektedir. Günümüzde ortalama bir insanın kendisi hakkında



depolanmış bilgileri kontrol edebilme imkanı çok düşüktür. Bizi ilgilendiren bilgileri doğru olup olmasalar da kontrol etmemiz güçtür. İnsanlar özel hayatlarının gizliliği konusunda endişe duymaktadır. Geçmişte bir kişi hakkında istenen bilgileri elde etmek için bir casusun telefon hatlarına girmesi veya minyatür kamera ve dinleyiciler kullanılması gerekliydi. Günümüzde bu imkanlar daha da minyatürize edilerek kullanılmakla birlikte artık bilgilerin pek çoğu mevcut bilgi tabanlarından rahatlıkla elde edilebilir. Bir kişiye şantaj yapmak için artık onu aylarca izlemeye gerek yoktur. Bilgi savaşı telefon hatları üzerinden bir bilgisayar yardımıyla istediğimiz bilgileri elde etmemizi sağlayacaktır. Açığa vurduğumuz bilgilerimiz ele geçirilmeye müsaittir. Dürüst olmak gerekirse hiç birimiz kredi kartı bilgilerimizin, hastane kayıtlarımızın ve adli işlem kayıtlarımızın açığa çıkmasını ve İnternet üzerinden tüm dünyaya yayılmasını istemeyiz. Daha da kötüsü eğer bu bilgilere birisi nüfuz edebiliyorsa bunların değiştirilebileceği gerçeğidir. Yapılacak bir hata veya kasıtlı değişiklik sonucu, hayatınız boyunca hiç kimsenin sorumlu olmadığı bir alanda bu bilgilerin doğruluğunu ispat etmekle uğraşabilirsiniz. Günlük yaşamda kullandığımız bilgilere artık sıkıca bağımlıyız. Eğer herhangi bir kişi adli ve mali kayıtlarınıza ekleme yapabiliyorsa; kullandığınız kredi kartının çalıntı olmadığını, pasaportunuzun sahte olmadığını, uyuşturucu kaçakçısı olmadığınızı ya da interpol tarafından aranmadığınızı devriye arabasındaki bilgisayarı üzerinden hakkınızda bilgi alan polis memuruna nasıl izah edebilirsiniz. Hepsi bir araya toplanacak olursa, sonuç olarak şunlar söylenebilir.

- Birarada tutulan binlerce bilgi hayatımızın dijital imajını oluşturmaktadır.
- Bilgisayarlardaki hakkımızda tutulan bilgilerin değiştirilebildiği bir gerçektir.
- Elde edilebilir bilgiler doğrulanamamaktadır.
- Elde edilen yanlış bilgileri doğrulamak oldukça zordur.

Kişisel bilgi savaşları şimdilik potansiyel bir tehdit olarak görülmemektedir. Fakat herhangi bir kişinin kimliğini açığa çıkarabilir, tahrip edebilir veya değiştirebilirsiniz. ABD başkanlık seçimleri öncesinde başkan adaylarının özel yaşamlarına ait bilgilerin medya ve İnternet vasıtasıyla yayılması, başkanın şahsında, neredeyse dünyanın siyasi gidişatını etkileyebilecek boyutta etkiye sahip olmaktadır.



3.1.2. Şirketlerarası Bilgi Savaşı

Bir anlamda günümüzdeki şirketlerin arasındaki rekabeti ifade etmektedir. Rakibinin yaptığı pazar araştırmasına ait bilgi tabanına girerek 15 milyon dolar mülk olmuş araştırma sonuçlarını elde etmek için 1 milyon dolar harcamayı göze almış pek çok şirket vardır. Bunun yanı sıra rakip şirketin yeni bir ürünle pazarda yer almasını engellemek amacıyla o şirketin yeni ürünü ve pazar araştırmasıyla ilgili bilgi tabanının tahrip edilmesi veya “kazayla” bir virüs tarafından etkilenmesi de imkan dahilindedir.

Bu çeşit bilgilere yönelik mücadele yeni bir oluşum değildir. ABD ve Sovyet Rusya’nın bilgi casuslarının bu tip faaliyetleri Soğuk Savaş döneminden çok iyi hatırlanmaktadır. O zamanlarda bu faaliyetler, sanayi casusluğu tanımı altında yer alıyordu.

Günümüzde şirketler arası bilgi savaşının başka bir boyutu da oluşmuştur. Artık devletlerde bu oyunun içerisinde aktif olarak rol almaktadır. Devletler öğrencilerin yurtdışı eğitimi görmelerini desteklemekte; onlardan uyanık olmalarını istemekte sadece üniversitelerde gördükleri eğitimin neticelerini değil aynı zamanda stajlarında çalıştıkları uluslararası şirketlerin bilgilerini de ülkelerine taşımalarını talep etmektedir.

Bu tip bilgi savaşı sadece bilgilerin ele geçirilmesini değil aynı zamanda gerçek veya hayali bilgi dağıtmayı da içermektedir. Astıma karşı yeni bir ilacı piyasaya sürecektir olan bir ilaç firmasına karşı rakip firmanın faaliyet gösterdiği ülkenin laboratuvarlarında yapılmış bilimsel bir araştırma sonucu ilaç daha piyasaya sürülmeden bu ilacın hammaddesinin akciğer kanserine yol açtığını gösterebilir. Bu sonuç medya yoluyla bilimsel bir yaklaşımla tüm dünyaya açıklanabilir. Bu durumda henüz ilacı piyasaya sürmemiş olan firmanın yapacağı tek şey milyonlarca dolar harcayarak yeni ilacın kansere sebebiyet vermediğini ispatlamak veya para sarf ettiği yatırımdan vazgeçmektir.

Aynı şekilde bir örnekte bilgisayar dünyasından verilebilir. Otomobil hava yastıklarını kontrol eden bilgisayar chipinin yüzde yüz randımanlı olmadığı iddiasına karşı chipi üreten firmanın yapacağı şey herhalde kamuoyu önünde yüz tane hava yastığını patlatmak değildir.

3.1.3. Küresel Bilgi Savaşları



Bu tip bilgi savaşının hedefi tüm ülkeler, küresel ekonomik güçlerdir. (Şirketler, Uluslar arası Para Fonu-IMF, Dünya Bankası v.b.) Sadece araştırma sonuçlarının ele geçirilmesi amacından daha çok ülke ve şirket sırlarının çalınması ve bu sırların sahiplerine karşı silah olarak kullanılmasıdır.

Diğer iki grubun etkisinden çok daha fazla etkiye sahip olan küresel bilgi savaşında para ve şahıslar çok önemli değildir. Önemli olan küresel etki yaratacak olan bilgi gücünün ele geçirilmesi ve bunun kullanılmasıdır. Totaliter rejimlere sahip ülkelerin veya terör örgütlerinin yaptığı kimyasal ve biyolojik silah araştırmaları, nükleer teknolojiye salt askeri anlamda sahip olma çabaları; bu güçlerini kullanmaya yönelik niyetleri bir şirket veya şahsı devre dışı bırakmaktan çok küresel tahrip etkisi yaratmayı hedeflemektedir. Nitekim 11 Eylül 2001 günü ABD’de Dünya Ticaret Merkezine ve Pentagon’a yapılan terörist saldırılar ve devamındaki gelişmeler bu etkinin boyutlarını gözler önüne sermiştir. Basit anlamda ele alacak olursak; bir üçüncü dünya ülkesini yöneten diktatör bu teknolojiyi elde edebilecek bilgi tabanına erişmek için 200 milyon doları harcayabilmektedir. Söz konusu saldırının Wall Street’e yapılmış olduğunu farz edelim. Herhalde önce ABD bankacılık sisteminde ve devamında dünya ticaretinde yaratacağı negatif etkiden nasibini almayan ülke ya da kuruluş kalmazdı.

Kimi zaman bireysel maksatlarla da yasadışı faaliyetlerde bulunan kişi ya da gruplar, küresel anlamda İnternet üzerinden eylemlerde bulunmaktadır. Genel olarak siber terörizm olarak adlandırılan bu eylemlerin ciddiye alınmadığını söylemek mümkün değildir. Nitekim; ABD’nin Irak’ı vurmak için askeri hazırlıklarını yoğunlaştırdığı günlerde, Malezyalı bir hacker, Irak vurulduğu takdirde dünyanın en yıkıcı virüsünü yayma tehdidinde bulunmuştur. ABD’nin Afganistan’a yönelik operasyonunun ardından El Kaide lideri Usame bin Ladin’e sempati duyduğunu açıklayan ve ABD’yi cezalandırmak için onun ismiyle yüzbinlerce bilgisayara virüs bulaştıran Vladimir Chamkovich isimli hacker, şimdi aynı şeyi Irak için yapacağını açıklamıştır. “Melhacker” lakaplı 23 yaşındaki bilgisayar korsanı ABD’de yayımlanan New York Post gazetesine gönderdiği e-postada, ABD’ye ve bu savaşta onu destekleyen her ülkeye virüsleri aracılığıyla savaş açacağını bildirmiştir. E-postasında, “Savaştan nefret ediyorum. İnsanların ölmesinden nefret ediyorum”

diyen Melhacker, virüsle küresel ekonominin dahi zarar göreceğini söylemiştir. İDefence isimli İnternet güvenlik şirketi de, Melhacker'ın süper tehlikeli virüsler olarak tanımlanan SirCam, Klez ve Nimda kutlarını biraraya getirdiğini ve Scezda adı verilen bir virüs yarattığını ifade etmiştir. Virüs yazılımcısı Melhacker'ın bugüne kadar Nedal (tersten okununca Laden), VBS.OsamaLaden.mm, BugBear, Melhack, Kamil ve BleBla.J kurtlarını yazdığı veya yazımında yer aldığı belirlenmiştir. Rus ve Pakistanlı hackerlar ile işbirliği içinde olduğu belirtilen Melhacker'ın, El Kaide Örgütü ile de yakın ilişkiler içinde bulunduğu tespit edilmiştir. İnternet güvenliği için çalışan firmalar da bu tehdidi ciddiye aldıklarını belirtirken, virüsün milyarlarca dolar arar yaratabileceğini doğrulamıştır (Malezyalı Hacker Irak İçin Vuracak, 2003).

Yukarıdaki bölümlerde Bilgi Savaşının değişik kaynaklardan yapılan tanımlarını açıklamaya çalışıldı. Ancak konu gereği olarak Türkiye'de bilgi savaşı kavramının nasıl algılandığı ortaya konulmalıdır.

Türkiye'de bilgi savaşı kavramı 1990'dan itibaren literatüre girmiştir. Özellikle Türk Silahlı Kuvvetlerinin Komuta Kontrol sistemleri kapsamında yürüttüğü çalışmalar esnasında bu sistemlerin güvenliğinin ve etkin kullanılabilmesinin ancak etkili bir bilgi güvenliği ile sağlanabileceği görülmüştür. Konuyla ilgili konsept ve doktriner çalışmalara hız verilmiş, yönergeler hazırlanmıştır. Başlangıçta iletişim ortamı güvenliği için kullanılan muhabere güvenliği (COMSEC), bilgisayarların kullanıma başlanmasıyla, bilgisayar güvenliği (COMPUSEC) ve söz konusu ortamların entegrasi sonucu bilgi güvenliği (INFOSEC) askeri literatüre girmiştir (TSK Bilgi Harbine Nasıl Hazırlanmalıdır?, s. 89).

NATO Bilgi Harekatı Konseptine göre Bilgi Harekatı;

“Politik ve askeri hedefleri desteklemek amacıyla, kendi bilgi ve bilgi sistemlerini etkili bir şekilde kullanarak ve korurken, hasmın bilgiye dayalı işlemlerini, komuta kontrol (C2), muhabere ve bilgi sistemlerini etkileyerek karar vericilerin müessir olmalarını sağlamak maksadıyla icra edilen faaliyetlerdir.” şeklinde tanımlanmaktadır (Tatar, 2001, s. 74).

Şimdi Türk Silahlı Kuvvetlerinin bilgi savaşının tanımını nasıl yaptığını inceleyeceğiz. Türk Silahlı Kuvvetleri Bilgi Harekatı Konseptinde Bilgi Savaşı bir

dizi harekatı ifade etmektedir. Başka bir deyişle Bilgi Savaşı, çeşitli Bilgi Harekatlarından oluşmaktadır. Bilgi Harekatı ise;

“Karar vericiler tarafından ortaya konulan hedeflere ulaşılmasını desteklemek için, kendi bilgi ve/veya bilgi sistemlerini etkin kullanırken ve korurken, başkalarının bilgi ve/veya bilgi sistemlerini etkileyerek yapılan faaliyetlerdir” şeklinde tanımlanmaktadır (TSK Bilgi Harbine Nasıl Hazırlanmalıdır?, s. 7).

Bilgi Harekatı barışta, krizde, çatışmada ve tekrar barışa geçişte olmak üzere geniş bir alanda uygulanabilmektedir. Bu hareket stratejik, operasyonel ve taktik seviyede icra edilebilmektedir. Bilgi Harekatı tüm ülkeyi ve ülkenin kurumlarını kapsamaktadır. Sürekli bir faaliyettir. Bilgi Harekatının vizyonu, barış, kriz ve savaşta milli ve askeri hedeflere ulaşmak amacıyla, bilgi üstünlüğünü sağlamak ve sürdürmektir.

Bilgi Savaşının hedefi; “Bilgi avantajı sağlayarak, düşman üzerinde üstünlük ve tam kontrol sağlamaktır” (TSK Bilgi Harbine Nasıl Hazırlanmalıdır?, s. 7).

Yapılan tanımların hepsinin ortak paydalarını alıp benzer bir tanım yapılabilir: Bilgi Savaşı; bir taraftan; teknoloji temeli olan bilginin kullanılarak bilgi ortamının kontrol edilip, kısmi ya da stratejik düzeyde milli menfaatlerin elde edilmesine yönelik olarak kullanılması yönündeki faaliyetleri ifade ederken, diğer taraftan; düşmanın yapabileceği bir bilgi savaşına karşı alınacak tüm aktif ve pasif tedbirleri de içermektedir. Genel olarak tanımdan da yola çıkarak taarruzi ve savunma bölümleri açık olarak ortaya konulan bilgi savaşının diğer alt bölümlerini ise kesin olarak ayırmak oldukça zordur. Bu kapsamda ancak uygulama araçlarına göre bir tasnif sözkonusu olabilir (Tatar, 2001, s. 74-76).

3.2. Bilgi Savaşının Bölümleri

3.2.1. Komuta Kontrol Savaşı

Bilgi savaşının askeri kuvvetlerinde kullanıldığı çatışma ortamlarında icra edilen kısımıdır. Fiziki imhayı da içermektedir. Amacı düşman komuta kontrol merkezleri ile savaşan askeri kuvvetlerin arasındaki komuta bağlantısının kırılmasıdır. Körfez

Harekatında, ABD ve İngiliz birlikleri tarafından, Irak ordusunun komuta kontrol merkezlerinin imha edilmesi suretiyle uygulanmıştır.

3.2.2. İstihbarat Temelli Savaş

Taktik resmin elde edilmesi maksadıyla kullanılan tüm vasıtalar ve sensörler ile bu bilgileri işleyen, değerlendiren ve askeri birliklere yayan sistemleri kapsamaktadır. Amacı, savaşın bilinen bir parçası olan sürprizleri engellemek ve komuta merkezlerine planların şekillendirilmesinde yardımcı olmaktır. İyi bir istihbarat, harekatın koordinasyon ve senkronizasyonunu sağlar. Savaş başladığında bir tarafta görevini anlamış ve yerine getirmeye hazır askeri birlikler varken, diğer tarafta karışıklık ve şok yaşayan birlikler yer alır.

3.2.3. Elektronik Harp

Düşmanın elektromanyetik spektrumu kullanmasına engel olmak veya yeteneğini azaltıp, kendi kuvvetlerimize etkin kullanımını sağlayarak elektromanyetik spektrumdan daha fazla yararlanmak amacıyla icra edilen askeri faaliyetlere elektronik savaş adı verilmektedir. Bunlar Elektronik Destek Tedbirleri (EDT), Elektronik Karşı Tedbirler (EKT) ve Elektronik Koruyucu Tedbirler (EKOT) adları altında üç bölümde incelenmektedir.

3.2.4. Bilgisayar Korsan Savaşı

İşlemci temelli sistemlere karşı yapılan bir savaş türüdür. Bu çeşit savaş şahıslar, şirketler ve devlete karşı uygulanabilir. Düşmana karşı, fiziki bir kuvvet müdahalesi yapılmaksızın, bilgisayar virüsleri gibi daha çok yazılım tabanlı araçlar kullanılmaktadır. Bir tür gayrinizami bilgisayar savaşı olarak değerlendirilebilir.

3.2.5. Ekonomik Bilgi Savaşı

Bilgi savaşı ve ekonomik savaş, aynı boyutta, bilgi ambargosu ve bilgi emperyalizmi metotlarıyla ekonomik bilgi harekatına dönüştürülebilir. Bir bilgi ambargosu ekonomik ambargoya benzer şekilde hedef ülkeye ekonomide kullanılan bilgi girişini fiziksel anlamda engelleyerek uygulanır. Hedef ülkenin dünya pazarlarıyla olan iletişimi engellenebilir. Bilgi emperyalizmi ise; hedef ülkenin etkin

ve söz sahibi olduđu belli bařlı endüstrilerin dünyadaki pazar payını, diğerk rakip ÷lkelere sađlanacak teknoloji transferi veya ekonomik bilgi giriřiyle daraltmaktır.

3.2.6. K÷lt÷r Empozesi

Psikolojik savař kapsamında deđerlendirilmekle birlikte, savařın öncesinde d÷řman ÷lkenin deđer yargılarına ve bilinç seviyesine, özellikle iletiřim vasıtaları kullanılarak, bir yönlendirme yapılmakta ve toplumda kabulleniş yaratılmaktadır. Uzun sürelidir. Süreç sonunda kimi zaman d÷řman ÷lkenin kuvvetleri bir kurtarıcı gibi algılanabilmektedir.

3.2.7. Beyin Göçü

Bilginin depolama ve işleme ortamlarını deđerlendirdiğimizde en önemli araç olarak karřımıza insan beyni çıkmaktadır. Bu kapsamda bir ÷lkenin beyin gücünü oluşturan nüfusuna yönelik Bilgi savařı kapsamında bir tehdit söz konusudur. Eđitim ve buna benzer amaçlarla yurtdışına gönderilen bu kitleye karřı sistematik bir yaklaşımla uygun řartlar ve imkanlar sađlanarak geri dönmeleri engellenmekte, bu suretle rakip ÷lkenin beyin gücü ve bilgi potansiyeli kayba uğratılmaktadır.

3.2.8. Propaganda/Psikolojik Savař

Politik ve askeri hedefleri ele geçirmek maksadıyla, d÷řman, dost ve tarafsız olan kesimlere yöneltilen davranış ve tutum deđiřtirmeye yönelik planlanmış psikolojik etki faaliyetleridir. Savařta ve barıřta uygulanabilir.

3.2.9. Siber Savař

Bilgisayar ve ađ sistemlerini esas alan bir savař türüdür. Üç alt kategoriye ayrılmıştır. Bunlar;

- Bilgi Terörizmi: İnsanlara ait özel bilgilerin açığa çıkarılarak kamuoyuna açıklanması veya bu insan ve topluluk bilgi kartlarına yanlış bilgilerin girilmesi şeklinde uygulanmaktadır.

- Semantik Hücumlar: Sistemin arızalı olduđu anlaşılamadan yanlış sonuç vermesi sađlanmaktadır. Sistemin sağlıklı işlemediđi zor anlaşılmaktadır. Karar verme sistemlerine yönelik olarak uygulanmaktadır.

- Simüle Edilmiş Savaş: Savaş ortamı oluşmadan taraflara ait bilgilerle savaşın bilgisayarda simüle edilerek oynanması ve sonucun rakip ülke aleyhine gelişeceği izlenimi verilmesidir.

Bilgi Harekatının spesifik hedeflerini örnekleyecek olursak;

- Milli ve Sivil Ekonomik Altyapı (Enerji ve Üretim Sistemleri)
- Milli Telekomünikasyon Sistemleri
- Silah Sistemleri
- Hava Trafik Kontrol Sistemleri
- Seyrüsefer Sistemleri
- Radarlar, Limanlar
- Ekonomik Altyapı Sistemleri (Bankacılık, Borsa)
- Mikro İşlemci Destekli Tıbbi Sistemler
- Medya

Bu hedeflerin ortak özelliği; bir ülkenin hayati öneme haiz yapılarını karıştırarak ve bozarak ülkenin yaşam standartlarını aniden düşürecek, halkın işini kaybetmesine sebep olacak, yiyecek, içecek, ulaşım düzenini aksatacak, para akımı ve halka sağlanan hizmetlerin aksamasına neden olacak ve sonuç olarak ülke yönetimine olan güveni sarsacak hedefler olmasıdır.

3.3. Bilgi Savaşının Özellikleri ve Araçları

Yapılan tanımların ışığında; Bilgi Savaşı yelpazesinin normal politik ve ekonomik rekabetten, krize; krizden, sıcak çatışmalara ve çatışmalardan , savaşlara kadar geniş bir alanı kapsamaktadır. Öyleyse bilgi savaşının birinci ve en belirgin özelliği zaman ve mekana tabi olmaksızın her yerde ve her zaman uygulanabilmesidir.

Bilgi savaşının diğer bir özelliği toplumun her kesimine yayılabilmesi; çatışma ve rekabet ortamı yaratabilmesidir. Bu anlamda askeri, ekonomik, politik, sosyal, ideolojik ve dini sorunları kendisine temel almaktadır.

Bilgi savaşı her seviyede uygulanabilir olma özelliğine sahiptir. Başka bir deyişle bilgi savaşı stratejik, operatif ve taktik seviyedeki hedeflere uygulanabilir.

Bilgi savaşı bağımsız olarak uygulanabileceği gibi, diğer savaş çeşitlerine yardımcı olarak beraber veya destekleyici olarak icra edilebilir. Gelişen teknolojiye paralel olarak bilgi savaşının çehresi de hızlı bir değişim içerisinde. Gelişen teknoloji bilgi savaşının metotlarını, tekniklerini ve hedeflerini de sürekli değiştirmektedir.

Bilgi savaşlarının stratejik seviyede denge sağlama özelliği vardır. Askeri mikrosensörler ve herşeyi bilen video ekranları pahalı olabilir. Ancak, bilgi sistemlerine saldırmak için ihtiyaç duyulan teknolojinin çoğu düşük maliyetlidir, yaygın olarak bulunabilir ve etkilidir. Alvin Toffler bilgi savaşının denge sağlayıcı özelliğine dikkati çekmektedir. Toffler;

"Bilgi savaşında ihtiyaç duyacağınız savaş tekniğini uygulayabilmek için büyük ve zengin olmanız gerekmez. İşte bu nedenle, fakir ülkeler, teknolojik olarak gelişmiş ülkelerden daha hızlı bir şekilde bilgi savaşını benimsemektedir" demektedir (Toffler, 1995, s. 121).

Bilgi savaşı hem saldırı hem de savunma amacıyla kullanılabilir. Hedefleri bireylerden organizasyonlara, ülkelerden uluslar arası kuruluşlara, devlet ve onun yapısal unsurlarına kadar yayılabilir.

Bilgi savaşı yöntemlerini iyi kullanabilen bir savunma anlayışıyla hem ülke içerisindeki hem de ülke dışındaki her türlü tehdit kriz veya çatışma ortamına gelmeden bertaraf edilebilir.

Bilgi savaşının uygulamalarının sonuçları hemen alınmaz. Sonuç biraz da karşı tarafın bilgi kullanımı hususundaki imkan ve kabiliyetine bağlıdır.

Bilgi savaşı gizli olarak yürütülen bir dizi faaliyeti kapsar. Bu yönüyle genellikle psikolojik hareketla iç içe aldatma ve propaganda tekniklerinin de yoğun olarak kullanıldığı bir ortam içerisinde sürdürülür. Toplum kesimlerinin eğitim seviyesi, gelişmişliği ve sosyal doku bilgi savaşının etkilerinin derecesini tayin edici unsurlardır. Memnuniyetsiz kitlelerin provakasyonu amaç olabilir.

Ülkenin iletişim alt yapısının gelişmişliği ve uluslararası sistemlere entegrasyonu, İnternet ve elektronik posta gibi iletişim imkanlarının bilgi savaşının araçları olarak kullanılmasına imkan verir. Klasik savaş araçlarından oldukça farklı

bir karaktere sahip olan Bilgi Savaşının araçlarına bakıldığında, genel olarak gruplanacak olursa;

- Tespit-Teşhis Sistemleri
- Uydular
- Aldatma ve Karıştırma Sistemleri
- Bilgi İletişim ve Bilgi İşlem Sistemleri
- Casuslar, Ajanlar
- Medya gibi halihazırda kullanılan ve farkına varabileceğimiz araçlardır.

Ancak yeni bir kavram olarak ortaya konan Soft Killing araçları özellikle sistemlerin bilgi güvenliğine yönelik en etkili araçlar olarak gündemdeki yerini almıştır. Bunlar aşağıdaki başlıklar altında sayılabilir:

3.3.1. Bilgisayar Virüsleri

Kendi kendini büyük programların içine kopyalayabilen program parçalarıdır. Bir virüs yalnız bulunduğu ana program çalıştırılınca aktif hale geçer ve görevini yapar. Bilgisayarların çökmesine, sabit disklerin silinerek tüm bilgilerin kaybolmasına neden olabilir. Virüsler, bilgisayarlardan çok dijital telefon ağı devreleri gibi bilgi işlem tabanlı sistemlerde etkin olarak kullanılabilir (Tatar, 2001, s.75).

3.3.2. Kurtlar

Bağımsız birer bilgisayar programıdır. Kendisini networkler üzerinde bilgisayardan bilgisayara kopyalayarak çoğalır. Networklerin çökmesine, bilgilerin kaybolmasına, bağlantıların kaybolmasına sebep olabilir (Tatar, 2001, s. 75).

3.3.3. Truva Atları

Programlar içine programın gerçek fonksiyonundan başka fonksiyonları gerçekleştirmesini sağlamak için koyulmuş program parçalarıdır. Bu tür program, özellikle network güvenlik programı gibi programlara yerleştirilerek, sistemin güvenlik açısından zayıf noktalarının programı yerleştiren kişilerin eline geçmesine sağlayabilir. Truva atı programları virüslerin ve kurtların gizlenmesinde de kullanılabilir (Tatar, 2001, s. 75-76).

3.3.4. Mantık Bombaları

Bir çeşit Truva atı programıdır. Esas amaçları önceden üretilmiş virüs, kurt gibi programları aktif hale getirmek için gerekli ikazı sağlar. Hemen hemen tüm dünyada yaygın olarak kullanılan network işletim sistemlerine üretici firma tarafından yerleştirilebilecek mantık bombaları aktif hale geldiklerinde söz konusu network işletim sisteminin kullanıldığı, banka ATM şebekesi, borsa bilgisayar ağı gibi sistemlerin çökmesine neden olacaktır (Tatar, 2001, s. 76).

3.3.5. Tuzak Kapılar

Arka Kapı olarak da adlandırılır. Üretici firmalar ve tasarımcı tarafından, sistemlere koyulabilecek mekanizmalardır. Bu mekanizmalar, tasarımcıya, kullanıcıya hissettirmeden sistemlere nüfuz etme ve sistemi kendi arzusu doğrultusunda kullanabilme imkanını verir (Tatar, 2001, s. 76).

3.3.6. Chipping

Yazılımlarda olduğu gibi, donanımların da, çok rahatlıkla kendinden beklenen fonksiyon haricinde son kullanıcısının bilmediği bir veya birden fazla fonksiyonu yapacak şekilde dizayn edilmesi mümkündür. Bunun için özel imal edilmiş mikroçipler, çeşitli amaçlar için, silah ve sistemlerde kullanılan kartlara monte edilebilir veya belirli bir fonksiyon için üretilmiş devrelere ilave fonksiyonlar kazandırabilir. Günümüzde entegre bir devre (chip) içinde 5 milyon transistörle yapılabilecek kadar çok büyük fonksiyonlu devreler dizayn etmek mümkündür. Kullanıcı bu fonksiyonlardan yalnız teknik kataloğunda belirtilen özellikleri kullanabilir ve bilebilir. Diğer fonksiyonların tespit edilmesi imkansız denecek kadar zordur. Entegre devrelerin kullanıldığı elektronik cihazlar, üretici firma tarafından kazandırılacak ilave fonksiyonlar bir sinyalle harekete geçirilebilir, entegre devrenin bulunduğu kart yanarak sistem devre dışı kalabilir (Tatar, 2001, s.76).

3.3.7. Nano-Mekanikler ve Mikroplar

Karıncadan küçük mekanik robotlar ve silisyum yiyen mikroplar, geleceğin Bilgi Savaşı silahları olarak düşünülmektedir (Tatar, 2001, s. 76).

3.3.8. High Energy Radio Frequency (HERF)

Bunların yanı sıra hard killing olarak adlandırdığımız HERF (High Energy Radio Frequency) topları ile Elektromanyetik Pals Bombası (EMP) bu araçların arasında sayılabilir. Belirli bir hedefe yüksek güçte yönlendirilmiş radyo sinyali göndererek hedefi elektronik olarak köreltebilen HERF silahlarının ABD ve Rusya'nın elinde olduğu bilinmektedir. HERF silahları herhangi bir elektronik sisteme veya bilgisayar sistemine karşı kullanılabilmekte, yüksek yoğunluklu elektromanyetik enerjiyi yönlendirilmiş olarak göndermekte ve o sistemde bulunan elektronik devreleri yakarak devre dışı bırakmaktadır. HERF topu bir minibüsün içine monte edilebilir ve telefon santralleri, televizyon verici istasyonları ya da bir bilgisayar network sistemi üzerindeki main server bilgisayarın üzerinde kullanılarak söz konusu sistemleri devre dışı bırakabilir.

EMP etkisi ise ilk kez nükleer silahların yüksek irtifa infilakında farkedilmiştir. EMP nano saniyelerle ifade edilen kısa zaman dilimlerinde, çok yoğun olarak ortaya çıkan ve geniş bir sahaya yayılan bir elektro manyetik şok dalgası olarak tanımlanabilir. Bu şok dalgasının meydana getirdiği güçlü manyetik alan, etki sahası içindeki elektronik devreler, kablolar ve her türlü iletken madde üzerinde kilo voltlar seviyesinde voltaj oluşturmaktadır. EMP etkisine maruz kalan bilgisayar sistemleri, iletişim vasıtaları ve bünyesinde elektronik devre bulunan her türlü cihaz hasar görecektir. Elektronik cihazların EMP etkisine karşı yalıtımları da oldukça zordur. İletişim araçlarının antenleri, radarlar, bilgisayar ağlarının kabloları ve modemlerin bağlı olduğu telefon hatları, EMP etkisini bağlı oldukları cihazlara, elektromanyetik olarak yalıtılmış olsalar dahi, taşıyacaklardır. Bilgi savaşı kapsamında kullanılan EMP bombası nükleer değildir ve elektromanyetik şok dalgasını meydana getirmek için, patlayıcı ile tahrik olan, bir elektromanyetik akı jeneratöründen istifade eder. Elektromanyetik akı jeneratörü, 10-20 mikro saniye içerisinde ön milyonlarca joule enerji üretir. Pik akımı tipik bir yıldırımın 1000 katıdır. Bir EMP bombasının etki sahasının artırılması, bombanın gücünün artırılmasına bağlıdır. Örnek olarak; 10 GW, 5 GHz'lik bir EMP bombası yüzlerce metre yükseklikten 400-500 metre çapında bir etki sahası meydana getirebilmektedir.

Mevcut durum itibariyle sadece ABD ve Rusya Federasyonunun elinde EMP bombası üretimi için gerekli teknoloji, alt yapı ve bilgi birikimi olduğu bilinmektedir.

Ancak EMP bombasının üretilmesi için, gerekli mühendislik çizimleri olduğu takdirde 1940'ların teknolojisi yeterlidir. Rusya Federasyonundaki iç istikrarsızlık da göz önüne alındığında, bu silahın, diğer ülkeler tarafından da üretilmesi söz konusu olabileceği değerlendirilmektedir (Hayden, 2001, s. 1-3).

3.3.9. Uzaktan Nöral Denetim

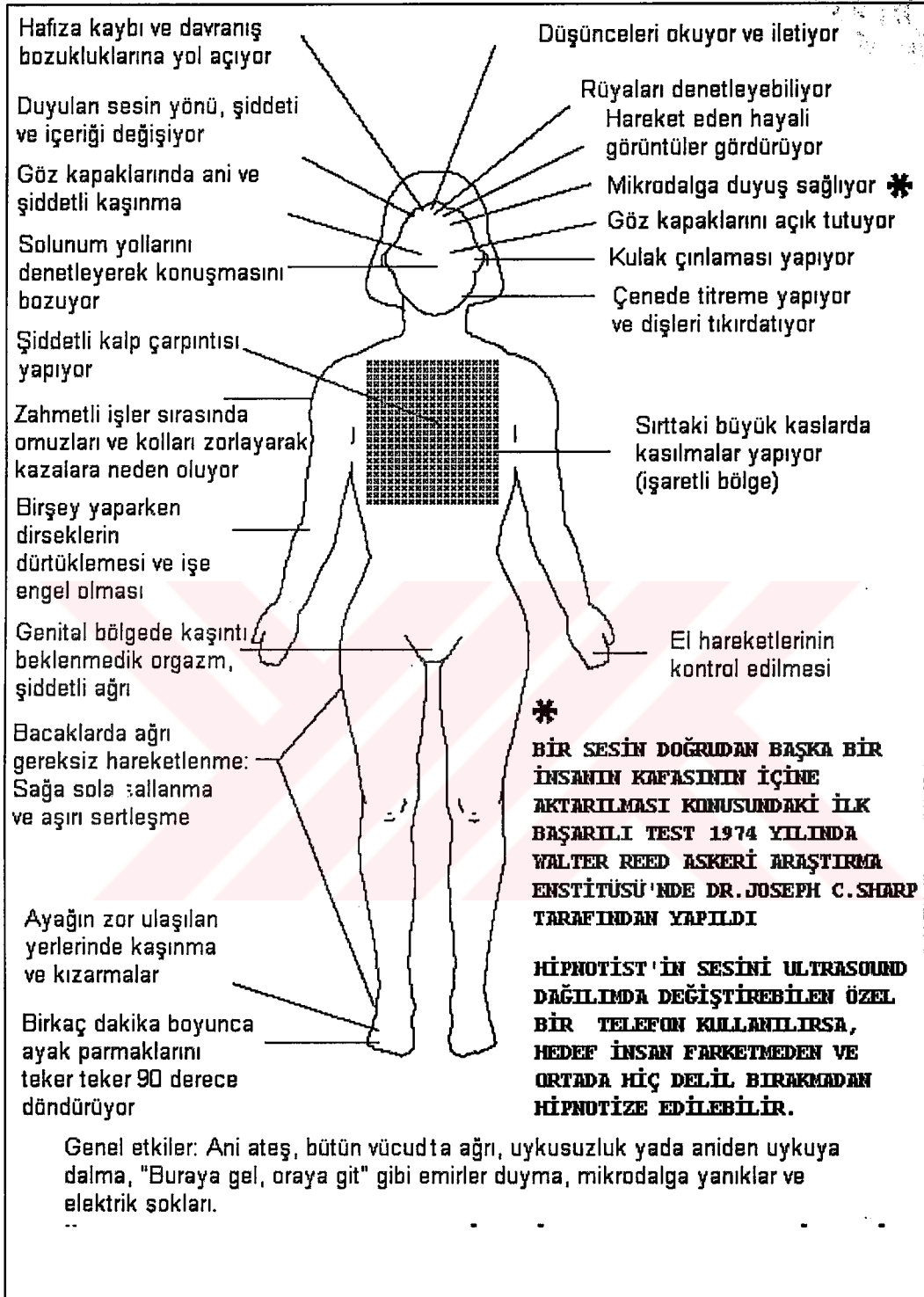
Hard killing silahların grubuna girebilecek bir diğer yöntem ise insan vücudu ve beyninin bilgisayar vasıtasıyla uzaktan kontrolüne yönelik Uzaktan Nöral Denetim projesidir. Amerikan Güvenlik Ajansının 1950'lerden beri üzerinde çalıştığı proje ışınım istihbaratı adı verilen; radyoaktifliği ve nükleer patlamaları içermeyen ve çevrede bulunan bir kaynaktan istemeyerek (kasıtlı olmayan bir şekilde) yayılan elektromanyetik dalgalardan oluşan bilginin elde edilerek insan beyninin uyarılmasını esas almaktadır. Amerikan Güvenlik Ajansı insandaki elektriksel faaliyetleri uzak mesafeden analiz eden özel elektronik donatıya sahiptir. Bilgisayarlarda üretilen beyin planlaması yoluyla, beyindeki elektriksel faaliyetleri sürekli olarak denetleme imkanı vardır. Oluşturulan bilgi tabanında binlerce insanın ferdi beyin haritaları kaydedilmekte ve şifrelenmektedir. Elektro manyetik alanla beynin uyarılması, beyin-bilgisayar bağlantısının sağlanması, askeri savaş uçaklarında ordu tarafından da gizlice kullanılmaktadır (Özkaya, 2002, s. 448)

Elektronik gözetim amacıyla, beynin konuşma merkezindeki elektrik faaliyetleri, hedefin sözlü düşüncelerine çevrilebilir. Kulağı devre dışı bırakarak, ses haberleşmesinin doğrudan beyne gitmesini sağlayarak, şifrelenmiş işaretleri, beynin işitme korteksine gönderebilir. Bu işaretler, paranoid şizofreninin karakteristiği olan işitsel halüsinasyonları taklit ederek, hedef kişinin gizli olarak fiziksel ve beyinsel gücünü azaltmak için kullanabilirler. Hedefle herhangi bir temas olmaksızın, Uzaktan Nöral Denetim, bir kişinin beynindeki görsel korteksteki elektrik faaliyetlerini planlayabilir ve kurbanın beynindeki tasvirleri (görüntüleri) bir videonun monitöründe gösterebilir. Hedefin gözlerinin gördüğü her şeyi bu yolla görmek mümkündür. Görsel hafıza da görülebilir. Uzaktan Nöral Denetim gözleri ve optik sinirleri atlayarak (devre dışı bırakarak), doğrudan görsel kortekse görüntü gönderebilir. Beynin programlama gayesi için, gözetim altındaki kişi REM uykusunda iken, onun beynine gizlice görüntü yerleştirmek için bu yöntem kullanılabilir.

Kişileri izlemek ve bunların beyinlerindeki işitsel-görsel bilgileri fiziksel temas olmadan denetlemek için kullanılan Uzaktan Nöral Denetim sistemi, gözetim ve yurt içi istihbarat için kullanılmaktadır. Bu işlerin tümü, kişiyle fizikî bir temas olmadan yapılır. Uzaktan Nöral Denetim metodu, konuşma, üç boyutlu ses ve şuuraltı ses, kişinin beyninin işitme korteksine (kulaklar by pass edilerek) gönderilebilir ve görüntüler görsel korteksin içine gönderilebilir. Bu metotla hedef kişinin algıları, ruh durumu ve motor kontrolü değiştirilebilir (Bkz. Şekil 3.1.).

Uzaktan Nöral Denetim, görsel-işitsel beyin ile beyin arasında veya beyin ile bilgisayar arasında tam bir bağlantı sağlayabilir (Özkaya, 2002, s. 448).





Şekil 3.1.:NÖROMANYETİK SİLAHLARIN ETKİLERİ
(Özkaya, 2002, s. 448)



3.4. Bilgi Savaşının Yöntemleri

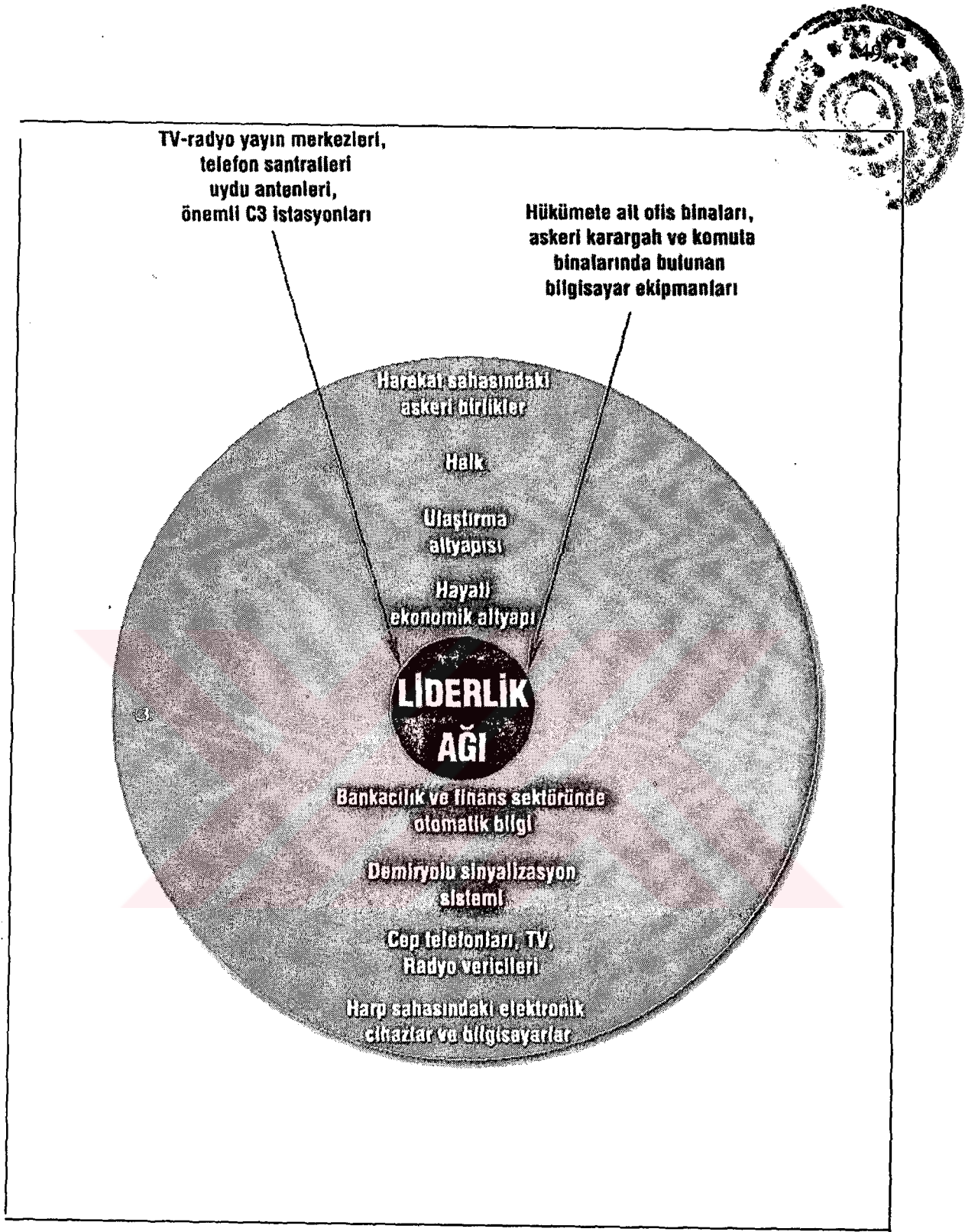
3.4.1. Warden Modeli

ABD Hava Kuvvetlerinde görevli Albay J.A. Warden tarafından tasarlanan ve elektromanyetik silahların stratejik hedeflere yöneltildiği, bir hava savaşı modeli mevcuttur. Bu modelde düşman ülkenin stratejik hedef listesi; liderlik ve liderliği destekleyen komuta kontrol sistemi, hayati önem taşıyan ekonomik altyapısı, ulaştırma ağı, halkı ve savaş alanındaki askeri kuvvetleri olarak önem sırasına göre beş ana bölüme ayrılmıştır (Bkz. Şekil 3.2.). Bu hedefler içten dışa doğru halkalar şeklinde ifade edilmiştir (Tatar, 2001, s. 76).

En içte yer alan birinci halkada yer alan liderlik ve liderliği destekleyen komuta kontrol sistemi içerisinde o ülkenin savaş mekanizmasını harekete geçirme ve savaşı sürdürme imkan kabiliyetine sahip olan hükümet merkezi, askeri karargahlar gibi karar verme mekanizmalarıyla, karar vericilerin milli gücün diğer unsurlarıyla irtibatını sağlayan telefon, bilgisayar ağları, televizyon yayıncılığı gibi iletişim unsurları yer almaktadır.

İkinci halkada yer alan düşman ülkenin hayati önem taşıyan ekonomik altyapısının tespiti her ülkenin özelliğine göre değişmektedir. Ancak özellikle yüksek seviyede otomasyon uygulanan, elektronik ve bilgisayar kullanımının yoğun olduğu borsa, bankacılık sistemi gibi finansal yapılar; enerji üretim, dağıtım ve kontrol şebekeleri ile üretim tekniğinde otomasyon gerektiren petro-kimya, metal işleme tesisleri oluşturulacak hedef listesinde öncelikli hedefler olarak değerlendirilmektedir. Bu listenin önceden yapılacak bir tespit ile hazırlanması önerilmektedir.

Ulaştırma hizmetleri kapsamında bilgi savaşlarının hedefleri; hava kontrol sistemleri ve demiryolu sinyalizasyon sistemi gibi bilgisayarlarca kontrol edilen sistemler olacaktır.



Şekil 3.2.: 5 HALKALI WARDEN MODELİ
(Tatar, 2001, s. 76).

Warden modelinde düşman ülkenin halkı da bilgi savaşlarının hedefidir. Özellikle medyanın kullandığı yayıncılık modelleri ve haberleşme vasıtaları ile psikolojik hareket tekniklerinin de kullanılarak halkın moral ve motivasyonu üzerinde yıpratıcı ve yıkıcı bir etki yaratılması amaçlanmaktadır.

Son halkada yer alan savaş alanına sevk edilen askeri birliklerin ise özellikle taktik haberleşme ve komuta kontrol sistemlerinin etkisiz hale getirilmesi, radar ve diğer hedef tesbit vasıtalarının körleştirilmesi, silah ve mermi güdüm sistemlerinin aldatılması ve yanlış yönlendirilmesi yoluyla pasifize edilmesi öngörülmektedir.

Elektromanyetik silahların Warden modeline uygun olarak aynı anda veya kademeli olarak düşman ülkeye karşı kullanılması; daha ilk aşamada yüksek tempolu bir savaşın çok fazla can kaybına neden olmadan icrasına imkan vererek dünya kamuoyunda doğacak tepkileri engelleyecektir. Kuvvet tasarrufu sağlayacaktır. Her şeyden önemlisi stratejik felç adını verdiğimiz bir etki ile düşman ülkenin savaşma imkan kabiliyetini önemli ölçüde etkileyecektir. Bilgi savaşı bu yöntemle kademeli olarak kullanıldığında (strategy of graduated response) deniz veya hava ablukasına gibi bir yaptırım aracı olarak kullanılabilecektir. Düşman ülkenin yaptırımlara verdiği tepki doğrultusunda bilgi savaşının hedefleri dereceli olarak etkisiz hale getirilmektedir. Bu yöntemle krizlerin sıcak çatışma veya savaş ortamına gelinmeden çözülmesi mümkün olacaktır.

3.4.2. Sayısal Bilgi Harekatı

Sayısal Bilgi Harbi (Digital Information Warfare-DIW); sivil, askeri, politik, ekonomik ya da kişisel amaçlarla bir bilgi sistemine (bu sistem çok geniş bir bilgisayar ağı olabileceği gibi herhangi birine ait kişisel bilgisayarlarda olabilir) kullanıcının haberi olmadan zararlı bilgisayar yazılımı (malicious code) sokulması işlemidir. Gizli olarak uygulanan bir faaliyettir (Ünal, 2000, s. 36). Uluslar arası konjüktürün açık bir mücadeleyi uygulamak için uygun olmaması durumunda üstü örtülü olarak yapılabilir. Kapsamı kolaylıkla kontrol edilebilir. Belirli hedeflere yöneltilebilir. Hedef, bir ülkenin tüm ekonomik altyapısı olabileceği gibi, spesifik bir bilgisayar sistemi de olabilir. Günümüzde teknik olarak uygulanma durumu mümkündür. Aşağıdaki amaçlara ulaşmak maksadıyla kullanılabilir:

3.4.2.1. Devre Dışı Bırakma

Adından da anlaşılacağı gibi, hedef alınan bilgi sistemin yazılım veya donanım olarak kullanım dışı bırakılmasıdır. Bu tip bir saldırı hedef bilgi sistemine çoğunlukla zararsız görülen, paylaşımına açık bilgisayar yazılımları ile bulaştırılırlar. Hasar verici zararlı bilgisayar yazılımı kullanılır. Bir virüs kullanılarak, işlemcinin çalışma frekansının artırıp limitlerin dışında daha hızlı çalışması sağlanarak aşırı ısınmasına ve yanmasına sebep olunabilir. Dolayısıyla donanımın tamamen ya da kısmen arızalanması da sağlanabilir (Ünal, 2000, s. 36).

4.4.2.2. Zayıflatma

Hedef alınan sistemin yapmakta olduğu işlevlerini gereği gibi yapamaz hale getirilmesi işlemidir. Hedef alınan sistemin işlevini gereği gibi yapamaz hale getirilmesi maksadıyla kullanılır. Kullanıcıya hissettirilmeksizin kullanılan bilgi sisteminin çalışma performansının düşürülmesini kapsar. Dolayısıyla normal şartlarda anında ulaşılabilecek bilgilere belli bir zaman kaybı meticesinde ulaşılabilecek; bilgi sisteminin zayıflatılması sağlanacaktır. Böyle bir saldırının gerçekleştirilmesi halinde ilk önce bilgi sisteminin donanımı kontrol edileceğinden dolayı ya da sistem yazılımının yeniden kurulması gerekeceğinden dolayı bilgi sistemi etkinlikle kullanılamayacaktır (Ünal, 2000, s. 36). İnternet yoluyla bilgisayardan bilgisayara kopyalanarak çoğalan bir yazılım bilgisayarları belirli bir süre ile kilitlenmesine sebebiyet verebilir.

3.4.2.3. Aldatma

Hedef alınan sistemin, farkında olmadan yanlış bilgi üretmesi ve ürettiği bu bilgiyi doğruymuş gibi işleme sokması durumudur. Bu şekilde saldırıya uğrayan bilgi sisteminin borsaya bağlı şirketlere, bankalara, bir ülkenin radar kaplama sahasına, ulaşım faaliyetlerini denetleme ağına ya da sağlık kuruluşlarında bulunan hasta kayıtlarına bağlı olabileceğini düşündüğümüzde böyle bir saldırı sonrasında olabilecek tek şeyin kaos olduğunu görebiliriz. Askeri alanda da kullanılabilir. Örneğin bir füzenin radar ekranında gerçekte var olmayan ekoları algılayarak yanlış hedefe yönlendirilmesi sağlanabilir. Aldatma tekniğinin diğer bir etkisi de ortaya

çıkan kaos ortamında bile herşeyin normal olduğunun sanılarak hazırlıksız yakalanılması durumudur (Ünal, 2000, s. 36).

3.4.2.4. İstismar Etme

Hedef alınan sistemden gizlice bilgi sızdırılması durumunu ifade eder.

Sayısal bilgi hareketi stratejik, operatif ve taktik seviyelerde uygulanabilir. Sayısal bilgi hareketine başvurabilecek kişi, kuruluş ya da örgütler genellikle belirli aşamaları uygulamaktadır (Ünal, 2000, s. 37).

Kullanmak istediğimiz bilgi savaşı aracının, en zayıf noktasından sisteme sokulması aşaması sızma aşamasıdır. Bu safhada nüfuz noktası ve nüfuz yöntemi önem kazanmaktadır. Sistemin en zayıf noktasının tespiti gereklidir. Araç; sisteme en zayıf noktasından ya direkt olarak ya da çevre birimleri vasıtasıyla sızdırılır. Nüfuz yönteminde iki teknik kullanılmaktadır:

Araç; sisteme dizayn amacına uygun bir yapıda sızdırılmasına ön kapı tekniği denir. Sisteme daha üretim aşamasındayken nüfuz edilebilir. ABD Savunma Bakanlığının ABD tarafından üretilen bazı silahların kontrol sistemlerine yerleştirilmek üzere kodlu bir radyo sinyali ile aktive olabilecek virüsler üzerinde çalıştığı bilinmektedir. Bir disket veya CD rom ile sisteme zararlı yazılım sokulması da sisteme uygun araçlarla giriş yapıldığı için ön kapı tekniği kapsamında değerlendirilir.

Arka kapı tekniği aracın; sistemde dizayn amacı dışında bir etki ile girmesidir. Yüksek enerjili radyo frekansı veya kontrollü elektro manyetik palslar bu maksatlarla kullanılabilir.

Sisteme sokulan aracın, sistem içerisindeki hedefine ulaşmaya kadar izlediği safhaları yayılma safhasını ifade eder. Hedef çoğu zaman sistem içindeki bir server bilgisayar ya da ağ düğüm noktası olabilir.

Sisteme sokulan araç, ya zaman ayarlı olarak ya da ikaz alınmaya kadar pasif durumda beklemeye geçer. Bu safha bekleme safhasıdır.

Aracın tetiklenerek, aktif hale getirilmesi ve amacına uygun olarak fonksiyonunu yerine getirmesi aktif hale geçme durumudur. Araç; zaman ayarlı olarak veya ikaz ile yukarıda açıklanan devre dışı bırakma, zayıflatma, istismar etme gibi amaçların elde edilmesi için harekete geçer. Bazen araçlar direkt olarak sisteme nüfuz eder etmez faaliyete geçebilir. Örneğin dijital telefon ağları için geliştirilmiş bir yazılım sisteme girmesiyle birlikte kendi kendisini kopyalayarak çoğalır ve sistemi aşırı yükleyerek çökmesine sebebiyet verir.

Amacın elde edilmesini müteakip, sonuç safhasında, araç tekrar pasif konumuna dönebilir ya da hiçbir iz bırakmaksızın kendi kendisini sistemden siler. Bu durumlarda saldırının kim tarafından ne şekilde yapıldığı anlaşılmaz hale gelir. Eğer sistemden istismar etme yöntemiyle bir takım bilgiler elde edildiyse durumun farkına dahi varılmayabilir. Saldırı sonrası saldırının yapıldığına dair bir iz bırakılmışsa da sistem tüm güvenilirliğini yitirir ve yenilenmesi gerekebilir.

Sayısal bilgi hareketinden korunmak oldukça zordur. Bilgiyi elde etmek için açık sistemlerden de faydalanmak zorunluluğu, kendi bilgi sistemimizin hassasiyetini arttırmakta ve yetkisiz girişlere sebep olmaktadır. Alınacak her türlü korunma yöntemine karşı değişik tür ve sayıda saldırı tekniği kullanılabilir. Ancak kapalı bir sistemde bilgi edinmenin getireceği dezavantajlar da değerlendirilerek alınacak birkaç savunma yöntemiyle en azından mevcut risklerin asgari düzeye indirilmesi sağlanabilir.

Aşağıda sayılan savunma yöntemlerinin uygulanabilir olduğu düşünülmektedir (Ünal, 2000, s. 37):

- Sayısal bilgi hareketi yazılımlarının bilgi sistemimize girmelerini önleyecek olan; korsan yazılımların kullanılmaması, önemli bilgiler içeren bilgi sistemlerinin çoklu erişim ortamlarına girmelerinin önlenmesi, kayanağı bilinmeyen yazılımların kullanılmaması gibi tedbirlerin sürekli olarak uygulanması.

- Eğer bilgi sistemimize girmiş olduğu tespit edilen ya da girdiğini sandığı sanılan bilgi hareketi yazılımının, belli tarayıcı programlar kullanılmak suretiyle tespit edilerek sistemden silinmesinin sağlanması.

- Sayısal bilgi hareketi saldırısına uğrayan bilgi sisteminin yeniden formatlanmak suretiyle tekrar eski durumuna döndürülmesi.

- Eğer formatlama ile de bir sonuca varılamıyor ise, devre dışı kalan bilgi sisteminin yerine yeni bir bilgi sisteminin kurulması .

3.4.3. Stratejik Felç

Stratejik felç, teknolojinin getirdiği imkanlar sayesinde minimum hasar ve sivil halk kaybı ile düşmanın savaşma azim ve iradesine direkt etki eden stratejik ve ekonomik hedeflere taarruz edilerek, düşmanın teslim olmaktan başka hiçbir çıkar yolunun kalmaması durumudur (Kahya, 1999, s. 49).

Warden modeliyle ilişkilendirilen stratejik felcin amacı bir ülkeye yönelebilecek düşman tehditlerini muhasım ülkenin stratejik hedeflerine yapılacak teknoloji yoğun bir hareketle etkisiz hale getirerek bertaraf edilmesidir. Burada hedef spesifikasyonu önem kazanmaktadır. Hedefler genellikle düşman ülkenin milli gücünü oluşturan ve kaybı halinde o ülkenin toplam milli gücünü etkileyecek türdendir. Belirgin bir hedefin seçilmesi ve iyi bir zamanlama ile diğer hedeflerinde etki altına alınması amaçlanır. Biz bu hedefleri Milli Değer Parametreleri (National Elements of Value – NEV) olarak adlandırıyoruz (Kahya, 1999, s. 49).

Savaşın zamanı ve hedeflerin birbirlerini etkileme derecesi de hedef seçiminde diğer önemli faktörler olarak öne çıkmaktadır. Stratejik felce giden yol dereceli bir tepkidir (graduated response). Yıpratma hareketinden, bütünüyle imhaya kadar olan aşamaların o ülkenin sosyal, politik, ekonomik ve askeri gücüne etkileri de dereceli olmaktadır. Düşman tehdidi kimi zaman sıcak çatışma ortamına gelinmeden engellenmektedir. Bir tehdidin en az maliyetle, silahlı güçleri devreye sokmadan veya bir kısmının devreye sokularak bertaraf edilmesi; stratejik felç yaklaşımını benimseyen ülkeye kaynak tasarrufu sağladığı gibi inisiyatif de eline geçirmesine imkan tanımaktadır. Tanımdan da anlaşılacağı üzere stratejik felç stratejisinin vasıtalarını teknoloji yoğun silahlar oluşturmaktadır. Genellikle hava kuvvetlerini esas alan ve gelişmiş hedef tesbit vasıtaları, hassas güdümlü füzeler, uydular, görünmezlik teknolojileriyle desteklenen silah sistemleri stratejik felce giden yolda kullanılan vasıtalarlardır.

İkinci Dünya Savaşında Almanların ve Japonların stratejik felç yaratmaya yönelik hareketleri olmuştur. Almanların Norveç'e yaptığı hava indirme hareketi ile Norveç hükümetini etkisiz kılarak yerine kendisine dost bir yönetimi getirmesi,

Norveç'in siyasi karar alma mekanizmalarını devre dışı bırakmıştır. Japonların meşhur Pearl Harbour baskınının maksadı stratejik üstünlüğe giden yol denizlerden geçer fikrinden hareketle ABD'nin Pasifik donanmasını etkisiz hale getirip; ABD'nin sadece bir kara ülkesi konumunda kalmasını sağlamaktı. Nitekim müttefikler de aynı yöntemle karşılık vermiştir: Berlin Almanya için her şey demektir. Alman savaş gücünün sembolüydü. Berlin düşürüldü ve savaş sona erdi. ABD'nin Körfez hareketinde özellikle Irak ordusunun Cumhuriyet Muhafızları adı verilen seçkin birliklerini hedef olarak seçmesi aslında sadece askeri anlamda bir hedef listesinin gereği değildi. Cumhuriyet Muhafızları savaşmayı bıraktığında Irak ordusu yenilgiyi kabul etmişti. Aşırı merkezîyetçi bir organizasyon yapısı olan Taliban için Molla Ömer ve Usame Bin Laden ne ise kapitalizm için Dünya Ticaret Merkezinin ikiz kuleleri de odur. Burada dikkat çekici olan ise hedeflerin her ülkeye göre anlam ve öneminin farklılıklar göstermesidir. Diğer bir husus; bir hedefe yöneltilen taarruzun topyekün bir mücadelenin başlatıldığına dair olan işaretidir. Warden modelindeki beş halkanın her biri teorik olarak birbiriyle ilişkilidir ve stratejik felcin hedef listesini oluşturmaktadır. Bilgi savaşı silahlarının geleceğin savaşlarında stratejik felç maksadıyla kullanılması hem düşmanı gizleyecek hem de önemli oranda kaynak tasarrufu sağlayacaktır. Stratejik felcin tanımında da yer aldığı gibi rakip ülkeye teslim olmaktan başka çıkar yol kalmayacaktır.

3.4.4. Dünyanın Gözleri ve Kulakları (ECHELON)

Elektronik istihbarat dünyasının en gizli ve en çok konuşulan sistemi Echolon sistemidir. Bu sistem, edinilen bilgilere göre Amerika, İngiltere, Kanada, Avustralya ve Yeni Zelanda arasında kurulmuş bir sistemdir. Sistem, dünya çevresinde beş ana stratejik uydu kullanılmaktadır. Bu uyduların her birinin yeryüzü üzerinde bir ana üssü yani istasyonu bulunmaktadır. Ayrıca sistem 100'ün üzerinde irili ufaklı uyduyu da kullanmakta ve yönlendirmektedir. Bu uydular eliyle sistemin dinlemediği, görmediği, izlemediği pek bir şey bulunmamaktadır. İletişim imkanlarının hemen hemen neredeyse tamamını tarayabiliyor ve kontrol altında tutabiliyor, telefon, cep telefonu, e-mailler, faks, tele-faks, bilgisayar ve hatta okyanusun altından geçen iletişim hatlarının tamamı izlenebiliyor.

Echelon dakikada 2 milyon, günde ise tam 3 milyar telefon görüşmesini izliyor ve dinliyor. Üstelik bu rakamlar 1998 yılını içermektedir. Sistem bu işlemi yaparken

sadece kayıt etmekle kalmıyor bir yandan da konuşmanın yapıldığı çıkış noktasını tespit etmeye çalışıyor. Dünya üzerindeki coğrafi koordinatlarını ele geçirinceye kadar sistem işletiliyor. Böylece evinizin posta adresi şekilleniyor. İçinde Türkiye'nin de bulunduğu birçok ülkede yerleştirilen radyo antenleri sayesinde uydudan yapılan iletişimi takip eden sistem birçok yöntemle bilgiler toplamaktadır. Bunların başında anahtar sözcükler gelmektedir. Bu anahtar sözcükler sayesinde iletişim kaydedilmekte ve bilgi isteyen ülkeye verilmektedir. Anahtar sözcük olarak şahıs ve yer isimleri de kullanılmaktadır. Bu sistem sayesinde birçok ülkenin en hassas gizli bilgilerinin diğer ülkelerin özellikle ABD'nin eline geçmesi büyük olasılıktır. Bilgi savaşlarının başladığı değişen dünya şartlarında gizli bilgilerin dost bile olsa başka ülkelerin eline geçmesinin riski, bugün Afganistan'da Taliban'ın ABD uçaklarına yine ABD füzeleriyle (dost olduğu dönemde verdiği) karşılık vermesi ile çok iyi anlaşılmaktadır. Eğer bu sistem söylendiği gibi askeri değil de sadece özel iletişimi takip ediyorsa bu durumda da özel yaşamın dokunulmazlığı veya şirketlerin telefonlarının dinlenmesi ile teknoloji casusluğuna kadar gidebilecek amaçlar ile kullanılıyor olabilir. Nitekim İngiliz İstihbarat Örgütü MI5, İngiliz şirketlerinin uluslararası yatırımları için bilgi toplayabileceği ve bu şirketlerin ortakları ve muhtemel ortakları hakkında bilgi verebileceğini toplantıya çağırdığı 64 büyük İngiliz şirketinin yöneticilerine belirtmiştir (EU Report on the Existence of Echolon, 2001, s. 194).

3.4.5. Çift Kullanımlı Teknolojiler (GPS)

Hem sivil, hem de askeri uygulama potansiyeli ve jenerik tabanı olan ve bazılarında daha geniş bir uygulama alanı bulunan teknolojiler; "Çift Kullanımlı Teknolojiler" olarak adlandırılmaktadır. Genellikle savunma sanayinde başlayan ve daha sonra sivil sektörlerde de kullanım alanı bulabilen teknolojiler; ülkelerin de bilim teknoloji seviyesinin yükseltilmesine katkıda bulunmaktadır. 1970'li yıllarda ABD Ordusu tarafından sivil üniversitelerde geliştirilen İnternet projesi, kısa sürede sivil sektöre yansımış ve bugünün vazgeçilmezi haline gelmiştir. Bu gelişme, askeri amaçla üretilen bir teknolojinin sivil sektöre transferine iyi bir örnektir. (Ayhan, 2002, s. 232)

1970'li yıllarda ABD Savunma Bakanlığı tarafından uzayda 20 200 kilometre yükseklikte altı farklı yörüngeye oturtulan 24 uydudan oluşan uzay bazlı konum

belirleme sistemi; Küresel Konumlama Sistemi (Global Positioning System-GPS)” olarak isimlendirilmiştir.Sistem; ABD Savunma Bakanlığı mülkiyetinde bulunmasına rağmen, tüm dünyanın kullanımına açıktır. Sistemin en önemli özelliği; herhangi bir zamanda, her türlü hava şartlarında, gece ve gündüz bulunulan noktanın konumunu belirleyebilmektedir. Hata payının son derece düşük olduğu bu sistemin haritacılık uygulamalarında hata payı, birkaç santimetreye kadar düşmektedir. Elektronik ve bilgisayar teknolojilerinin tabanında gelişen GPS teknolojileri, 1990’lı yıllarda ABD tarafından Körfez Savaşı sırasında çok etkin ve yaygın biçimde kullanılmıştır. Askeri alandaki GPS uygulamaları;

- Acil Durum Müdahaleleri,
- Akıllı Füzelere Yönlendirilmesi,
- Askeri Birliklerin Durumlarının Belirlenmesi,
- Düşman Kuvvetlerinin İzlenmesi,
- Kıtalar arası Füzelere Eşzamanlı Yönlendirilmesi,
- Uzaydan Kıtalar arası Balistik Füzelere İmhası,
- Helikopterle Mayın Koordinatlarının Tespiti olarak sayılabilir.

Askeri amaçla geliştirilmiş olsa da GPS uygulamalarının sivil sektörde uygulamaları daha yaygındır. Özellikle tarım, belediyeçilik ve lojistik alanlarındaki uygulamalar dikkat çekicidir. Ancak; teknolojinin ana kaynağı olan uyduların, ABD’ne ait olması zaman zaman tek taraflı kısıtlamaları da beraberinde getirmektedir. ABD’nin askeri amaçla kullandığı sinyallere diğer ülkeler ulaşmamaktadır. Bilgi Savaşının en etkili silahlarından birisi olan GPS teknolojisi, diğer ülkelerin coğrafi istihbarat bilgilerinin elde edilmesine yönelik olarak kullanılabildiği gibi; bu teknolojiye bağımlı olanların körleştirilmesi maksadına yönelik olarak kullanılabilir (Ayhan, 2002, s. 233,234).

4. TÜRKİYE’NİN BİLGİ SAVAŞINA YÖNELİK KONSEPTİNİN BELİRLENMESİ

Konsept, geleceğin tasarımıdır. Geleceğe yönelik faaliyetlerle ilgili olan ancak kesinlik taşımayan, olması muhtemel hususları içeren bir düşünceler bütünüdür. Konsept, değerlendirmenin yapıldığı alanda “Ne özelliklere sahip olacak? Nasıl yapılacaktır?” sorularına mantıklı bir değerlendirme yapılarak cevap verilmesi sürecidir. Konsept bu anlamda yaşayan düşünceleri ifade eder. Dinamik ve değişebilen düşüncelerdir. Değerlendirme sürecinde konsepti etkileyen faktörlerde meydana gelebilecek değişimler, konseptin güncelleştirilmesini zorunlu kılar. Konseptte etki eden faktörler netleştikçe, varsayımlar gerçeğe dönüştükçe konseptler uygulamaya dökülür ve doktrin haline gelirler (Özkil, 1999, s. 21).

Konseptler bir fikirler grubu olarak algılanmalıdır. Konseptler orta vadede (15-20 yıl) içerisinde gerçekleştirilmesi düşünülen temel faaliyetleri açıklayan fikirlerdir. Yol göstericidir. Zaman periyotlarına göre, birkaç defa konsept belirlenebilir veya mevcut konseptlerde değişiklikler yapılabilir (Bütün, 2000, s. 58). Türkiye’nin bilgi savaşına nasıl hazırlanacağına yönelik olarak ifade edilecek konseptte; elde edilecek teknolojik imkan ve yetenekler, bunların temin metodları, eğitim gereksinimi, kurumsallaşma gibi alt başlıkların nasıl sorusuna da cevap verecek şekilde ifade edilmesi önem taşımaktadır.

Bu kapsamda ortaya konacak bilgi savaşı konseptinde; Türkiye’nin gelecekte uygulayacağı veya maruz kalacağı bir bilgi savaşına yönelik nasıl bir yapılanma içerisine girmesi gerektiği sorusuna cevap aranacaktır. Bir konseptin belirlenebilmesi için öncelikle konsepti etkileyen faktörlerin teker teker ele alınıp değerlendirilmesi gerekmektedir. Türkiye’nin bilgi savaşına yönelik konseptini belirlerken bu faktörleri aşağıdaki başlıklar altında inceyip, değerlendireceğiz:

- Ekonomik, Politik, Sosyal ve Kültürel Yapıda Gelişmeler
- Jeopolitik Değerlendirme
- Türkiye’nin Savunma Stratejisinde Değişiklikler
- Türkiye’nin Bilim ve Teknoloji Politikaları
- Dünya Devletlerinin Bilgi Savaşı Potansiyeli
- Türkiye’de Bilgi Savaşı Konusunda Mevcut Durum

4.1. Ekonomik, Politik, Sosyal ve Kültürel Yapıda Gelişmeler

Yirmi birinci yüzyılın ilk yarısında yirminci yüzyılın son çeyreğinde başlayan teknolojik gelişimin devam ederek özellikle bilgisayar ve mikro elektronik alanındaki gelişmelerin hızlanacağı beklenmektedir. Mikro elektronikteki gelişmelerle bu alanda kullanılan malzemelerin hız ve güvenilirliklerinin artacağı maliyetlerinin düşeceği; dolayısıyla bu malzemelerin kullanım alanlarının genişleyeceği öngörülmektedir. Gelecekte beklenen enerji sıkıntısının ise elektronik bilgisayarların yerini optik bilgisayarların almasıyla çözüleceği tasarlanmaktadır. Elektronların yerine fotonların denetimine dayalı optik bilgisayarlar, bilgisayar teknolojisinin zaman ve mekan boyutunu genişleterek uzayı da kapsayan bir donanım yapısına ulaşacaktır. Elektronikte ışığın kullanılması optoelektronığı yaratacaktır. Optoelektronik bilgisayarlarla, mikroskobik lazer ışığı içeren yongalar kullanılacaktır. İnce kablolar yerini süper hızlı fotonlara bırakacaktır. Fotonlar en küçük ışık enerji birimleri olup, ışık hızıyla hareket ederler. Lazer ışıklı yongaya sahip bilgisayarlar üretildiğinde, bilgisayar hafızaları aşırı boyutta hızlanacak ve bilgi aktarımı damlacıklardan kitlevi duruma dönecektir (Erkan, 1998, s. 88-89).

Teknolojik gelişmenin diğer bir boyutu ise yapay zeka olacaktır. Yapay zekaya sahip bilgisayarlar akıllı robotların evriminin başlangıcı olacaktır. İnsan gibi düşünebilen ve işlem yapabilen robotların bir sonraki aşaması ise biyocomputerlerdir. Biyoteknoloji alanındaki gelişmeler robot teknolojisine etki edecek ve organik chipler gündeme gelecektir. Bu sayede bir yandan akıllı bilgisayarlar yapılırken, diğer yandan insan beyninin ve vücudunun da bilgisayarlar gibi belli koşullarda kontrol edilebilme imkanı ortaya çıkacaktır. Örneğin; İnsan beynine yerleştirilecek bir chip ile bir yabancı dile ait konuşma ve anlama yeteneği geliştirilecektir (Erkan, 1998, s.90).

Ulaştırma vasıtalarında bu yeni teknolojilerden yararlanacak, daha hızlı daha az enerji harcayan araçlar geliştirilecek, bunun yanı sıra bu araçlar elektronik kontrol sistemleri ile donatılacak ve insan kontrolundan rota kontroluna geçilecektir (Erkan, 1998, s. 90).

Gelecekte dünyada teknoloji alanında bu gelişmeler yaşanırken Türkiye nerede olacaktır sorusunun cevabını verebilmek için öncelikle şu anda neredeyiz sorusunun cevabını vermek gerekir.

Sistem bütünlüğü içerisinde bilgi toplumuna geçişi dört ana alt sistemin değerlendirmesini yaparak incelemek gereklidir. Bunlar;

- Ekonomik alan,
- Sosyal alan,
- Politik alan
- Kültürel alanlardır.

Bilgi toplumuna geçiş birdenbire olmayacaktır. Belirli aşamaların geçirilerek; bir alt sistemde meydana gelen değişimin kurumsallaşması ve devamında diğer üç alt sistemi etkileyerek dönüşümü (transformation) gerçekleşmesi gerekmektedir. 1980'lerde dışa açılmayı başarabilen Türkiye'de diğer üç alt sistemi belirgin olarak etkileyebilecek alt sistem ekonomidir. Ekonomik alandaki değişimlerin diğer alt sistemleri de sırasıyla dönüşüme zorladığı görülmüştür (Erkan, 1998, s.92-93).

Dünya Bankasının raporlarında Türkiye için ekonomik olarak bilgi toplumuna doğru giden yolda üç safha belirlenmiştir:

- Geçiş Halinde Endüstriyel Ekonomi: Bankacılık, uluslararası ticaret, vergilendirme gibi bilgi yoğun sektörlerin bilgi işlem sistemlerinden yararlandığı ekonomiler,
- Sınırlı Bilişim Ekonomisi: Bilgi tabanlı sistemlerin ekonomilerde verim arttırmak maksadıyla tasarım, üretim, pazarlama gibi teknolojik rekabet üstünlüğü sağlayabilecek alanlarda kullanıldığı ekonomiler,
- Bilişim Tabanlı Ekonomi: Kamu ve özel sektörün bilgi tabanlı olarak örgütlendiği ekonomiler.

Bu tasnifte Türkiye'nin 1990'lı yıllarda birinci safhayı bütünüyle olmasa bile tamamladığı ve ikinci safhaya geçişin başladığı görülmektedir. 1980'li yıllarda yoğun olarak yaşanan donanım ihtiyacı yerini yazılım ihtiyacına terk etmiştir. Ancak özellikle rekabet gücüne yönelik bilgi tabanlı sistemlerin sadece büyük şirketlerde kullanıldığı, ülkenin üretim gücünü oluşturan imalat sanayinin küçük ve orta ölçekli

şirketlerinde henüz yaygınlaşmadığı da bir gerçektir (İlyasoğlu, 1997, s. 70-71). Diğer bir tespitte kamu kesiminin bu adımları çok yavaş attığıdır. Türkiye’de bilgi tabanlı sistemlerin en yaygın kullanıldığı alan hizmet sektörüdür. Kişisel bilgisayar kullanımındaki artışta dikkat çekicidir.

Ekonomik alandaki bu kıpırdanmalar sosyal alanda da kısa zamanda etkisini göstermiş ve bilişim sektörü cazip sektörlerden birisi haline gelmeye başlamıştır. Artık gençler için en gözde meslekler doktorluk, avukatlık, öğretmenlik olmayıp; bilgisayar mühendisliği, bilgisayar programcılığı, elektronik mühendisliğidir. Artan uzmanlaşma ve işbölümü bilişim sektöründe çağ nüfusuna hem yurtiçinde hem de yurtdışında geniş bir istihdam olanağı imkanı sunmaktadır. Bu elemanlara olan ihtiyaç sürekli artmaktadır. Eğitim sisteminde yapılacak düzenleme ile bilişim sektörü eleman kaynağının yüksek öğrenimden orta öğrenime kaydırılması demografik yapı olarak avantajlı durumda bulunan Türkiye’nin gelecekte ihtiyaç duyacağı istihdam açığını kapatmak için bir çözüm olarak değerlendirilebilir.

Henüz kurumsallaşmayan ve küçük adımlar olarak niteleyebileceğimiz bu gelişmelerin politik alana etkisi ise oldukça sınırlı kalmıştır. Sistem değişikliği söz konusu olmadığı gibi, merkezi yapı muhafaza edilmeye çalışılmıştır. Bunda henüz bilgi yoğun bir kültür yapısına sahip sosyal yapının oluşmamasının yanı sıra; teknolojinin politik değişimi zorlayacak olan sıradan insanın yaşamına sadece medya araçlarıyla ulaşabilmesi de önemli rol oynamaktadır.

Kültürel alandaki değişim en az ve en son hissedilen değişimdir. Çünkü değişime tepkisel olarak bir direnç insanoğlunun doğasında vardır. Toplumda yeni davranışlar, yeni tarzlar, yeni alışkanlıklar hemen benimsenmez. Mevcut yapıya ve davranış kalıplarına uygun hale getirilerek özümsemeye çalışılır. Zaman alıcı bir süreç yaşanır. Geçmişin etkisi uzun sürer. Sık yaşanan kültürel değişimler ise daha fazla toplumsal dirençle karşılaşır. Türk toplumunda on dokuzuncu yüzyılda başlayan kültürel değişim, cumhuriyet ile hız ve süreklilik kazanmıştır. Ancak bu hız kimi zaman toplumsal bunalımlara da yol açmaktadır. Eğitim tabanlı olmayan değişimler yadırganmaktadır. 1980’li yıllarda başlayan dışa açılma ve iletişim imkanlarının artması küreselleşmenin etkilerini ülkemize taşımaya başlamıştır. Ancak bilgi toplumunun gerektirdiği rekabetçi ve bilgi yoğun bir kültür yapısına sahip olmak şimdilik zamana bağlıdır.

Sonuç olarak Türkiye yirmi birinci yüzyılın başında henüz tam sanayi toplumu aşamasına geçememiş ancak dünyadaki teknolojik gelişimlerden etkilenecek bilgi toplumu olma yolunda eşikte beklemektedir. Genç nüfusun yenilikçi teknolojik yaklaşımları kolay benimsediğinden hareketle, önümüzdeki dönem içerisinde bu etkilenenin boyutlarının daha da genişleyeceğini bekleyebiliriz. Türkiye henüz endüstrileşmiş bir ülke değil yarı endüstrileşmiş ülkedir. Sanayi toplumunun sosyal yapısına henüz ulaşamamış, ekonomisinde yapısal sorunları olan, dünya pazarlarında kitlesel ve kaliteli üretimiyle rekabet edebilecek bir sanayi altyapısı olmayan, ithal teknolojiye bağımlı, teknoloji üretmekte zorlanan ve politik, kültürel yapısıyla da çağdaş bir ülke görünümü sunamayan Türkiye'nin önümüzdeki dönemde bölümün başında söz konusu olan teknolojik gelişmelere sadece seyirci kalabileceğini değerlendirmek pek zor olmasa gerek. Bir sıçrama hepimizin beklentisidir. Sıçramanın altyapısı ise eğitim sürecidir. Aslında dünyada sadece birkaç ülkenin bilgi toplumu seviyesine ulaşma aşamasında olduğunu düşünürsek geç kalınmış sayılmaz. Şu anda alınacak tedbirler ülkemizi on yıl sonra sürecin içerisine sokabilir. Gelişmenin sadece ekonomi, para politikaları veya milli gelir hesabı boyutundan çıkararak toplumsal boyutuyla ele almak gereklidir. Halihazır durumda on yıl sonrası için bir değerlendirme yaptığımızda karşımıza şöyle bir tablonun çıkması beklenebilir:

Endüstrileşme sürecinde biraz daha mesafe alan Türkiye'nin teknoloji tabanlı üretim sürecine giremeyişi dünya pazarlarında rekabet gücünü düşürmektedir. Sanayide robot kullanımı yaygınlaşmamıştır. Ucuz işgücüyle kitlesel üretim yapılabilmekte ancak pazar problemi çekmektedir. İthal teknolojiye olan bağımlılığı sürmektedir. Gelişmiş ülkelerin teknolojik ürünleri için Türkiye iyi bir pazar durumuna gelmiştir. Bu pazar uluslar arası şirketlerin iştahını kabartmakta, ancak sermaye aktarımına yönelik yatırım yapma yerine ürün pazarlama yolunu seçmektedirler. Bu yüzden teknoloji transferinde de sıkıntılar yaşanmaktadır. Sadece savunma sanayi 1990'larda belirlenen stratejinin sonuçları doğrultusunda diğer sektörlerden farklı bir özellik arz etmektedir. Günlük yaşam değişmeye başlamıştır. Anadolu'nun en ücra köşelerinde bile zincir mağazalardan alışveriş yapılmakta, pek çok bankacılık ve finans işlemini yapabilme özelliğine sahip kredi kartları yaygın olarak kullanılmaktadır. El bilgisayarları hem iletişim hem de bilgi alışverişi maksadıyla özellikle şehirlerde yoğun kullanılır hale gelmiştir. Elektronik ve

bilgisayara yönelik eğitim artan talebe bağlı, zorunlu olarak eğitim sisteminde ağırlığa sahip olmuştur. Yetiştirilen teknik elemanların istihdam sorunu bu elemanları 1960'lı yıllardaki işçi göçüne benzer şekilde Avrupa Birliği ülkelerine göçe zorlamıştır. Politik sistemde halen özel statülü üyelik görüşmelerinin sürdürüldüğü Avrupa Birliği normlarına uygun düzenlemeler yapılmış, ancak bunların büyük kısmı pratiğe geçirilememiştir. Yalnız 2000'li yılların başında yasal düzenlemesi yapılan yerel yönetimlerin yetki devri olumlu sonuçlar vermeye başlamıştır. Birkaç Anadolu şehri Türkiye standartlarının üzerinde bir gelişme göstermiştir. Nüfus artış hızı düşmesine rağmen gelişmiş ülkelerin ilerisindedir. Hala ekonomik gelişme modelleri üzerinde tartışmalar yapılmaktadır. Asıl sorun devam etmektedir; ürettiğimizden çok tüketmekteyiz. Yüzyılın başına göre; kamunun küçülerek ekonomi üzerindeki etkisini kaybetmesi, finans sektörünün yapısal değişikliklerle uluslararası anlamda da güven verici hale getirilmesi, yapılan özelleştirmelerin özellikle büyük şehirlerde kaliteli sağlık ve eğitim hizmeti şeklinde kendisini göstermesi olumlu değişimler olarak görülmektedir.

4.2. Jeopolitik Değerlendirme

Türkiye dünyanın en duyarlı coğrafyasında yer almaktadır. Çevresindeki ülkeleri ele aldığımızda her birinin birbirleriyle sorunları vardır. Dünya üzerindeki kriz bölgeleri Türkiye'nin etrafındadır. Bu sorunlar yumağının ortasında Türkiye tek istikrar adasıdır. Balkanlardan Orta Asya'ya uzanan geniş bir coğrafyanın merkezinde olan Türkiye, bir yandan dünyadaki barışı korumak faaliyetlerini etkin bir şekilde korumaya devam ederken, diğer yandan barış zamanında; barışı korumak, istikrarı sürdürmek, krizleri önlemek çatışma durumunda ise, toprak bütünlüğünü korumak ve milli menfaatleri muhafaza etmek için yeterli bir seviyede askeri kuvvet idame etmek durumundadır.

Yeni dünya düzeninin bir uzantısı olan yeni güvenlik mimarileri, tehdit değerlendirmelerine dayalı olarak Türkiye'nin ve üyesi olduğu NATO'nun güvenlik stratejilerini de etkilemiştir. "İleriden Savunma" yerine "Kriz Bölgelerine İntikal" stratejisini benimseyen NATO, bu anlayışa hizmet edecek yeni bir yapılanma sürecine girmiştir. Bu strateji ise daha az kuvvet ile devamlı bir gelişim sergilemekte olan teknoloji ağırlıklı silah ve destek sistemlerini kullanarak, muhtemel bir istikrarsızlığa en seri şekilde istikrar kazandırmaya dayalıdır. Türkiye bu politika

doğrultusunda, dünyanın bir çok bölgesinde barış ve istikrarı sağlamak üzere NATO'nun ve Birleşmiş Milletlerin güvenlik sağlama görevlerine katılmaktadır. Türk Silahlı Kuvvetleri, Birleşmiş Milletler ve NATO tarafından dünya barışının korunmasına yönelik olarak alınmış kararlar çerçevesinde Afganistan, Arnavutluk, Bosna-Hersek, Kosova, Filistin, Kuveyt gibi ülkelerdeki faaliyetlere katılırken, aynı zamanda ikili ilişkiler çerçevesinde Gürcistan ve Azerbaycan gibi ülkelerde de bulunmaktadır.

Dünyadaki yeni oluşumlar ve yapılanmalar ışığında önümüzdeki 10 yıllık süreç içerisinde Türkiye'nin ülke stratejilerine temel dayanak olarak alması gereken üç temel yaklaşım bulunmaktadır. Birincisi üniter devlet yapısının korunarak ülkenin bütünlüğüne ve güvenliğine ilişkin ortaya çıkabilecek tüm tehditlerin etkisiz hale getirilmesidir. İkincisi Batı dünyasının özellikle Avrupa Birliği (AB)'nin gelişim stratejilerinin ayrıntılı olarak tahlil edilerek dönem içerisinde bu blok ile tam olmasa bile ülkeye ekonomik ve politik avantajlar sağlayacak bir tarzda entegrasyona gidilmesidir. Üçüncüsü ise 1800'lü yıllardan beridir süregelen toplumsal değişim çabasına ivme kazandırılarak ülke insanının 200 yıldır yaşadığı kimlik karmaşasının sona erdirilmesi ve her yönüyle; eğitimde, siyasette, kültürde, sanatta, bilimde, ticarete modern bir toplum aşamasına geçilmesidir.

4.2.1. Milli Güvenlik Kavramı

Devletlerin temel görevi vatandaşlarına müşterek güven ve refah ortamı sağlamaktır. Bu kapsamda; yurtiçi veya yurtdışından ülke bütünlüğüne yönelecek herhangi bir şiddet hareketi ve silahlı tecavüze karşı milli güç unsurlarını (siyasi güç, askeri güç, ekonomik güç, sosyo-ekonomik güç) harekete geçirerek şimdiye kadar güven ve refah ortamına yönelik elde edilmiş kazanımlarının korunması devletin milli güvenliğe yönelik stratejisinin esasını oluşturur. Aslında geçmişe yönelik olarak yapılan bu tanım savaş ve ayaklanmalara karşı yapılmış bir tanım olarak algılanmaktadır. Devletin milli güvenlikten sorumlu makamlarının herhangi bir savaş ya da ayaklanmaya karşı ne tür bir teşkilatlanmaya gideceği, bunların nasıl eğitileceği, silahlı mücadelenin hangi yöntemle yapılacağı, güvenlik kuvvetleri dışında kalan kamu ve özel sektör kurumlarının sorumluluklarının ne olacağı, muhtemel tahribatın nasıl etkisiz kılınacağı (sivil savunma) gibi dar bir çerçeveye oturtulmuş milli güvenlik tanımı özellikle İkinci Dünya Savaşı sonrasında ortaya

çıkan soğuk savaş metoduyla bir değişime uğramıştır. İki kutuplu dünyada soğuk savaş hedef ülkenin milli gücünü oluşturan unsurların zayıflatılarak, coğrafi ve sosyal bütünlüğünün bozulması maksadına yönelik örtülü bir savaş metodu olarak uygulanmaya başlanmıştır. Politik olarak anlaşmazlıkların açıkça telaffuz edilmediği bir ortamda; perde arkasından sosyo/kültürel alandaki zaafiyetler körüklenerek, siyasi alandaki girişimler engellenerek, ekonomik avantajlar yok edilerek hedef ülkelerin yıpratılması amacı güdülmüştür. Bu nedenle başlangıçta yaptığımız milli güvenlik kavramının boyutu sadece güvenlik tedbirleri boyutundan çıkıp genişleyerek siyasi, ekonomik ve sosyo/ekonomik boyutlarına genişlemiştir. Günümüzde ise küreselleşme, belirsizlik ortamı, bölgesel çatışmalar, enerji kaynaklarına olan ihtiyacın artışı, devlet dışı oluşumlar, nüfus artışı, uluslararası terörizm, insan hakları ve demokratik devlet olgusu, muhtemel kutuplaşmalar gibi faktörler milli güvenlik kavramını tamamen farklı bir boyuta oturtmuştur. Artık devletler barış zamanından itibaren kendi güvenlik ortamlarını şekillendirmek gereği hissetmeye başlamıştır. Stratejiler dinamik bir hal almış; sürekli değişime uğramaya başlamıştır. Sadece bir stratejiye yönelip, milli güç unsurlarını buraya kanaliz eden devletler bu karmaşık yapı içerisinde güvenlik sorunlarıyla boğuşur hale gelmiştir. Artık bir güvenlik oluşumunun içerisine girmekte kolay bir güvenlik sağlama yöntemi değildir. Çünkü bu oluşumlar da sürekli şekil değiştirmeye başlamıştır. Devletler mücadelelerini uzay boyutuna taşımışlardır. Hal böyle olunca milli güvenlik kavramı da yeniden yorumlanmış ve eskisinden daha basit bir ifadeyle ülke bütünlüğüne yönelik oluşan veya oluşabilecek tehditlere karşı alınması gereken tedbirlerin tümü olarak algılanmaya başlanmıştır. Gelecekle ilgili öngörüler de güvenlik kavramı içerisine dahil edilmiştir. Ancak bu gelecek eskiden olduğu gibi belirgin bir geleceğin ötesindedir. Bilgi teknolojilerinde meydana gelen gelişmelerin toplumları çok çabuk etkilemesi ve teknolojinin süratle eskimesi, karar vericilerin elinde stratejik güç olarak sadece tek bir olguyu bırakmıştır: Bilgi.

Herkes tarafından kolay elde edilebilir ve her alanda kullanılabilir olması, yeni milli güvenlik stratejilerinin oluşumunda bilgi gücüne yönelik kazanımların hedef olarak seçilmesini zorunlu kılmıştır. Ancak bilgiyi edinmekle iş bitmemiş, devletler için; bilginin bir milli güç unsuru olarak saklanıp, korunması da bir güvenlik problemi olarak milli güvenlik kavramı içerisinde yerini almıştır (Çörekçi, 2001, s. 42,44).

4.2.2. İç Tehditler

Genel değerlendirmeyi ve milli güvenlik kavramına yeni yaklaşımları analiz ettiğimizde, mevcut durumda birtakım güvenlik sorunları ve buna bağlı engellerle karşılaştığımızı görüyoruz. Ülkenin sık sık yaşadığı ekonomik krizler, iç ve dış tehditlerin şekil değiştirerek sürekli olarak ülke güvenliğini ve bütünlüğünü tehdit etmesi, Batı ülkelerinin güven vermeyen yaklaşımları, kendi iç dinamiğimizde ise idari yapının değişim ve gelişimi hızlandıracak ve yön verecek nitelikte olmayışı hatta engelleyici olması, ülke yönetiminin dünyadaki hızlı oluşumların farkına varamaması, gelecekle ilgili topluma yön verecek stratejiler üretememesi dolayısıyla sürekli bir belirsizlik ortamının mevcudiyeti ve bunun yaygın bir toplumsal güvensizlik ortamına dönüşmüş olması bu engellerden ilk akla gelenlerdir. 21 nci yüzyılın başlangıcında Türk toplumu dünya uygar milletler ailesi içerisinde hakettiği yeri almak istemektedir ancak onu oraya götürecek yöntem ve araçlardan yoksundur. Bu aşamada dış etkileri ayıracak olursak aslında ortada bir arz ve talep meselesi vardır. Toplum yenilik, değişim ve güç talep etmekte; sistem ise buna cevap verememektedir. Defalarca söz verildiği halde ortada nesnel elle tutulur bir sonucun olmaması tepkiye yol açmaktadır. Toplumun da buna tepkisi doğal olarak güvensizlik hatta zaman zaman kızgınlık şeklinde ortaya çıkmaktadır. Yapılan kamuoyu araştırmaları bu tepkiyi açıkça ortaya koymaktadır. İşte bu tepki güvenlik stratejileri açısından incelendiğinde mevcut ve muhtemel iç tehditlerin kaynağı olarak değerlendirilebilir. İç tehditleri sadece dış güç odaklarına ve ekonomik yetersizliklere bağlamak sınırlandırılmış bir yaklaşımdır. Bu faktörlerin mutlaka katkısı vardır ki, bunlardan ayrıntılı olarak bahsedilecektir. Ancak doğrudan ve dolaylı bütün sebeplerin ortaya konulması gerekir. Sözü edilen toplumsal tepki iç tehditlere de kaynak oluşturmakta; toplum içerisindeki memnuniyetsiz ve hayal kırıklığı yaşayan insanlardan taraftar bulmaktadır. Halihazırda iç tehditler üç ana grupta toplanabilir. Bunlar:

- Yıkıcı ve bölücü akımlar
- İrticai akımlar
- Aşırı sol ve sağ akımlar şeklinde sıralanabilir.

2002 yılı itibariyle değerlendirildiğinde yıkıcı ve bölücü akımların 15 yıl süren başarısız bir silahlı mücadeleden sonra strateji değiştirerek mücadelesini politik alana

kaydırdığı; irticai akımların ise silahlı bir mücadeleye girme aşamasının eşiğinde alınan bir takım önlemlerle kısmi olarak pasifize edildiği görülmektedir. Aşırı sol ve sağ akımlar ise gücünden çok şey kaybetse de her zaman varlığını korumuştur. Ancak unutulmaması gereken husus özellikle irticai akımların organize bir şekilde faaliyetlerini devam ettirdiği ve değişen dünya konjunktürü içerisinde önümüzdeki dönemde gelişimini sürdüreceğidir. Diğer bir dikkat çekici husus, yıkıcı ve bölücü akımların geçmiş dönemde ülke sınırları içerisinde faaliyet gösteren silahlı unsurlarını tasfiye etmediği ve bir tehdit unsuru olarak komşu ülkelerin topraklarında muhafaza ettiğidir.

Kısa dönem içerisinde iç tehditlerin nasıl bir şekil alacağını değerlendirmek güç bir iş olmakla birlikte bazı öngörülerde bulunabiliriz:

- Dönem içerisinde her üç tehditin de varlığını güçlenerek devam ettireceği,
- Batı dünyasının yıkıcı ve bölücü faaliyetleri terörist unsurlar olarak algılamayacağı ve siyasal desteğini artırarak sürdüreceği, devletin ekonomik zafiyetinden yararlanılarak politik mücadelenin yoğunlaştırılarak sürdürüleceği,
- İrticai akımların sertleşen Batılı devletlerinin politikalarına tepki olarak eylemsel bir yapı içerisine gireceği ve radikalleşeceği; emniyet kuvvetlerine yönelik açık mücadeleden ziyade ABD'deki eylemlere benzer şekilde devletin siyasal, ekonomik, moral ve bilgi gücünü oluşturan stratejik hedeflere yöneleceği, irticai örgütlerin diğer ülkelerdeki aynı tür örgütlerle işbirliğini güçlendireceği ve eylem birliğine gideceği; bu suretle güç kazanacağı,
- Bu tehditlere ek olarak küreselleşme karşıtı unsurların da yasa dışı faaliyete başlayacağı, özellikle Batılı ülkelere tepki olarak başlayacak bu hareketlerin, ekonomik krizlerin yarattığı bunalım ortamından da güç alarak, yıkıcı sol veya anarşist akımlar şeklinde ortaya çıkacağı değerlendirilmektedir.

Sonuç olarak kısa dönemde durumda herhangi bir iyileşme beklenmemekte, tam tersine iç tehdit unsurlarının ülke güvenliğine yönelik eylemlerinde artış ve şekil değişiklikleri beklenmektedir. Fakat iç tehditlerle mücadele konusunda tecrübe, hatta bağışıklık kazanmış olan Türk toplumunun; her ne kadar ekonomik, politik ve psikolojik zorluklar içerisinde olsa da yine sağduyusuyla hareket edeceği ve devletiyle birlikte hareket ederek bu tehditlerin kısa dönemde amaçlarına ulaşmasında en büyük engel olacağı da değerlendirilmektedir.



4.2.3. Dış Tehditler

Türkiye; coğrafi konumu, büyüklüğü, yer altı ve yer üstü kaynakları, siyasi yapısı gibi değerleriyle Asya, Avrupa ve Afrika kıtaları arasında bir köprü, Balkanlar, Kafkaslar ve Ortadoğu kriz bölgelerinde çıkış noktası olabilecek bir demokrasi adası, başta Osmanlı İmparatorluğu olmak üzere dünyayı büyük ölçüde etkileyen ve yönlendiren Türk tarihi ve Türk kültürünün mirasçısı, Avrasya Türklüğünün lideri, bölgedeki tek demokratik, laik, sosyal bir hukuk devletidir. Dünya güç merkezlerinin kıyasıya çıkar ve nüfuz mücadelesi yaptığı bir bölgede, demokrasi içinde kalkınmaya çalışan; ekonomik, askeri ve siyasal gücü arttıkça çevresi ile daha fazla ilgilenmeye başlayan Türkiye, jeopolitiğinin gereği olarak lider ülke olmaya mecburdur. Türkiye'nin bu mecburiyeti kendisini aynı zamanda doğal olarak hedef ülke durumuna da getirmektedir. Hedef ülke konumundan dolayı Türkiye jeolojik olarak deprem kuşağı üzerinde olduğu gibi jeopolitik olarak da deprem kuşağı üzerindedir. Nasıl ki jeolojik olarak bir depremin yeri ve zamanı önceden kestirilemiyorsa ülkemize yönelen dış tehditlerin de sürekli olarak bir belirsizliği ve sürekliliği vardır. Strateji biliminde biz buna "sürekli tehdit" adını veriyoruz. Günümüzde Türkiye üzerinde milli menfaat ve hedeflerine uygun emeller taşımakta olan ülkeler, özellikle Türkiye'nin içinde bulunduğu politik, ekonomik ve sosyal şartları da hesaba katan dış politikalar izlemektedir. Bu politika, duruma göre tek başlarına veya dahil oldukları ittifak çerçevesinde Türkiye'nin yanında veya karşısında bulunma şeklinde görülmektedir. Jeopolitiğin üç temel unsuruna bağlı olarak değişken bir yapı içeren yaklaşımlar ve politikalar zaman zaman bölgenin güvenliğini ve istikrarını tehdit etmektedir. Türkiye bugün birden fazla istikametten sıcak ve soğuk harbin tehditi karşısında bulunmaktadır. Şimdi, coğrafi etkenlerin politikaya olan etkilerini inceleyen ve bu etkilerden arzu edilen politikaların oluşturulmasında nasıl faydalanılacağını inceleyen bir disiplin olarak tanımlanan jeopolitiğin/sözkonusu üç temel unsurunun neler olduğundan kısaca bahsederek, bu kapsamda Türkiye'ye yönelen dış tehditlerin tanımlamalarını ortaya koyacağız:

Bir ülkenin demografik yapısı (nüfusu, nüfusun cinsiyete göre dağılımı, işgücü, genç-yaşlı nüfus v.b.), siyasi yapısı, uluslar arası ilişkileri ve bağlantılı olduğu uluslar arası kuruluşlar (AB, NATO, AGİT v.b.), ekonomik gelir düzeyi ve ekonomik yapısı (fabrikaları, yer altı-yerüstü kaynakları, bunları kullanma ve işleme biçimleri v.b.),



bilim teknoloji düzeyi gibi unsurlar jeopolitiğin değişen unsurları olarak adlandırılır (Toptaş, 2001, s. 76).

Ülkenin fiziki coğrafyasından kaynaklanan unsurlardır. Örneğin dünyadaki fiziki konumu, ada ya da kara devleti olması, sahip olduğu doğal engeller (dağlar, nehirler, göller, denizler v.b.), komşuları gibi unsurlar ise jeopolitiğin değişmeyen unsurlarıdır (Toptaş, 2001, s.76):

Değişen veya değişmeyen unsurlardan birini veya birkaçını öne çıkarabilen, değerini arttıran veya düşüren en önemli faktör zamandır. Örneğin; bir enerji kaynağı olarak petrol, zamana bağlı olarak uluslar arası önem kazanıp, kaybedebilir; NATO, AB gibi uluslar arası paktların önemi zamana bağlı olarak artabilir ya da azalabilir ya da Varşova Paktında olduğu gibi tamamen yok olabilir. A ülkesinin önemi birden bire artabilir ya da azalabilir (Toptaş, 2001, s. 76).

Bu unsurlardan hareketle özellikle komşularımızın ülkemiz için oluşturduğu dış tehditleri ülke başlıklarıyla inceleyecek olursak;

4.2.3.1. Yunanistan

Yunanistan'ın Türkiye'ye karşı uyguladığı politikanın temelini "Türkiye'nin zararına olan her şey Yunanistan'ın yararınadır" görüşü oluşturmaktadır. Bu ülke milli ideali olan "Megalo İdea"nın gerçekleşmesinde kendisine karşı en büyük engel olarak Türkiye'yi görmekte ve gerek içte gerekse dışta aktif bir "Türk düşmanlığı" politikası izlemektedir. Askeri alanda nisbi olarak Türkiye'ye karşı güçsüz olduğunun farkında olan Yunanistan'ın, Türkiye'ye yönelik politikaları, genellikle uluslar arası alanda Türkiye'nin her türlü girişimini engelleme, uluslar arası platformda Türkiye'ye sürekli olarak saldırgan ve uzlaşmaz bir ülke imajını kazandırma, Türkiye ile sorunları olan ülkelerle ve Türkiye içerisinde iç tehdit unsuru olan güçlerle güç birliği yapma şeklinde ortaya çıkmaktadır. Sonuçta iç dinamiklerini de "doğudan gelecek tehdit" konseptine dayandıran Yunanistan Türkiye için kısa orta ve uzun dönemde sürekli tehdit niteliğine sahip bir ülkedir.

4.2.3.2. Bulgaristan

Türkiye ile tarihsel anlamda çelişkileri bulunan Bulgaristan, Soğuk savaş döneminde Varşova Paktında Sovyetler Birliğinin en sadık müttefiki olarak karşı pakt da (NATO) olan komşusu Türkiye'ye karşı, yıllarca hasmane bir tutum sürdürmüştür. Özellikle ülkesi içerisinde azınlık durumunda bulunan ve Türk-Müslüman kimliğine sahip soydaşlarımızı, kendisi için sürekli bir tehdit unsuru olarak algılayan Bulgaristan, hemen yanı başında güçlü bir Türkiye'nin varlığından rahatsızlığını her fırsatta belli eden politikalar izlemiştir. Uzun yıllar soydaşlarımıza baskı ve asimilasyon politikaları uygulamıştır. Varşova Paktının dağılmasından sonra uzunca bir süre kendi iç dengesini bulamamış, silah, uyuşturucu ve kara para trafiğinin merkezi durumuna gelmiştir. Bu durumu Türkiye'deki iç tehdit unsurları için bu ülkeyi bir üs konumuna getirmiştir. Ancak son dönemde Doğu Avrupa'daki bağımsızlık hareketleri ve demokrasi fikrinden etkilenerek, yeni bir politika izlemeye başlamıştır. AB'ne girme çabaları gerek toplumsal, gerekse ekonomik alanda Bulgaristan'a ivme kazandırmıştır. Batı ülkeleriyle ve Türkiye ile olan temaslarını artırma ve sıklaştırma çabaları, Türkiye'nin bu ülkeye karşı bekle gör tarzı bir politika geliştirmesine sebep olmuştur. Günümüzde Türkiye'ye karşı askeri bir tehdit olma niteliğine sahip olmayan Bulgaristan'ın; kısa dönemde Batıyla bütünleşme çabaları desteklenmeli ve yapılacak temaslar ve ekonomik işbirliği ile, orta ve uzun dönemde dost ve müttefik bir ülke konumuna gelmesine yönelik politikalar izlenmelidir.

4.2.3.3. Rusya Federasyonu

Hali hazırda dünyanın belli başlı güç odaklarından biri olan Rusya'nın, gerek geçmişte gerek günümüzde gerekse gelecekte, Türkiye için sürekli tehdit niteliğini taşıdığı ve taşıyacağı açıktır. Genel stratejisinin her basamağında Türkiye, Rusya için her zaman bir hedef ülke konumunda olmuştur. Gelecekte bu durumun değişeceği sanılmamaktadır. İdeolojisini bile değiştiren Rusya'nın Türkiye'ye ilişkin politikalarında hiçbir değişiklik olmamıştır. Bununda ötesinde Varşova Paktının dağılmasından sonra ortaya çıkan belirsizlik ve istikrarsızlık ortamı bu ülkenin Türkiye'ye; Türkiye'nin de bu ülkeye yönelik politikalarında da bir belirsizlik ve istikrarsızlık durumunu ortaya çıkarmıştır. Kafkasya ve Orta Asya'da bulunan Türklere karşı tarihsel sorumlulukları olan ve nüfuz arayışında olan Türkiye bu

bölgelerde karşısında hep Rusya'yı bulmuştur. Buna karşılık Rusya'da sıcak denizlere inme, petrol bölgelerini kontrol etme ve eski Sovyetler Birliği'ni yeniden yaratma stratejilerinin karşısında Türkiye'yi hedef ülke olarak görmüştür. Her ne kadar eski teknoloji kullanıyor olsa da konvansiyonel ve nükleer silah gücünü sürekli olarak muhafaza eden Rusya zaman zaman bu gücünü kriz bölgelerinde kullanmak istemektedir. Bu yönüyle de Türkiye için askeri bir tehdit niteliğini sürdürmekte olan bu ülke ile çok dikkatli bir ilişki düzeyinin sağlanması, belki de Türkiye'nin 21 nci yüzyılda izleyeceği dış politikanın mihenk taşıdır.

4.2.3.4. Ermenistan

Türkiye ile tarihten gelen sorunları olan ve Türkiye'den toprak talebi olan Ermenistan, Türkiye'ye karşı genel olarak Yunanistan'a benzer bir politika yürütmektedir. Azerbaycan'la Karabağ yüzünden savaş durumundadır. Bir taraftan Türkiye'yi arkasına alan Azerbaycan'a karşı Rusya ile askeri işbirliğine giderken, diğer tarafta uluslar arası kamuoyunda kontrol edemediği "Diaspora" ile her alanda Türkiye'nin karşısında yer almaktadır. Bu yaklaşım doğal olarak Türkiye tarafından tepkiyle karşılanmaktadır. Ülke içindeki ekonomik, politik yetersizliklere eklenen Türkiye düşmanlığı ve Türkiye'de faaliyet gösteren yıkıcı bölücü örgütlere verilen destek, Ermenistan'ı Türkiye için bir tehdit unsuru haline getirmiştir. Askeri anlamda Türkiye'ye karşı Rusya'nın desteği olmadan herhangi bir imkan kabiliyeti yoktur. Kısa ve orta vadede dönemsel krizlere sebep olabilecek Ermenistan'ın, özellikle tarihsel iddialarını inatla sürdürmesi, uzun dönemde de Türkiye'ye yönelik dostluk ve işbirliği içermeyen oluşumların içerisinde yer alacağının göstergesidir.

4.2.3.5. Irak

Irak; milliyetçi, sosyalist, tek tip bir toplum oluşturmayı, Kürt sorununu milli birliğini bozmaksızın çözümlemeyi, Türk ve Kürt azınlığı zaman içerisinde Araplaştırmayı, Basra Körfezi'ni nüfuzu altına almayı, Filistin sorununu kuvvet zoruyla çözümlemeyi ve Arap dünyasının lideri olarak Arap Birliği kurmayı "milli amaç" olarak benimsemiştir. Mevcut gücü ve saldırgan tutumu ile Irak kısa ve orta dönemde Türkiye için fiziki bir tehdit unsuru oluşturmaktadır. Elinde mevcut uzun menzilli füzeleri ve biyolojik-kimyasal silah kapasitesi dikkat çekicidir. Uzun dönemde özellikle ABD'nin etkisiyle Irak'ın tam anlamıyla olmasa bile tutum ve

yaklaşımlarında zorunlu bir değişiklik yaşanacağı değerlendirilmektedir. Totaliter bir rejimle yönetilen Irak, yönetim sorunlarını aştığı takdirde bölgede Türkiye için işbirliği yapılabilecek ülke konumuna gelebilir. Özellikle kendi ülke toprağı olan Kuzey Irak'ın kontrolü dışında bulunması, yıkıcı ve bölücü terör örgütlerinin bu bölgeyi üs haline getirmelerine imkan tanımış ve bu bölge Türkiye için yıkıcı ve bölücü iç tehdidin kaynağı olmuştur. Bu rahatsızlığın çözümü, şimdikinden farklı anlamda güçlü bir Irak yönetiminin bölgeyi kontrol altına almasıdır. Bu kapsamda Irak'ın toprak bütünlüğünün korunması, Türkiye'nin Irak politikasının ana unsuru olmalıdır. Bunun yanı sıra mevcut yönetimle de Irak halkının tepkisini çekecek düşmanlık tarzında bir ilişkiden ziyade, kontrollü bir ilişkinin takibi Türkiye'nin siyasi ve ekonomik menfaatleri icabıdır. Çünkü Irak halkının tepkisini çekecek işbirlikleri ve izlenecek politikalar Türkiye ile Irak arasında tarihsel anlamda uçurumlar oluşturacak ve uzun dönemde sürekli bir rahatsızlık ortamı yaratacaktır.

4.2.3.6. Suriye

Suriye, Hatay ilinin ülkesine katılmasını bir devlet politikası olarak benimsemiştir. Hatay sorununun yanı sıra, Türkiye'ye yönelik terör faaliyetlerinin desteklenmesi, su sorunu, kaçakçılık sorunu gibi yıllardan beridir mevcut olan ve çözüm önerileri henüz açıkça ortaya konmayan problem sahaları Türkiye ile Suriye arasında süregelen huzursuzluğun kaynakları olmuştur. Yunanistan ile işbirliğine yönelik temasları Türkiye için rahatsızlık yaratmaktadır. Irak gibi totaliter bir rejimle yönetilen Suriye'de kendi iç siyasi dengesini bulamamıştır. Azınlığın tahakkümüne dayalı bir yönetim şekliyle zaman zaman iç karışıklıklara maruz kalmıştır. Ezeli düşmanı İsrail ile sürekli olarak gerginlik stratejisini benimseyen Suriye, son dönemde diğer Arap devletleri gibi, Türkiye-İsrail yaklaşması ve işbirliğine açıkça tepki duymaktadır. Özellikle savunma sanayi alanındaki işbirliği ve askeri tatbikatlardan duyduğu rahatsızlığı açıkça ifade etmektedir. Yıllarca Türkiye'ye yönelik bölücü terör örgütlerine yardım ve yataklık eden Suriye, 1998 yılında Türkiye'nin birtakım yaptırımlara yönelmesiyle bölücü terör örgütünün başını sınır dışı etmek zorunda kalmıştır. Güneydoğu Anadolu Projesinin (GAP) Türkiye'nin gelişimine sağlayacağı katkıyı ve bu projenin bölgeye getireceği yapısal ekonomik ve sosyal değişimleri bir tehdit olarak algılayan Suriye, Fırat ve Dicle nehirlerinden gelen sudan yeteri kadar faydalanamadığını öne sürerek, uluslar arası kamuoyunda

bir “Su sorunu” yaratma gayreti içerisinde. Nitekim Arap ülkeleri arasında bu konuda kendisine yandaşlar bulmakta zorluk çekmemiştir. Son dönemde Hafız Esad’ın ölümünden sonra yerine geçen oğlu Beşir Esad, uzun yıllar dış dünyadan kopuk olarak yaşayan ve ABD’nin her yıl yayınladığı terörist ülkeler listesindeki mevcudiyetini yıllardır sürdüren Suriye’yi bu yalnızlığından kurtarmak için bir takım girişimlerde bulunmaktadır. 2001 yılında BM Güvenlik Konseyine üye olarak seçilen Suriye’nin bu açılımları desteklenmeli ve Türkiye ile arasındaki sorunları somut bir şekilde ele alınmalıdır. Eski Rus askeri modeline ve malzemesine sahip askeri varlığı, Türkiye’den ziyade İsrail için bir sorun teşkil etmektedir. Kısa vadede dış yaptığı açılımların Türkiye tarafından desteklenmesinin orta ve uzun vadede Türkiye’ye bu ülke ile daha sağlıklı bir ilişki kurulmasına zemin sağlayacağı muhakkaktır. Ancak günümüzde Suriye, Türkiye için henüz iyi niyetli ve dostane davranışlar gösteren bir ülke olma özelliğinden uzaktır.

4.2.3.7. İran

Jeopolitik ve jeostratejik konumu itibarıyla Türkiye’ye benzer bir yapıya sahip İran’da, 1979 yılında bir rejim değişikliğine gidilmiş ve yönetim şeriat düzeninin esas alındığı mollaların denetimine geçmiştir. Bu aşamadan itibaren İran içte islami rejimi her alanda hakim kılma; dışta ise kademeli olarak islam devriminin ihracını kendi yönetimine hedef seçmiştir. Devrim Konseyince belirlenen politikanın aşamalarından birisi de islam devriminin Türkiye’de gerçekleştirilmesidir. Türkiye’nin gelişmekte olan diğer islam ülkelerine model olabilecek laik ve çağdaş yapısı, İran’ı sürekli olarak rahatsız etmiştir. Bu kapsamda Türkiye içerisindeki irticai unsurlara destek sağlamakta, Türkiye’yi zayıf düşürmek için yasadışı PKK örgütüne lojistik destek vermekte, Kuzey Irak’ta nüfuz mücadelesi yapmaktadır. Türkiye’nin içişlerine zaman zaman yapılan göndermeler Türkiye için rahatsız edici boyutta olmaktadır. Pek dostane olmayan bu yaklaşımlar Türkiye tarafından dikkatle takip edilmektedir. İran ile doğal sınırları olan Türkiye’nin bu ülke ile olan ilişkilerinde sürekli ihtiyatlı bir tutum takındığı dikkat çekmektedir. Neticede önemli bir komşu olan İran’da kısa ve orta dönemde ticari ilişkilerin geliştirilmesi ve enerji kaynakları için sürekli bir alternatif ülke olarak elde bulundurulması esasına dayalı kontrollü bir politika Türkiye’nin çizgisi olmalıdır. Uzun dönemde dünyaya açılma ve modernleşme çabalarında Türkiye’nin aracı rolü oynaması ve iki ülkenin Kuzey

Irak politikalarındaki benzerliğin hayata geçirilmesi, İran'ın Türkiye'ye karşı takındığı dostane olmayan tavırdaki iniş ve çıkışlara bağlı olacaktır.

Azerbaycan ve Gürcistan ile ikili ilişkilerin dostane bir seviyede yürütülmesi ve yakın işbirliği yapıldığından dolayı; Türkiye için potansiyel bir tehdit oluşturmadığı fikrinden hareketle bu iki ülke değerlendirmenin kapsamına alınmamıştır. Genel olarak dış tehditleri değerlendirdiğimizde şu sonuçlara ulaşabiliriz:

- Yunanistan ile anlaşmazlıkların diplomasi yoluyla çözülemeyeceği artık bir gerçektir. Ufak anlaşmazlıklardan, sıcak çatışmaya kadar gidebilecek bir yelpazede yürüyen ilişkiler Türkiye'nin savunma stratejisinin belirlenmesinde bir etken olarak Yunanistan'ı baş köşeye oturtmuştur.
- Rusya Federasyonu her dönemde Türkiye için bir tehdit oluşturmıştır ve oluşturmaya devam edecektir. NATO, AB, Avrupa Güvenlik ve İşbirliği Teşkilatı (AGİT) gibi uluslararası kurumlar Rusya Federasyonu'na karşı güvenliğimizin garantisidir.
- Irak'ın toprak bütünlüğü mutlaka korunmalıdır.
- İran, Ermenistan ve Suriye'nin Türkiye'nin düşmanlarına verdiği destek her ne surette olursa olsun engellenmelidir. Bu ülkelerin dışa açılımları desteklenmelidir.
- Kıbrıs özel statüsü gereği hukuki haklarımızdan (garantörlük) ve toprak Bütünlüğünden vazgeçilmeden koruma altında bulundurulmalıdır.
- Azerbaycan, Gürcistan, Bulgaristan ile sağlanan temas ortamı sıklaştırılarak sürdürülmelidir.

4.3. Türkiye'nin Savunma Stratejisinde Değişiklikler

İki kutuplu dengenin sona ermesine karşılık ortaya çıkan istikrarsızlık ve belirsizlik ortamında yeni küresel güvenlik sorunları önem kazanmıştır. Bunlar: Ülkelerdeki nüfus artışları, kaynakların paylaşımı, aşırı şehirleşme ve çevre kirlenmesi, teknolojik gelişmeler, merkezi devlet yapılarının zayıflaması, uluslar arası kuruluşların milli güç unsurları üzerindeki etkinliğinin artması, siyasi ve ekonomik istikrarsızlıklar ve belirsizlikler, uluslar arası organize suçlar, dini ve etnik çatışmalar ve kitle imha silahlarının yayılma eğilimi, tehdit kavramını daha da muğlak hale getirmiştir. Bu nedenle tüm dünyada olduğu gibi Türkiye'de de stratejik tehdit algılamalarında bazı değişimlere yol açılmıştır. Tehdit kavramı daha önce

belirgin ve kitlesel iken, bugün, dünyadaki global eğilimler ve gelişmeler neticesinde risk alanları; ülkelerin milli menfaatlerinin önem derecesine bağlı olarak, çok yönlü, çok boyutlu ve değişken bir hale gelmiştir. Balkanlar'dan Orta Asya'ya uzanan geniş bir coğrafyanın merkezinde yer alan ve bölgesinin vazgeçilmez bir istikrar unsuru olan Türkiye, bu tehditleri bertaraf edebilecek milli güç unsurlarına sahiptir. Türkiye bu stratejik konumuyla; genel savunma stratejisi olarak, daha barışçı ve istikrarlı bir güvenlik ortamı yaratmak için bölgesinde çatışmaları önleyerek, gerginlikleri azaltmaya ve istikrarı yükseltmeyi yardımcı olmayı amaçlamalıdır. Türkiye'nin içerisinde bulunduğu politik-askeri ortamın bir gereği olarak caydırıcı bir yapının oluşturulması ve muhafazası bu politikaların ayrılmaz bir parçası olmalıdır (Kıvrıkoğlu, 1998, s. 10-12).

Bu düşünceler ışığında Türk Silahlı Kuvvetlerinin Savunma Konsepti'de aşağıdaki temel askeri strateji prensipleri üzerine inşa edilmiştir:

- Caydırıcılık
- Kollektif Güvenlik
- Kriz Yönetimi ve Çatışmaların Önlenmesi,
- İleriden Savunma.

Bu bağlamda Savunma Konsepti aşağıdaki tedbirlerin alınmasını öngörmektedir:

İç tehditle ilgili olarak;

Ülkenin bölünmezliğini, birlik ve bütünlüğünü, Türkiye Cumhuriyeti'nin demokratik ve laik hukuk devleti yapısını tehdit eden terör örgütü ve irticai unsurlarla mücadele ederek iç tehditi bertaraf etmek

Dış tehditle ilgili olarak;

- Türkiye Cumhuriyeti'nin bağımsızlığını, toprak bütünlüğünü ve halkın bütünlüğünü sağlamak maksadıyla öncelikle muhtemel dış tehditi caydırmak,
- Caydırmanın yetersiz kalması ve bir krizin ortaya çıkması halinde, krizin kontrol altına alınarak Türkiye'nin hak ve menfaatleri lehine sonuçlanmasını sağlamak,
- Savaşı önlemek, uluslar arası gerginlikleri azaltmak, adil ve devamlı bir barışı temin için NATO ve diğer kollektif güvenlik sistemleri içinde üzerine düşen her türlü katkıyı yapmak,

- Bir savaş durumunda, Türkiye Cumhuriyeti'nin sınırlarını, hava sahasını, karasularını ve ekonomik bölgelerini korumaktır (Kıvrıkoğlu, 1998, s. 10-12).

Yapılan değerlendirmelerin ışığında ortaya çıkan gerçek, Türkiye'nin içte ve dışta bir takım belirgin tehditlere maruz olduğu ve bu tehditlerin süreklilik arz eden bir mahiyette olduğudur. Bu da güçlü bir Silahlı Kuvvetlere sahip olunması gerektiğinin somut bir delilidir. Genel savunma stratejisi olarak "Yurtta barış, dünyada barış" ilkesini benimseyen ve bunu dış ilişkilerine de yansıtan Türkiye'nin, bölgesindeki son dönemde meydana gelen gelişmeleri değerlendirdiğimizde; önümüzdeki dönemde ülkesinin birliğini, bütünlüğünü ve güvenliğini sağlamak için yeni savunma stratejileri oluşturmasının ve bunları uygulamaya geçirmesinin gerekliliği de ortaya çıkmaktadır. Ülke güvenliği için değişen savaş kavramı içerisinde yeni değerlendirmeler yapılmalı ve hayata geçirilmelidir. Temelde insan gücü yeterliliği ve ekonomik kaynaklara dayalı geliştirilen savunma stratejisi yeni bir anlayış içerisinde yorumlanmalı, eğitilmiş insan ve teknoloji temeline dayalı daha etkin, verimli ve rasyonel bir savunma yapılanması oluşturulmalıdır. Dış politikada olmazsa olmaz koşullar ortaya konmalıdır. Bu hususlar milli menfaatlerimiz olarak açıkça ilan edilmelidir. Milli menfaatlerimizi sadece Türkiye'de değil dünyanın her yerinde koruyacak ve kollayacak bir savunma stratejisi uygulamaya konulmalıdır. Yapısal olarak şu anda Türkiye'deki en organize güç olan Silahlı Kuvvetlerin bu stratejinin yürütülmesindeki payı arttırılmalıdır. Ekonomik, teknolojik, kültürel ve toplumsal alanda mücadelenin boyutları genişlemelidir. Günümüzde dünyada meydana gelen gelişmeler Türkiye'nin tarihsel misyonunu yerine getirmesi için gerekli koşulları yaratmıştır. Bütün olumsuzluklara rağmen, NATO üyesi, AB'ne üye olma sürecindeki Türkiye; teröre karşı verdiği mücadeleden başarıyla çıkmış, 1946'dan beridir sahip olduğu çok partili parlamenter düzenini kesintilerle de olsa muhafaza etmiş, laik ve hukuka dayalı bir toplumsal düzen oluşturmuş, son dönemde ekonomik sıkıntılar içerisinde de bulunsa sosyal refahı yaygınlaştırmış ve modern bir toplum yaratma yolunda toplumsal ve kurumsal altyapısını tamamlamıştır. Bu süreç içerisinde milli birlik, bütünlüğüne ve güvenliğine yönelik her türlü tehdit doğru olarak algılamış ve mücadele edilmiştir. Tehdit değerlendirmesinde bahsedilen üç temel stratejiden; üniter devletin muhafazası ve tehditlerin bertaraf edilmesi amacı gerçekleşmiş, AB'ne üyelik yolunda önemli adımlar atılmış, modern bir toplum yapısı yaratma çabaları ise sürdürülmektedir. Ülke insanı, kısa dönemde kendisini

umutsuzluğa ve karamsarlığa düşüren sıkıntıların, uzun dönemde kazanımlar şekline dönüştüğünü görmek istemektedir. Fırsatların belirsizlik ortamlarından çıktığı unutulmamalıdır.

Daha somut olarak ele alacak olursak yeni savunma stratejisinin temel taşlarını şunlar oluşturmalıdır:

- Caydırıcılığı esas alan, teknoloji ağırlıklı bir savunma gücü oluşturulmalıdır.
- Barışta güvenlik ortamının şekillendirilmesinden, kesin sonuçlu konvansiyonel harbe giden süreç içerisinde adım adım müdahale stratejisi benimsenmelidir.
- Tehditler geniş bir yelpazede değerlendirilip açık olarak tanımlanmalı ve mücadele edilmelidir. (devletler, silahlı güçler, terörizm, çeteler, uyuşturucu tacirleri, silah kaçakçıları v.b.)

4.4. Türkiye'nin Bilim ve Teknoloji Politikaları

Bilim ve Teknoloji Politikası; bilimsel ve teknolojik çalışmaların bir ülkenin ekonomik, sosyal, politik ve askeri alanlardaki ihtiyaçlarına ve hedeflerine göre geliştirilmesi ve yönlendirilmesidir (Özdaş, 1999).

Ülkelerin uzun vadeli kalkınma hedeflerine ulaşmaları, sistematik olarak üretilen ve uygulamaya konulan politikalarla mümkündür. Bu çerçevede, stratejik anlamda hayati önem taşıyan ve mümkün olduğunca zamanında ve en iyi şekilde uygulanmaya çalışılan politikaların başında “Bilim ve Teknoloji Politikaları” gelmektedir. Bilim ve teknoloji politikalarının tabanı olan bilim ve teknoloji üretimi; küresel rekabetin şartlarına ayak uydurabilmenin ve ekonomik kalkınmayı hızlandırabilmenin yegane yoludur. Ulusal kalkınmanın temel taşı olan bilim ve teknolojinin üretimi, yönetimi ve uygulanması; tutarlı ve uzun vadeli politikalarla bağlantılıdır. Başarılı politikaların özünde ekonomik büyüme ve ihracaat performansının arttırılması gibi iki ana hedef gözetilir (Ayhan, 2002, s. 307-307).

Türkiye’de, 1990’ların ortasına değin, teknoloji yabancı yatırımların bir türevi olarak görülmüştür. Bundan dolayı ayrıca teknoloji üretimi için kaynak tahsisi öngörülmemiştir. İktisat teorilerindeki değişime paralel olarak kalkınma modellerinin dayandığı temel dinamik olan üretimin bir parçası olarak teknoloji 1970’li yıllardan itibaren mikro iktisatın ilgi alanlarından biri haline gelmiştir. Türkiye’de bu anlayışa

uygun olarak atılan ilk adım TÜBİTAK'ın kurulması olmuştur. Ancak bu kurum ülke sanayisi ile organik bir bağ kurmadan sadece bilimsel araştırma yönüyle, akademik çevrelerle bağlantı kurarak, ilerisi için bir potansiyel geliştirmekle meşgul olmuştur. Geç gelen sanayileşme sürecinin getirdiği bir zorunluluk olarak ithal ikamesine dayalı, daha çok sermaye yoğun, kullanılmış tekniklerle bol düz emek istihdam eden bir üretim yolu seçen Türkiye, patent haklarından, mesleki eğitime kadar pek çok yeni hukuki düzenleme yaparak yeni kurumlar ve mekanizmalar oluşturma gerekliliğini öngören teknolojinin kurumsallaştırılması yolunda mesafe alamamıştır. Teknoloji, üretim ve kalkınma ilişkisi oluşturulamamıştır (Ayhan, 2002, s. 106).

Türkiye'de 1800 Islahat Fermanı ile başlayan yenilik hareketleri Osmanlı Devleti'nin yıkılmasından sonra da devam etmiş ve refah toplumu yaratmak yönündeki çalışmalar ilk kez 1930'lu yıllarda planlı bir yapıya kavuşturulmuştur. Nitekim bu yıllarda kazanılan ivme ile toplum ve devlet yapısında önemli değişimler yaşanmış ve 1950-1980 arası ikinci planlı dönemin altyapısı oluşturulmuştur. Ancak dikkat edilmesi gereken husus bu süreçlerin sanayileşme çabası içerisinde yürütülmesiydi. Çünkü o yıllarda sanayi toplumu olmak refah toplumu olmakla eş anlama geliyordu. 1980'li yıllara gelindiğinde ise dünyada bir şeyler değişmeye başladı. Sanayileşme sürecini aşan ABD ve Batı Avrupa ülkeleri yenilikçi bir hareketin içerisine girmişlerdi. Bilim ve teknoloji tabanlı bu hareket kısa zamanda toplumsal yapıda da etkisini göstermiştir. Duvarlar yıkılmıştır. Anlayışlar büyük bir değişime uğramıştır. Dünyanın siyasi yapısında devrim niteliğinde gelişmeler yaşanmıştır. Teknolojik gelişim üretimi ve ticareti etkilemiş, ekonomik küreselleşme başlamıştır. Özellikle Doğu blokunun çöküşü Türkiye için pek çok fırsatları da beraberinde getirmiştir. Ancak, Türkiye bu dönem içerisinde planlı stratejilerini bıraktı ve bilinçsiz bir şekilde gelişimini sürdürmeye çalışmıştır. Dünya ticaretindeki küreselleşmenin aradığı pazarlardan birisi haline gelmeye başlamıştır. Bu dönemde teknoloji tabanlı yığmsal üretimin ürünleri Türkiye pazarlarında boy göstermeye başlamıştır. Maalesef evlere giren televizyon, buzdolabı ekonomik gelişmenin göstergeleri gibi sayılmıştır. Temelde ülkeyi bir sonraki toplum aşaması olan bilgi toplumuna taşıyacak olan yenilikçi bir yaklaşıma sahip bilinçli stratejiler geliştirilmemiştir. Bunun yanı sıra sanayileşme çabamızdaki şimdiye kadar elde edilen mesafe de bir ölçüde heba edilmiştir. Rekabet gücü zayıflamıştır. Ancak tekstil, inşaat ve turizm gibi birkaç sektörle ekonomik girdiler arttırılmaya

çalışılmıştır. Teknolojiye, yeniliğe, üretime ve dünya pazarlarında rekabete dayalı bir ekonomik sistem yerine esasî ithal ikamesine dayalı, faiz ve döviz tabanlı, üretimi değil tüketimi destekleyen sistemsizlik ekonomik yapıya egemen olmuştur. Yüksek enflasyon ve faiz sarmalı bir yandan sanayicinin yapacağı yatırımların önünü keserken diğer taraftan toplumsal yapıda sahip olunan değerler de yıpratılmaya başlanmıştır. Yolsuzluklar çoğalmıştır. Büyüme hızlarında dönemsel büyük düşüşler yaşanmış, milli gelir azalmış, iç ve dış borç çoğalmış, gelir dağılımı bozulmuştur. Nihayet 90'lı yılların ikinci yarısından itibaren ülkenin toplumsal yapısını ve devlet düzenini de etkileyen büyük ekonomik krizler ardı ardına çıkmaya başlamıştır. Doğu blokunun çökmesiyle Türkiye'nin küreselleşme süreci içerisinde ele geçirdiği fırsatlar iyi değerlendirilememiştir.

Aslında eksik olan şey planlı bir yenilenme stratejisidir. Halbuki çalışmalar 1980'li yılların başında başlamış; 4 Ekim 1983 tarih ve 18181 sayılı Resmi Gazete'de yayınlanan 77 sayılı Kanun Hükmünde Kararname ile kurulan Bilim ve Teknoloji Yüksek Kurulu, 3 Şubat 1993'te yaptığı ikinci toplantısında 1993-2003 yılları arasında Türkiye'nin bilim ve teknoloji politikalarını belirleyerek, ulaşılması gereken hedefler ortaya koyulmuştur. (Başbakanlık Genelgesi, 1993, s. 2).

- 10 000 nüfusa yüzde 7 olan bilimsel araştırmacı sayısını yüzde 15'i aşması,
- ARGE harcamalarının, gayri safi milli hasıla içerisinde binde 33 olan payının yüzde 1'i aşması,
- Ülkemizin evrensel bilime katkı açısından, sıralamasında kırkinci sıradan otuzunculuğa çıkarılması,
- Ülke ARGE harcamaları içindeki özel sektörün payının yüzde 18'den yüzde 30'a çıkarılması

Bu rakamsal hedeflerin yanı sıra ülkeye kazandırılması gereken yetenekler kapsamında ileri teknolojiler olarak şu alanların öncelikli gelişiminin sağlanması da kararlaştırılmıştı (Gök, 1999, s. 39).

- Bilişim teknolojileri (bilgisayar, mikroelektronik, telekomünikasyon teknolojilerinin bileşimi)
- İleri teknoloji malzemeleri
- Biyoteknoloji
- Nükleer teknoloji
- Uzay teknolojisi

Bilim ve Teknoloji politikasına ulaşma yolunda alınması gereken tedbirler ise dört ana başlık altında sıralanmıştır (Gök, 1999, s. 39):

- Parasal kaynağın yaratılması
- İnsangücü kaynağının yaratılması
- Özel kuruluşların ARGE harcamalarındaki paylarının arttırılması
- Dünyadaki bilim ve teknolojiye katkı düzeyinin arttırılması

Bu suretle resmi bir belge haline getirilen Türk Bilim ve Teknoloji Politikasına ilişkin esaslar, 1995 yılı içerisinde TBMM tarafından kararlaştırılan Yedinci Beş Yıllık (1996-2000) Kalkınma Planı kapsamına da dahil edilmiştir. Böylece tesbit edilen politika gereğince adımların atılmasına imkan sağlanmıştır (Gök, 1999, s. 40):

- Türkiye Bilimler Akademisinin kurulması (1993)
- Dünya bilim literatürüne katkıya yönelik teşvik uygulamalarının TÜBİTAK tarafından yürürlüğe konması (1993)
- Türk Patent Enstitüsünün kurulması (1994)
- Patent haklarının korunmasına yönelik yasal düzenlemeler (1995)
- Faydalı Model Belgesinin yürürlüğe konması (1995)
- Endüstriyel tasarımların korunmasına yönelik yasal düzenlemeler (1995)
- Yazılım alanındaki fikri mülkiyet haklarının Fikir ve Sanat Eserleri Kanunu kapsamına dahil edilmesi (1995)
- Proje bazlı ARGE faaliyetlerine mali kaynak sağlamaya yönelik Para Koordinasyon Kurulu ve TTGV'ca yapılan teşvik ve kredi düzenlemeleri (1996-1997)

Sözkonusu kurul 1997 yılında üçüncü kez toplanarak; bilim ve teknoloji politikasının sistem bütünlüğü içerisinde değerlendirilerek bir bütünlük içerisinde yürütülmesini temin maksadıyla 29 konuda karar almıştır. BTYK'nun 1998, 1999, 2000 ve 2001 tarihlerinde yaptığı toplantılarda ise üçüncü toplantıda alınan kararlar ile ilgili uygulamaları ve gelişmeleri değerlendirilmiş ve yeni kararlar alınmıştır. BTYK'nun yaptığı çalışmalar aslında ülke gündeminde olmayan bir konunun ele alınması ve ülke bilim ve teknoloji kapasitesinin geliştirilmesi açısından atılan bazı adımlara öncülük yapması bakımından oldukça önemlidir. Ancak politikaların hayata

geçirilmesindeki gecikmeler ve kurumsallaşma yönünde adımların eksik atılması bilim teknoloji politikaları uygulama zaafiyetleri olarak karşımıza çıkmaktadır.

Bilim ve teknoloji politikalarının tespit ve uygulama aşamalarında değerlendirilmeye alınması gereken temel ilkeler bulunmaktadır.

- Kapsamlı bir bilim ve teknoloji politikasının hazırlanması, bunun için idari ve hukuki tedbirlerin alınması; devletin sorumluluğundadır.
- Politikalar bir sistem bütünlüğü gerektirdiğinden devlet, üniversite ve endüstrinin işbirliğini sağlayacak düzenlemeler esastır.
- Kısa vadeli ihtiyaçlar olsa bile, uzun vadeli hedeflerin seçilmesi ve bu hedeflerin uzun süre desteklenmesi zorunludur.
- Toplumun her kademesinde politik irade ve kararlılık lazımdır.
- Kurulacak bilim ve teknoloji sisteminin periyodik olarak performansının değerlendirilmesi ve buna göre yeni düzenlemelere gidilmesi şarttır (Özdeş, 1999).

Türkiye'nin Bilim ve Teknoloji Politikalarının uygulanabilir bir düzeye getirilmesi ve sürdürülebilir bir toplumsal kalkınma projesinin hayata geçirilebilmesini sağlamak maksadıyla nelerin yapılabileceğine ilişkin hususları kısaca ortaya koyabiliriz (Duna, 1996, s. 226):

Bilim ve Teknoloji Politikaları Türkiye'nin makroekonomik politikalarının bir parçası değildir. Planlı kalkınma planlarında önemi derecesinde yerini almalıdır. Ancak sadece teoriye dayanan ifadeler yerine pratikte uygulanabilir ve sonuç alınabilecek projeler olarak ifade edilmelidir.

Bilim ve Teknoloji Politikalarının politik platformda da söz sahibi olmasını sağlayacak yaklaşımlar ortaya konulmalıdır. Bu yaklaşımların en önemli itici gücü sivil toplum örgütleri olmalıdır. Özellikle teknoloji geliştirme amaçlı örgüt, vakıf ve derneklerle, stratejik düşünce kuruluşları bu doğrultuda siyasi mekanizmayı harekete geçirebilecek baskı grupları oluşturmalarıdır. Bilim ve Teknoloji Yüksek Kurulu'nun kabul ettiği kararlar ve teknoloji hedefleri kamuoyuna bu suretle iletilmeli ve benimsenmelidir.

Devletin AR-GE'ye ayırdığı katkının ciddi ölçülerde artırılması ve önceliğinde özel sektöre verilmesi sağlanmalıdır. Stratejik tasnifi yapılmış sektör ve alt

sektörlerde devlet teknoloji kullanma ve üretme ölçütlerine göre teşvik, vergi iadesi, risk sermayesi yatırımlarının desteklenmesi, eğitim desteği, kamu ihalelerinde rekabet avantajı gibi imkanları bu belirlenmiş alanlarda faaliyet gösteren özellikle küçük ve orta ölçekli firmalara sağlamalıdır (Kaymakçalan, 1999, s. 109-111).

AR-GE kurum ve kuruluşları arasında işbölümü yapılmalıdır. Üniversiteler temel bilimsel ve uygulamalı araştırmalarda odaklaşırken, kamu araştırma kuruluşları uygulamalı araştırmalar, destek hizmet ve teknolojileri, jenerik teknolojiler ve rekabet öncesi teknolojilere yönelmeli, özel sektör kuruluşları ise mülkiyetli teknolojiler üzerinde yoğunlaşmalıdırlar.

Lisansüstü öğrenim için yurtdışına gönderilecek öğrencilere ilişkin kontenjanların büyük bir bölümü matematik, fizik, kimya, biyoloji v.b. fen bilimleri eğitimi ile bilgisayar destekli eğitim, eğitim teknolojileri ve yabancı dil eğitimi alanlarına ayrılmalıdır. Bu organizasyon ayrı bir çatı altında toplanmalı; öğrenci seçme ve yerleştirme ve takibi; hazırlanacak istihdam ve personel temin planları ile desteklenmelidir.

Yüksek öğrenimde okullaşma oranının artırılması bir zorunluluktur. Geliştirilecek eğitim politikaları ile özellikle teknik eğitime yönelmiş ve ortaöğretim ile ilişkili bir yapılanma ortaya konularak ülkenin genç beyin potansiyeli harekete geçirilmelidir.

Teknoparklar, teknoloji üretim merkezleri, organize teknoloji merkezleri gibi teknoloji alanında faaliyet gösteren kurum ve kuruluşların sayısı artırılmalıdır. Teknoloji ile ilgili faaliyet alanları bir tür serbest bölge haline getirilmeli ve merkezîyetçi yapıdan ziyade özerk bir yönetim tarzına sahip olmalarına imkan sağlanmalıdır.

Yukarıda sayılan önerilerden bir ya da birkaç tanesinin hayata geçirilebilmesi maksadıyla, devlet içerisinde siyasi karar mekanizmasını etkileyebilen ve yürütme fonksiyonlarına sahip, bilim ve teknoloji politikalarının kurumsallaşmasına yönelik, bakanlık düzeyinde bir teşkilatlanmaya gidilmelidir.

Bilimsel bilgi; küresel ticari rekabette kritik hüviyeti nedeniyle stratejik bir özellik kazanmış, küresel güçlerin adeta odak noktası haline gelmiştir. Tüm politikaların

sağlıklı bir şekilde hayata geçirilmesi; ancak kısa ve uzun vadeli “Milli Bilim ve Teknoloji Politikalarının” oluşturulması ve aksaksız yürütülmesine bağlıdır. (Ayhan, 2002, s. 308).

Organizasyon, kurumlaşma ve entegrasyon; insan kaynaklarımızın yeni devriminin ateşini yakarak, ülkemizin uluslar arası toplumda hakettiği yeri almasına vesile teşkil edecektir. Milli gücün tüm dinamiklerini harekete geçirecek ilim çevresinin karar mekanizmalarını yeni, yarışmacı ve araştırmaya dayalı projeler üretmesi, Türkiye’nin özlemle ihtiyaç duyduğu hayati gereksinimler olarak mütalaa edilmektedir. Türkiye’yi yirmibirinci yüzyıla taşıyacak temel ARGE stratejilerini daha fazla zaman kaybetmeden ortaya koymalıyız. Türkiye, Bilgi Teknolojileri devrimini yaratacak insan gücü, alt yapı ve potansiyele sahiptir. Ülkemiz zengin doğal kaynaklara sahip olmayabilir, ancak yirmi birinci yüzyıla yön verecek esas maden cevherlerine, yani araştırmacı insan yeteneğine sahiptir (Caşın, 1999, s. 26).

Bu düşüncelerinden hareketle Bilim ve Teknoloji Politikaları stratejik bir yaklaşımla yeniden ortaya konulmalı ve ülke kalkınmasının odak noktası haline getirilmelidir.

4.5. Dünya Devletlerinin Bilgi Savaşı Potansiyeli

Günümüzde dünya üzerinde bilgi savaşını icra edebilecek olan devletlerin sayısı çok fazla değildir. Çünkü bilgi savaşını yürütebilmek için bir ülkenin hem bilgi sistemlerini kendisinin üretebileceği bir teknolojiye hem de stratejik seviyede bir planlamaya ihtiyacı vardır. Bilgi savaşına karar veren bir ülkenin kendi sistemlerini koruyacak ve dışarıdan gelebilecek bir müdahaleyi engelleyebilecek teknolojik altyapıya da sahip olması gerekmektedir. Bilgi savaşının araçları hedef ülke tarafından da teknolojinin satın alınması veya teknoloji transferi yoluyla elde edilebilir. Bu kapsamda herhangi bir devletin bilgi savaşı potansiyelini incelerken bunu hem saldırı hem de savunma potansiyeli değerlendirilmelidir. Bilgi savaşı potansiyeli, bir ülkenin;

- Sahip olduğu teknolojinin bilgi savaşını yürütmeye imkan sağlayıp, sağlayamadığı, yazılım yeteneğine sahip olup olmadığı
- Bilgisayar ve bilişim teknolojisinin dışa bağımlı olup, olmadığı
- Dışarıdan silah ithal edip, etmediği veya silah satışı yapıp yapmadığı

- Milli bilgi güvenliğine yönelik tedbirleri uygulama yeteneğinin olup olmadığı sorularına verilebilecek cevaplarla ortaya konulabilir.

Ayrıca bilgi savaşının gizli yürütülmesi, henüz tam anlamıyla literatüre girmemiş olması ve kavramsal bir nitelik içermesi bu potansiyelin değerlendirilmesini devletlerin genel teknolojik seviyesine, elde edilen kısmi istihbaratlara ve yorumlara bağlı kılmaktadır. Bu bölümde yukarıda sayılan faktörleri değerlendirerek; ABD, Çin, Fransa, İngiltere, Almanya gibi dünyada güç dengesini oluşturan ülkelerle, Rusya, Yunanistan ve İsrail gibi ülkemize yakın tehdit oluşturabilecek ülkelerin bilgi savaşı potansiyellerini değerlendireceğiz (TSK Bilgi Harbine Nasıl Hazırlanmalıdır?, s. 62-68):

4.5.1. Amerika Birleşik Devletleri

Bilgisayar teknolojisinin toplumsal hayatın her alanında uygulamaya sokan ABD, bilgi savaşı kavramının ilk ortaya çıktığı ülkedir. Askeri alanda da bilgisayar teknolojisine bütün birimlerine yerleştiren ABD, ordusunun klasik savaş anlayışını kökünden değiştirerek bilgi savaşının öncüsü olmuştur. ABD Savunma Bakanlığı söz konusu savaşın metotlarını uygulayarak, düşmanın haberleşme, komuta kontrol merkezleri ve askeri, ekonomik, sosyal sistemlerini tek bir mermi harcamadan etkisiz hale getirmenin planlarını yapmaktadır. Bilgi teknolojisini yoğun olarak kullanan ABD Ordusu gelecekteki savaşı bir bilgisayar oyunu oynar gibi ekran başında kazanmayı hedeflemektedir. Nitekim ABD Ordusu bu düşüncelerin ışığında 1991 yılında Körfez Savaşında geleceğin savaşının bir tasarımını gözler önüne koymuştur. Bu savaşta bilgi tabanlı sistemler bilgisayar desteğiyle savaş alanına transfer edilmiş, savaş alanının bilinmezlik, düzensizlik ve risk dolu ortamı karar verici komutanların önüne matematiksel ifadeler ve taktik şablonlar halinde konulmuştur. Olaylara eşzamanlı olarak müdahale edilmiş, daha esnek bir taktik anlayışla kararlarda hız ve doğruluk elde edilmiştir. Diğer savaşlara göre daha küçük ve daha az maliyete sahip bir savaş gücüyle neticeye gidilmiştir. Kendisi savaş alanındaki olaylara anında müdahale edebilirken Irak ordusu körleştirilmiş, iletişim imkanlarına müdahale edilerek sağırlaştırılmıştır. Daha savaşın ilk gününde cephedeki Irak birlikleriyle onları yöneten komuta merkezleri arasındaki haberleşme bağlantısı kesilmiş ve yoğun bir psikolojik hareketle Irak ordusunun savaşma azim ve iradesi çökertilmiştir. Körfez savaşının diğer bir farkı da lojistik alanda olmuştur. Bilgi tabanlı malzeme

yönetim sistemi ile 10 000 km. uzaklıktaki kaynaklar ABD Ordusunun kullanımına sunulmuştur. Uluslar arası kamuoyu desteğinin sağlanması maksadıyla medyanın etkili kullanımı ve savaşın dünya kamuoyunca desteklenmesi ile siyasi ve psikolojik üstünlük sağlanmıştır. Uydu ve hedef tespit araçlarının kullanılması ile silahların vuruş etkinliği artırılmış, bunun yanı sıra Irak Ordusunun hareketleri anlık olarak izlenebilmiştir. Körfez Savaşının sonucunda tüm dünya ABD'nin bilgi savaşı imkan kabiliyetine sahip olduğunu açıkça görmüştür. Kosova ve Afganistan savaşlarında da Körfez savaşında denediği bu imkan kabiliyetini savaş alanına süren ABD'nin bilgi savaşı hususunda lider ülke olduğu bir gerçektir. Ancak bilgi savaşı stratejisini oluştururken gidilen yolda ABD'nin de zayıf olduğu noktalar vardır. Alvin Toffler'in

“ Dünyada hiçbir ülke bilgi varlıklarının kaybı karşısında ABD kadar hassas değildir. Zira dünyada hiçbir ülkenin ABD kadar kaybedecek bilgi birikimi yoktur” (Toffler, 1995, s. 56) sözleri bu gerçeği vurgulamaktadır.

Kendisine karşı girişilebilecek bir bilgi savaşında kendi bilgi sistemlerinin alabileceği tahribatın derecesini tahmin etmek ABD için de zordur. Geçmişte klasik ve nükleer savaşlara karşı yürütülen caydırıcılık politikasının bilgi savaşında geçerliliği tartışmaya açıktır. Özellikle savaşın değişen yeni yüzü ile düşman kimliğinin değişikliklere uğraması ve bilgi savaşı araçlarının herkes tarafından temin edilebilir oluşu ABD'nin karşısına bilgi savaşında savunma stratejisi geliştirilmesi yolunda en büyük engel olarak çıkmıştır. 11 Eylül saldırılarını gerçekleştiren terörist oluşumlara karşı ABD yönetimince gösterilen tepkinin çok sert oluşunun altında bu gerçeğin göz ardı edilmemesi lazımdır. Söz konusu olayın altında da bilgi savaşının temaları bulunmaktadır. Teröristlerin bilgisayar destekli simülasyon sistemleri yardımıyla jet uçaklarının kullanımını öğrenmesi, saldırıların Dünya Ticaret Merkezi, Pentagon ve Beyaz Saray gibi bilgi savaşının hedef listesinde yer alan stratejik hedeflere yöneltilmesi bize bu konuda ip uçları vermektedir. ABD'nin yüz yüze olduğu başka bir zorlukta bilgi savaşının stratejik planlaması ile ilgili bilgilerin devlet sırrı ve şeffaf yönetim ikileminde nasıl değerlendirileceğidir. 11 Eylül olayından sonra ABD yönetimi tercihini devlet sırrından yana kullanmıştır. Ancak toplumuna tam demokrasi ve sınırsız özgürlük vaat eden bir ülkenin yönetiminin bu tercihi her zaman lehine kullanamayacağı da bir gerçektir.



4.5.2. Çin

Son dönemde ekonomik alanda yaptığı hamlelerini teknolojik alana da yaymayı hedefleyen Çin bilgi savaşının önemini fark eden ülkelerin başında gelmektedir. Dünyanın güç odaklarından biri olan ve “uyuyan dev” olarak nitelendirilen bu ülkenin son dönemdeki teknolojik gelişim çabaları incelendiğinde bilgi sistemleri teknolojisine verdiği önem dikkat çekmektedir. Bu amaçla ülke çapında üç büyük bilgi ağı sistemini kurarak diğer gelişmiş ülkelerle arasındaki farkı kapatmaya çalışmaktadır. Bunlar; Halk Komünikasyon Ağı, Ekonomik Bilgi Ağı ve Çin Eğitim ve Araştırma Ağlarıdır. Çin Elektronik Teknoloji Akademisinde bir grup bilim adamı tarafından yapılan “Çin’in Bilgi Devrimi ve Savunma Güvenliği” konulu araştırmada; bilgi savaşı hazırlığının Çin için gerekli olduğu vurgulanmış, ABD’de yapılan bilgi savaşı ile ilgili uygulamalar örnek verilerek, Milli ve milli savunma bilgi savaşı, stratejik bilgi savaşı, taktik bilgi savaşı, taarruzi bilgi savaşı ve savunma bilgi savaşı başlıkları altında değişik konseptler önermişlerdir.

4.5.3. İngiltere

Toplumsal dokusu yeniliklere pek açık olmayan bu ülkenin 19 ncu yüzyılda yaşadığı “güneş batmayan imparatorluk” hayali hiç bitmemiştir. Muhafazakar yapıda olan ve girişimciliğe gereken önemi vermeyen bir eğitim sistemine sahip İngiltere Batı dünyasının diğer ülkeleriyle kıyaslandığında bilgi teknolojilerinde çokta ileri bir seviyede değildir. Klasik sanayi toplumu özelliklerini kısa dönemde terk edecek gibi görünmeyen İngiltere aslında İkinci Dünya Savaşı yıllarında günümüz iletişim ve enformasyon ilerlemelerinin temelini atmıştı. Ancak İngiliz sanayicileri bu girişimleri fırsata çeviremedi. Ancak parlak geçmişe duyulan özlem İngiltere’yi son dönemde bazı arayışlara yöneltmiştir. Ordusunu yeniden yapılandırma yolunda mesafe alan ve siyasi arayışlarda olan bu ülkenin sanayi toplumuna geçişteki öncülüğünü göz ardı etmemek lazım. Ağır sanayi altyapısı, bilgi birikimi ve toplumsal tecrübesi bilgi toplumuna geçişte İngiltere’ye kılavuzluk edecek ve değişimde avantajlı kılacaktır.



4.5.4. Fransa

Merkezi bir yönetim anlayışının egemen olduğu Fransa İngiltere'den farklı olarak telekomünikasyon ve bilgisayar gibi kendilerini geleceğe taşıyacak teknolojilere büyük ilgi göstermiştir. ABD'nin fazla girmediği ve tarihsel bağları bulunan üçüncü dünya ülkelerine Fransız yapımı bilgisayar ihracatı konusunda çaba gösteren Fransa, aynı ülkelere yeni nesil silah ve savunma sanayi ürünleri de pazarlamaktadır. Uzay teknolojisi ve nükleer teknoloji alanında da dikkat çekici atılımlarda bulunmuştur. Eğitimli bir toplum yapısı, yetişmiş personeli ve günümüz teknolojilerine gösterilen ilgi Fransa'nın avantajlarıdır. Bilgi savaşı potansiyeli mevcut bu ülkenin, uygulamaya konulacak merkezi bir strateji ile gayretlerini bir noktaya yönlterek, bilgi çağını çok kısa bir sürede yakalayabileceği değerlendirilmektedir.

4.5.5. Almanya

Almanya İkinci Dünya Savaşından sonra başlattığı yeniden yapılanma hamlesinin olumlu sonuçlarını tam anlamıyla sanayileşmiş bir ülke ve refah toplumuna ulaşmış bir toplum olarak aldıktan sonra ikinci değişimi başlatarak bilgi çağını yakalama hedefine yönelmiştir. Ancak İngiltere'deki benzer şekilde yeniliğe, üretkenliğe ve girişimciliğe imkan sunmayan; katı ve aşırı uzmanlaşmaya yönelik eğitim sistemi bu hedefe ulaşmada Almanya'ya engel teşkil etmektedir. Özellikle Doğu Almanya ile birleşmesinden sonra yaşadığı ekonomik sorunlar ve yükselen işsizlik oranı Almanya'yı bilgi toplumuna geçişte geciktirici faktörler olarak öne çıkmaktadır. Diğer yandan bilgisayar sektöründeki yaşanan istihdam boşluğunu diğer ülkelerden bilgi işlem uzmanlarına iş imkanı sunarak kapatmaya çalışmaktadır. Sanayi toplumunun lokomotif sektörleri olan kimya, makine mühendisliği, temel metaller gibi alanlarda ise gün geçtikçe verim düşmektedir. Askeri alanda ise tamamen ABD'nin vesayeti altındadır. Küçük fakat modern ordusu tek başına hareket edememekte, NATO ve AB gibi milletler arası kuruluşların karar organlarına bağlı olarak görevler almaktadır. Ancak siyasi alanda Avrupa'nın merkez ülkesi olarak etkin bir rol oynamak istemekte ve AB'de lider ülke konumuna gelmeye çalışmaktadır. Mevcut toplum yapısı ve ekonomik birikimiyle bir süreç dahilinde de olsa bilgi çağına geçişinin kolay olacağı değerlendirilmektedir.



Genel olarak değerlendirildiğinde şu ana kadar durumları ortaya konan devletlerin bilgi savaşını yürütebilecek alt yapıya sahip olduklarını görüyoruz. Söz konusu devletler aynı zamanda dünyanın belli başlı silah satıcıları konumundadır. ABD, İngiltere, Fransa ve Almanya Türkiye'ye silah satan ülkeler durumundadır. Dış silah alımlarının bilgi savaşı açısından hassasiyet oluşturması sebebiyle, bu ülkeler Türkiye ile aralarında belirgin siyasal sorunlar bulunmamasına rağmen, potansiyel tehdit oluşturan ülkeler kapsamında değerlendirilebilir. Bunun yanında bu devletler ile burada potansiyelini değerlendirmedığımız İsveç, Hollanda, Kanada gibi devletlerin rakiplerimize örtülü destek vermek, ülkemize yönelen terörizme arka çıkmak ve komuta kontrol sistemlerimize sızmalar yapmak suretiyle potansiyel tehditler oluşturabileceği unutulmamalıdır.

4.5.6. Rusya Federasyonu

Dünya güç merkezlerinden birini oluşturan ve Türkiye için her zaman potansiyel bir askeri tehdit oluşturan Rusya, Sovyetler Birliğinin dağılmasından sonra pastadan en büyük payı almıştır. Stratejik bölgeleri kontrol altında tutmayı başarmıştır. Ekonomik sorunlarını dış destekle aşmaya çalışmaktadır. Silahlı Kuvvetlerini yeniden yapılandırmakta ve bölgesel krizlerde askeri etkinliğini arttırmaya yönelik aktif bir politika uyguladığı görülmektedir. Dünyanın en büyük silah üreticileri arasındadır. Yüksek oranda eğitilmiş bir toplum yapısına ve büyük bir teknoloji altyapısına sahiptir. Uzay çalışmalarına ara vermeden devam etmektedir. Ekonomik olarak toparlandıktan sonra eskiden olduğu gibi süper güç olma yolunda stratejiler uygulayacağı değerlendirilmektedir. Bilgi savaşına ve geleceğin savaşlarına yönelik bilinç seviyesi yüksektir. Ancak bilgi savaşı tekniklerini ne şekilde uygulayabileceği hususunda bir belirsizlik mevcuttur. Silahlı kuvvetlerini yeniden yapılandırma çalışmaları kapsamında bilgi savaşının silahlarından olan HERF (High Energy Radio Frequency) silahını ürettiği Batılı istihbarat örgütlerince tespit edilmiştir. Tek merkezden yönetilen Silahlı Kuvvetlerini klasik iletişim vasıtalarıyla komuta etmektedir. Denenmiş ve güvenilirliği artırılmış haberleşme araçlarını kullanmayı tercih etmektedir. İstihbarat toplamak için her türlü yöntem denenmekte ve başarılı olunmaktadır. Türkiye üzerinde askeri istihbarat çalışmaları yaptığı bilinmektedir. Emniyetsiz haberleşmemizi çalma ve yerlerini tespit etme imkanı ve kabiliyetine sahiptir. Taktik düzeyde elektronik savaş tekniklerini bize karşı uygulayabilir.



Nükleer güce sahip olan Rusya, füze sistemleri hususunda da kendisini geliştirmiştir. Bu büyük askeri gücüne rağmen, disiplin, moral ve motivasyon bakımından zayıflığı Silahlı Kuvvetlerinin zaafiyeti olarak değerlendirilebilir. Dış tehditler kapsamında da değerlendirildiği üzere Rusya Türkiye'yi her zaman kendisine hedef ülke konumunda görmüştür. Son dönemde Türk-Rus nüfuz alanlarının da birbiriyle çakışması her zaman var olan tehditin kısa vadede olmasa bile, orta vadede bilgi savaşına yönelik faaliyetleri de kapsayacak bir şekilde yeniden ortaya çıkacağının politik göstergeleridir. Türkiye Rusya'nın bilgi savaşı imkan kabiliyetini hem taarruz hem de savunma anlamında dikkatle değerlendirmelidir.

4.5.7. Yunanistan

Türkiye'yi ezeli düşman olarak algılayan ve dış politikası ve ülke stratejilerini bu ana fikir üzerine oturtan Yunanistan, son yıllarda bilgi savaşının özellikle savunma stratejisini oldukça bilinçli olarak hayata geçirmeye başlamıştır. Yakın zamana kadar dünyada üretilen on kriptoyazılımının Yunanistan'a ait olduğu istihbaratı elde edilmiştir. Gerçi bu yazılımları milli imkanları ile üretip üretmediği bilinmemektedir, ancak bu bile bize Yunanistan'ın konuya bakış açısını bizlere göstermektedir. Savunma sanayi alanında özellikle denizcilik faaliyetlerinde bir artış gözlemlenmektedir. Kendi üretimi olan yeni nesil su üstü savaş gemileri üretmeye başlamıştır. Elektromanyetik alanda ticari olarak yatırımlar yapmış olup, bu yeteneğini askeri alanda da kullanabileceği değerlendirilmektedir. Milli Gözetleme Sistemi projesi dahilinde ana karası ile Ege denizinde sahip olduğu adalarda mevcut radar tesisleri ve kontrol postaları arasında bilgi kaçağını engellemek maksadıyla fiberoptik kablolar inşa etmiştir. Bu sayede bilgi kaçağını önemli ölçüde düşürmüştür. Fiberoptik kablolarla ilave olarak gerçek zamanlı radar görüntüsü elde edebileceği, telefon görüşmesi ve data transferine de imkan sağlayan sualtı kablolarını da deniz tabanına, mevkiisi bilinmeyen yerlere döşemiştir. Deniz ve hava birliklerinin birbirleriyle olan emniyetli haberleşmesini sağlayacak sistemler üzerinde projeler yürütmektedir. Bütün bu çalışmalar Yunanistan'ın bilgi savaşı kavramının farkında olarak, bu kapsamda savunma maksatlı bilinçli ve önemli adımlar attığının göstergeleridir. Taarruzi bilgi savaşını uygulayabilmesi uzak bir ihtimal olmakla birlikte, bilgi savaşının araçlarını temin ederek Türkiye'ye karşı kullanma niyetli ülke ve terörist gruplara verebileceği ihtimal dahilindedir. AB'ne üye olduktan sonra

gelişen ekonomisi ve batılı ülkelerin desteği ile bilgi teknolojilerinde orta vadede bir atılım yapması mümkün görünmektedir. Türkiye aynı Rusya'ya karşı olduğu gibi Yunanistan'a karşı da bilgi savaşının hem taarruz hem de savunma yönünü değerlendirmek zorundadır.

4.5.8. İsrail

İsrail bilgi savaşına giden yolda çarpıcı bir örnek olduğu için bu değerlendirmeye dahil edilmiştir. Günümüzde İsrail, Ortadoğu'nun en büyük silah üreticisi konumundadır. Savunma sanayi dünya devletleri ile rekabet gücüne sahiptir. Bilgisayar yazılımı, güdümlü mermi, radar, savaş uçağı, elektronik savaş, elektro optik, mayın robotları, teknolojik donanımlı savaş gemileri, tank ve bilgi destekli savaş taktikleri ile İsrail'in bilgi savaşı imkan kabiliyeti çok yüksek boyuttadır. Kaliteli eğitim bir devlet politikası haline getirilmiş, üstün zekalı çocukları silahlı kuvvetlerine çekebilmek için özel programları uygulamaya koymuştur. Savunma sanayinde ileri teknoloji ve yüksek rekabet gücü ile sağlam bir altyapı oluşturmuştur. Savunma sanayini ülkenin lokomotif sektörü haline getirmiştir. AR-GE'ye kaynak ayırarak, mali kaynağı silah ve silah sistemleri ihracatına dayalı bir silahlanma stratejisi uygulamaktadır. İsrail günümüzde Türkiye'nin de bazı savunma sanayi projelerini de hayata geçirmektedir. F-5 uçakları silah ve sensör sistemi modernizasyonu, tank ve güdümlü mermi ortak üretim çalışmaları kamuoyunca da bilinen projelerdir. Bu günlerde İsrail ile ilişkilerimiz her zamankinden daha iyi ve olumlu seyretmektedir. Ancak dış silah alımlarının bilgi savaşının en hassas alanlarından birisi olduğundan hareketle, teknoloji alanında bizden daha ileride olan İsrail'in ortak projelerde Türkiye'nin bu hassasiyetine yönelik çalışmalar yapabileceği göz ardı edilmemelidir.

ABD, Japonya, AB ülkeleri gibi yüksek teknolojiye sahip ülkelerin toplum yapıları ikinci dalgadan üçüncü dalgaya geçiş aşamasındadır. Bu ülkeler üçüncü dalgaya özgü savaş yöntemlerini kullanabilmektedir. Bugün ikinci dalga ordularına ve toplumlarına sahip ülkelere üçüncü dalga silahlarının kullandığını görebiliyoruz. Medyada ileri teknoloji ürünü silahların kullanılması, Bilgi Savaşı kavramı altında yanlış olarak yorumlanmaktadır. Başta ABD olmak üzere yüksek teknolojiye sahip toplumlar Bilgi Savaşı saldırıları karşısında zayıftır. Çünkü bu toplumlar yüksek oranda elektronik iletişim ve bilgi alışverişi tabanına dayalıdır. Herhangi bir

saldırgan bu bilgi omurgasına düşük maliyet ve basit teçhizatla rahatlıkla saldırabilir. Çünkü;

- İleri teknoloji ürünü teçhizat tüm dünyada kolayca temin edilebilir.
- Bilgi Savaşına yönelik savunma faaliyetleri çoğunlukla teori düzeyindedir, pratiğe indirgenmemiştir.
- Pek çok bilgisayar sistemi savunmasız ve girişlere karşı korumasızdır.
- Saldırganlar sistemleri kırmak ve istedikleri bilgilere ulaşmak için karışık yöntemler kullanmaktadır.
- İnternet üzerindeki saldırılar fiziksel olarak dünyanın uzak yerlerinden kaynaklanabilmektedir.
- Bilgi sistemlerini tam anlamıyla emniyetli hale getirmek imkansızdır.
- Şirketler arası bilgi savaşları sürekli bir şekilde sürdürülmektedir. Bizler sadece çok küçük bir kısmını ancak medya yardımıyla öğrenmekteyiz. Yaşamımızı etkileyen pek çok etki bilinmemekte bir kısmı ise korku veya toplumsal tepkilerden dolayı saklanmaktadır.

4.6. Türkiye’de Bilgi Savaşı Konusunda Mevcut Durum

4.6.1. Savunma Güvenliği

Ülkemiz yüzyılı aşkın bir süreden beri sanayileşme çabası içerisinde. Aynı çaba, ülke sanayinin bir parçasını oluşturan savunma sanayi alanında da gösterilmektedir. Ülkemiz halen ana savunma sistem ihtiyaçlarının %79’unu yurtdışından karşılamaktadır. Türk Silahlı Kuvvetleri’nin modernizasyonu için 2030 yılına kadar 150 milyar dolarlık bir harcamanın yapılmasının planlandığı ve ana sistem bazında yurtiçi üretim oranının yüzde 70’lere yükseltilmesinin hedeflendiği kamuoyuna açıklanmıştır. Bir ülkede savunma sanayinin gerekliliği başlıca iki nedene dayanmaktadır (Esenergül, 2000, s. 72):

- Birincisi; ülke güvenliğinin sağlanması için silahlı kuvvetlerin özellikleri gizli olan ve yüksek teknolojiler içeren savunma sistemleri ile donatılması,
- İkincisi ise; büyük boyutlarda kaynak gerektiren savunma ihtiyaçlarının ülke içinden karşılanarak ekonomik ve sosyal fayda sağlaması yanında ülkenin bilim, teknoloji ve sanayi yeteneklerinin yükseltilmesine katkıda bulunmasıdır

Ülkemize yönelik tehditlere karşı caydırıcı olabilmek için çok iyi eğitilmiş ve modern silah sistemleriyle donatılmış silahlı kuvvetlerle birlikte, bu silah sistemlerini üreten ve sürekli harbe hazır halde tutulmasını sağlayan güçlü ve milli bir savunma yapılanmasına ihtiyaç vardır.

Günümüzde savunma sistemlerinde gizlilik, güvenilirlik, esneklik, desteklenebilirlik ve standartlık gibi temel kriterler aranmaktadır. Savunma sistemleri, ileri teknolojiler kullanılarak geliştirilmekte ve üretilmektedir. Bu nedenle bir ülkenin savunma gücü, teknolojik düzeyi ile doğru orantılıdır. Dolayısıyla ülkenin milli teknoloji yeteneğinin yükseltilmesi, savunma ihtiyaçlarının karşılanmasında öncelikli amaçlardan biri olmaktadır. Teknolojinin süratle gelişmesi (eskimesi), tehditteki belirsizlikler, iletişim hatlarının emniyeti ve yüksek maliyet savunma harcamalarının kapsamını değiştirmiştir. Son dönemde savunma sanayi üretim faaliyetlerinde yazılım, donanımdan daha önemli hale gelmiş ve bunun sonucu olarak klasik ana silah sistemlerine sahip olma geleneği değişmiştir. Bu anlayışa paralel olarak, gerek elde bulundurulana gerekse temini planlanan silah, gereç ve silah sistemlerinin bilgi savaşı kapsamında bilgi güvenliği altyapısının sağlanması maksadıyla Genelkurmay Başkanlığı'nın girişimleri ve yönlendirmeleriyle;

- Gebze'de TÜBİTAK bünyesinde Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü (UEKAE) kurulmuştur.

- UEKAE bünyesinde Kripto Analiz Merkezi kurularak milli kriptoloji algoritması üretilmiştir.

- Yine UEKAE bünyesinde TEMPEST (Elektromanyetik Sızıntı) Test Laboratuvarı kurularak, gizlilik dereceli bilgideki sızmaların tesbitine başlanmıştır. Bilginin kağıt ortamından elektronik ortama taşınmasıyla birlikte, bilginin güvenliğine yönelik çok değişik tehditlerde gündeme gelmiştir. Bunlardan bir tanesi de, ilk kez ABD'de 1950'li yıllarda fark edilen elektromanyetik sızıntı yoluyla bilginin elde edilmesidir. Elektromanyetik sızıntıların oluştuğu noktadan çok uzaklara yayılabilmesi, sızıntının oluştuğu "Bilgi Teknolojisi Cihazının" işlediği bilginin açığa çıkmasına yol açabileceğinden bilgi güvenliğine yönelik bir tehdit oluşturmaktadır. TEMPEST (Temporary Emanations and Spurious Transmission), gizlilik dereceli bilgi işleyen elektrikli ve elektronik teçhizatın istenmeyen

sızıntıları ve bu sızıntıların araştırılmasını ve incelenmesini ifade etmektedir. Bazen “bilgi içeren kaçaklar” ile eş anlamlı olarak kullanılır. (TEMPEST testi, TEMPEST araştırması gibi) “Bilgi içeren kaçaklar” (Compromising Emanations); ele geçirilip analiz edildiğinde iletilen, alınan veya herhangi bir bilgi işleyici cihaz tarafından kullanılan bilgileri ortaya çıkaran, veri ile ilgili veya bilgi içeren işaretler olarak tanımlanmaktadır. Diğer bir deyişle; haberleşme ve bilgi sistemlerinde kullanılan teçhizattan, çalışmaları sırasında oluşan veri ilintili elektromanyetik kaçaklardır. TEMPEST terimi, elektromanyetik formdaki bilgilerin korunması ve bu bilgileri işleyen elektromanyetik karakterdeki sistemlerin ve bu sistemlere ait yardımcı birimlerin bilgi emniyeti açısından ne derecede güvenilir olduklarının her zaman doğrulanabilecek ölçümlerle test edilmesi ve bu testler ile ilgili yöntemleri de içerir. “TEMPEST Karşı Tedbirleri” (TEMPEST Countermeasures) terimi ise; bilgi içeren kaçakların, ulaştığı alanlarda yetkisiz kişilerce elde edilmesini önlemek maksadıyla alınan tedbirlerin bütünü olarak tanımlanmaktadır (Salcan, 2001, s. 64-65).

- Türk Silahlı Kuvvetleri’nde kullanılmakta veya kullanılacak olan tüm kriptoteçhizatının gizlilik derecesi değerlendirecek sertifikasyon hizmeti yürürlüğe konmuştur.

- Yabancı kriptoteçhizatları yerine milli kriptoteçhizatı üretimine geçilmiştir.

Türkiye’nin bilgi savaşı ile ilgilenmesi için bir çok nedenler mevcuttur. Körfez Savaşı bir savaş organizasyonunda bütün bilginin bir yerde ve tam parmakların ucunda olması gerektiğini dikte etmiştir. Bilgi anlık olarak ve çok sık kullanılmaktadır. Bilgisayar tabanlı cihazlar sadece askeri kullanım için gelişmemektedir. Ticari bilgisayar ürünleri askeri faaliyetlerin her yerinde kullanılmaktadır. Açıklık ve bilginin serbestliği açısından her türlü bilginin İnternette yer alması şahıslar ve sivil organizasyonlarında bu bilgilere ulaşımına imkan sağlamaktadır. Askeri sistemlerin sivil bilgi iletişim alt yapısı tarafından desteklenmesi olgusu bir zorunluluk haline gelmiştir. Türkiye’nin bugünkü bilgi iletişim altyapısının esasını Türk Silahlı Kuvvetleri’ninkini dahil Türk Telekom’un sağlamış olduğu iletişim ortamı teşkil etmektedir. Bu ortamı oluşturan telefon hatları, kablolar, uydu, mikrodalga sistemler, telsizler hatta cep telefonları dinlenmeye, sızmalara ve manipülasyona karşı hassas olup, yeterli derecede güvenliğe sahip olduklarını söylemek zordur.

4.6.2. Haberleşme Güvenliği

Bir düzenleyici kuruluşun genelde yerine getirmesi beklenen işlevleri arasında lisans verme, ağlararası erişimin düzenlenmesi, son kullanıcı fiyatların oluşması, yaygın ve adil hizmet (evrensel hizmet) sağlanması, işletici sorumlulukları ve yükümlülüklerinin tespiti, denetleme, cezalandırma ve uyuşmazlıkların çözümü, iletişim politikaları ve bunların toplumsal sürdürülebilir gelişme boyutlarına ilişkin araştırmalar yapılması, rekabetin düzenlenmesi, frekans kuşağı yönetimi, sahiplik düzenlemelerinin yapılması ve tüketici haklarının korunması bulunmaktadır.

Türkiye’de bu alanda RTÜK, TGM, HGM, Haberleşme Yüksek Kurulu bulunmaktadır. Bu düzenleyici kuruluşların yetkileri arasında mevzuattan kaynaklanan karmaşa bulunmaktadır. Bu durum geleneksel kitle iletişim araçlarıyla sayısal iletişimin ve bilgisayarların tümleşimi (entegrasyonu) eğilimi karşısında daha da şiddetlenecektir. Örneğin RTÜK ile TGM’nin görev ve sorumluluk alanlarında çakışma bulunmaktadır. Kanun koyucu bu durumu bir ölçüde RTÜK’ü güçlendirerek ve bu kuruluşa TGM’ye görev verme yetkisi tanıyarak aşmaya çalışmıştır. Ancak bu yetkilerdeki içiçeliği yok edememektedir. Örneğin TGM’nin kurulmasını sağlayan ve yetkilerini düzenleyen Telsiz Kanunu’nda öngörülen Haberleşme Yüksek Kurulu’nun radyo ve televizyon vericilerine ilişkin olarak vereceği idarektiflerinl. RTÜK kararlarıyla çatışması olasılığı her zaman bulunmaktadır. Radyo Televizyon Kanunu’nda boşlukta veya kablo, cam iletken ve benzeri bir fiziki ortamda ışık hızı ile yayılan, suni olarak üretilmiş elektrik ve manyetik özellikleri olan dalgalar, elektromanyetik dalga olarak tanımlanmaktadır. Böylece, her türlü iletişim bir anlamda bu kanun çerçevesine girmektedir. Her ne kadar, kanun, kendini radyo ve televizyon yayınlarıyla sınırlamaktaysa da neyin radyo/televizyon yayını olduğu konusunda anlaşmazlıklar çıkmaktadır. Nitekim, sayısal televizyon yayıncılığına ilişkin ön çalışmalar çerçevesinde RTÜK, İnternet üzerinden yapılan radyo ve televizyon yayıncılığına ilişkin düzenlemelerinde ele alınmasına karar vermiş durumdadır. Sayısal televizyon yayıncılığına ilişkin başlatılan ön çalışmalar çerçevesinde, sayısal yayıncılığın bağımsız veri iletimini sağlayacağını belirtmektedir. Bu düzenleyici kuruluşlar içinde yalnızca RTÜK içerik denetimine ilişkin görev ve yetkilerle donatılmıştır. Yeni gelişen ağ sistemleri açısından önemli sorunların olduğunun göstergesi İnternet’e ilişkin kurallar bütünü olabilir. İnternet

teknolojilerinin zaman içerisinde gelişmesi ile, her türlü yayıncılık, iletişim ve enformasyon hizmetlerinin tümünün böyle bir ağ üzerinden verilmesi olasılığı, bu alanla ilgili düzenlenmelerin önemini daha da artırmaktadır. Yaygın, adil hizmet sağlanması ve tüketici hakları alanlarındaysa neredeyse hiçbir düzenleyici kuruluş, etkinliğe sahip değildir. Türkiye’de telekomünikasyon alanının bugüne dek kamu hizmeti olarak algılanması ve PTT’nin bu görevi yerine getiren bir kuruluş olması nedeniyle ayrı düzenlemelerin yer almaması yaygın ve adil hizmet kavramının bir yana bırakılmasını gerektirmemektedir. Dünyada gelişmeler çerçevesinde bu konuda evrensel hizmet standartları ayrıca ele alınmaktadır. Sonuç olarak Türkiye’de düzenleyici yapılar açısından önümüzdeki döneme ışık tutacak ilkeler şunlardır:

- Düzenleyici yapılar arasında yetki ve görevlere ilişkin karışıklık olmamalıdır.
- Geleneksel kitle iletişimiyle enformatik teknolojilerin bütünleşmesi nedeniyle tüm işlevler tek bir yapı tarafından en etkin olarak sağlanabilir.
- İçerik düzenlemeleri konusundaki yapılanmalar bir yandan geleneksel radyo ve televizyon yayıncılığında uluslararası standartlardaki kalitede yapılmalı bir yandan da İnternet gibi enformatik ağlara ilişkin içerik denetimi farklı bir düzlemde ele alınmalıdır.
- İşlevler günlük siyasi etkilenmelere kapalı olmalı, ancak düzenleyici işlevlerin tamamının ve telekomünikasyon alanında rekabeti artırmaya yönelik olanların kamu çıkarı, milli güvenlik, yakın coğrafyalarda etkinlik, milli teknolojiyi geliştirme, bilgi toplumuna geçiş, kamu hizmeti, yerli enformatik sanayinin geliştirilmesi, toplumun her kesiminin erişiminin sağlanması ve sürdürülebilir sosyo-ekonomik gelişme amaçlarına uygun olmasının sağlanması gerekmektedir.
- Ağlar arası erişimin düzenlenmesinde maliyet kavramının tanımlanması gerekmektedir. Türkiye, Türk Telekom’un maliyetinin ne olduğuna ilişkin konsepti tanımlamalıdır. Bu konsept günlük siyasi çekişmeler dışında tutulmalıdır.
- Düzenleyici yapılanmaya parasal kaynak yaratmalıdır.

4.6.2.1. Radyo Televizyon Yüksek Kurulu (RTÜK)

Özel televizyonları denetim altına almak ve bunların siyasi tarafsızlığını sağlamak kaygısından kaynaklanmıştır. Özerk ve tarafsız bir kamu tüzel kişiliği niteliğindedir. RTÜK, 1994 yılında yürürlüğe giren 3984 sayılı Radyo ve Televizyonların Kuruluş ve Yayınları Hakkında Kanun çerçevesinde oluşturulmuş

düzenleyici bir kurumdur. Söz konusu kanun, "her türlü teknik, usul ve araçlarla ve her ne isim altında olursa olsun elektromanyetik dalga ve diğer yollarla yurt içine ve dışına yapılan radyo ve televizyon yayınları ile ilgili hususları" kapsamaktadır.

Kanunda, "boşlukta veya kablo, cam iletken ve benzeri bir fiziki ortamda ışık hızı ile yayılan, suni olarak üretilmiş elektrik ve manyetik özellikleri olan dalgalar" elektromanyetik dalga olarak tanımlanmaktadır.

Kanun'da geçen ek yayın hizmetleri; "televizyon yayınlarında tahsis edilen kanal içinde kalmakla birlikte kullanılmayan bölümler üzerinden; radyo yayınlarında ise tahsis edilen kanal içinde ek taşıyıcılar aracılığıyla, televizyon ve radyo program yayınlarıyla birlikte yapılan, radyo veri sistemi, veri yayıncılığı, teletekst ve benzeri bağımsız hizmetlerini" kapsamaktadır. Kanun çerçevesinde oluşturulan RTÜK radyo ve televizyon faaliyetlerini düzenlemek amacıyla, özerk ve tarafsız bir kamu tüzel kişiliği niteliğindedir.

RTÜK'ün görevleri kanunda sayılmıştır. Bu görevler arasında şunlar bulunmaktadır:

- Milli ve bölgesel frekans planlamalarını yaptırmak,
- Önşartları yerine getirmiş müracaatçı kuruluşlara tarafsızlık ve hakkaniyet ölçüleri dahilinde yayın izni ve lisans vermek,
- Radyo ve televizyon kuruluşlarına, milli, bölgesel ve yerel yayınları için milli kanal ve frekans bandı planlamalarına uygun olarak tahsis edilen alanlarını kapsayacak verici tesisleri kurma ve işletme iznini vermek ve tesis şartlarının uygunluğunu denetlemek,
- Radyo ve televizyon kuruluşlarının milli ve yerel yayınlarına imkan verecek, milli kanal ve frekans bandı planında öngörülen radyo ve televizyon vericileri ile sabit veya hareketli yayın yerleri arasında mevcut telekomünikasyon şebekesi yanında, uydu aracı ile bağlantı kurabilmeleri amacıyla uç linkleri kurabilmeleri için telekomünikasyon tesislerini kurma ve işletme izni vermek ve tesislerin bu kanunda öngörülen izin esaslarına uygun olarak işletilmesini denetlemek,
- Radyo-televizyon yayınlarını izleme sistemleri kurarak, yayınların yukarıdaki madde hükümlerine ve bu alanda Türkiye'nin taraf olduğu milletlerarası antlaşmalara uygunluğu açılarından denetlenmesini yapmak,

- Yayın kuruluşlarının, bu kanun hükümlerine aykırı yayın yapması ve tahsis şartlarına uymaması halinde, gerekli müeyyideleri uygulamaya karar vermek,
- Yurtiçinde yayınların ulaşamadığı yerlerde, yerel imkanlarla radyo ve televizyon vericisi kurulmasına izin vermek,
- Şifreli yayınlarla kablolu radyo ve televizyon tesis ve yayınları ile ilgili kuralları bu kanundaki ilkeler çerçevesinde ve PTT İdaresi Genel Müdürlüğü'nün kablolu radyo ve televizyon tesislerini atıl bırakmamayı gözeterek belirlemek.

3984 Sayılı Kanun, radyo ve televizyon yayınlarını kimlerin, nasıl, nerede, hangi teknik çerçevede yapabileceğini düzenlemekte ve yayınların ilkelerinin ve içeriğinin denetimini de RTÜK'e vermektedir. Kanunun 24. maddesi, Telsiz Genel Müdürlüğü'nün, radyo ve televizyon yayınlarına esas olan bütün kanal, frekans bantları ve gerekli teknik bilgileri Ulaştırma Bakanlığı kanalıyla RTÜK'e bildireceğini, yapılan tahsisleri uygulayacağını ve teknik bakımdan izleyeceği hükmünü getirmektedir. Üst Kurul'un taleplerinin öncelikle yerine getirilmesinin esas olduğu da kanunda belirtilmektedir.

4.6.2.2. Haberleşme Yüksek Kurulu (HYK)

Haberleşme Yüksek Kurulu (HYK) ve Telsiz Genel Müdürlüğü (TGM) 1983 yılında yürürlüğe giren 2813 sayılı Telsiz Kanunu ile kurulmuştur. HYK, telsiz haberleşmesi alanında genel direktif birimidir. Başbakan'ın veya görevlendireceği bir devlet bakanının başkanlığında, İçişleri, Ulaştırma Bakanları ile Milli Güvenlik Kurulu Genel Sekreteri ve Genelkurmay Muhabere Elektronik Başkanı'ndan oluşan bir üst kuruldur. Görevi, ilke kararları almak ve direktifler vermektir. Yapılan uygulamaları incelemek, değerlendirmek ve yönlendirmek de görevleri arasında bulunmaktadır.

4.6.2.3. Telsiz Genel Müdürlüğü (TGM)

TGM'yi oluşturan kanun, büyük ölçüde, 1980'li yıllarda Türkiye'ye giren halk bandı (CB) telsizlerine ilişkin düzenleme yapılması gereksinmesinden kaynaklanmıştır. TGM ise, Ulaştırma Bakanlığı'na bağlı katma bütçeli bir kuruluştur. TGM Genel Müdürü ulaştırma bakanınca atanır.

2813 sayılı kanunun amacı; "haberleşme maksadıyla kullanılan ve elektromanyetik dalgalar yoluyla açık veya kodlu veya kriptolu ses, data ve resim vermeye veya almaya yarayan her türlü telsiz sisteminin kurulmasına, işletilmesine müsaade edilmesi ve kontrolü ile telsiz haberleşmesi alanındaki politika, hedef ve ilkelerin tespitine ilişkin usul ve esasları belirlemek ve bu konuda gerekli düzenlemeleri yapmaktır."

Telsiz kavramından,"aralarında herhangi bir fiziki bağlantı olmaksızın elektromanyetik dalgalar yoluyla açık veya kodlu veya kriptolu ses, data ve resimleri vermeye, almaya veya yalnızca vermeye veya almaya yarayan sistemler" anlaşılmaktadır.

TGM'nin görevleri arasında şunlar bulunmaktadır:

- Telsiz haberleşmesi ve endüstrisi alanlarındaki araştırmacı ve imalatçı kuruluşlarla da işbirliği yaparak elektronik ve elektromanyetik teknolojideki gelişmeleri takip etmek,
- Radyo ve televizyon verici istasyonları dahil olmak üzere her nevi frekans, planlama, tahsis ve tescil işlemlerini takat ve yayın sürelerini de göz önünde tutarak uluslararası kuruluşlarla işbirliği de yapmak suretiyle yürütmek,
- Usulsüz yayınları ve enterferansları izleyen ve tespit eden birimlerle karşılıklı işbirliği yaparak gerekli işlemleri yürütmek.
- Kanun, telsiz alıcı cihazları kapsamında şunları saymaktadır:
- Radyo/televizyon yayınlarını almaya yarayan cihazlar,
- Her çeşit resim, ses, data almaya ve kaydetmeye yarayan cihazlar.

4.6.2.4. Haberleşme Genel Müdürlüğü (HGM)

Haberleşme Genel Müdürlüğü 1926 yılından kalma (HGM) 406 sayılı Telgraf ve Telefon Kanunu'nu değiştiren 4000 sayılı kanunla kurulmuştur. HGM, doğrudan Ulaştırma Bakanlığı'nın örgütü içinde bulunan Haberleşme Daire Başkanlığı'nın genel müdürlük düzeyine yükseltilmesiyle ortaya çıkmıştır. HGM, Ulaştırma Bakanı'ndan alacağı emirleri 406 sayılı Telgraf ve Telefon Kanunu'na uygun olarak yerine getirecektir.

4.6.2.5. Tr-Net Bürosu

Ulusal/Küresel Enformasyon Altyapısı'nın ilk adımı sayılması gereken İnternet'e ilişkin düzenleme TÜBİTAK bünyesindeki TR-NET Bürosu aracılığıyla yapılmıştır. TÜBİTAK'ın yayımladığı TR-NET'te Uyulacak Kurallar şu noktalara dikkat çekmektedir:

- TR-NET kaynakları araştırma, eğitim ve haberleşme amaçlıdır. Ağ kaynakları başka amaçlar için kullanılamaz,
- Ağ üzerinden yolladığınız veya aldığınız mesajlarınızın, mektuplarınızın ve dosyalarınızın başkaları tarafından dokunulmazlığı güvence altında değildir. Bunların güvenliğini sağlamak gönderenin sorumluluğundadır,
- Kullanıcı TR-NET aracılığı ile bağlandığı bir ağ için konulmuş kurallara uymalıdır,
- Rasgele mesaj, tehdit edici ve saldırgan yazı/mesaj göndermek ve TR-NET'i ticari, politik ve dini propaganda için kullanmak yasaktır,
- Ağ kaynaklarını kötüye kullanmak ve zarar vermek yasaktır,
- Kaynakların kullanımını sağlayan TR-NET yönetimi, koyduğu kurallara ve kanunlarına karşı yapılan davranışları ilgili makamlara bildirme hakkına sahiptir. Bu tür davranışlar tespit edildiğinde; kullanıcı hakkı geçici veya sürekli olarak kapatılabilir, yargıya intikal ettirilebilir.

4.6.2.6. Kurumsallaşma Çabaları

Bilgi savaşı kavramının Silahlı Kuvvetler dışındaki devlet kurumlarında henüz çok yeni olmasına karşın özellikle hükümet seviyesinde ciddi çalışmalar da göze çarpmaktadır. Bu kapsamda Türk Silahlı Kuvvetleri'nin önerdiği bir kısım bilgi harbi projelerini üstlenip yürüten ve bu konuda Türk Silahlı Kuvvetleri'nde görevli personele özel eğitim veren bir kuruluş olarak TÜBİTAK'ı da görmekteyiz. Hükümetin direktifleri doğrultusunda Milli Bilgi Güvenliği teşkilatının oluşturulmasına yönelik çalışmalar da başlatılmış, Haberleşme Yüksek Kurulu'nun 4 Eylül 1997 tarihli toplantısında "Genelkurmay Başkanlığı'nın koordinatörlüğünde, İçişleri Bakanlığı, Dışişleri Bakanlığı, MGK Genel Sekreterliği, MİT Müsteşarlığı, Haberleşme Genel Müdürlüğü, Telsiz Genel Müdürlüğü ve Türk Telekom A.Ş. Genel Müdürlüğü'nün katılımı ile bir çalışma grubunun oluşturularak devlet bilgi

güvenliğinin yapılanmasının incelenmesi ve gerekli yasa tasarısının hazırlanmasına” oybirliği ile karar verilmiştir. Bu maksatla oluşturulan çalışma grubuna “Güven Çalışma Grubu” adı verilmiş ve faaliyetlerine başlamıştır.

Güven Çalışma Grubu, kendisine verilen görev çerçevesinde güvenlik alanına ilişkin olarak kurumsal yapılanma önerisi geliştirmiştir. Ulusal Bilgi Güvenliği Üst Kurulu ve Bilgi Güvenliği Kurumu oluşturulması önerilmektedir. Ulusal Bilgi Güvenliği Kurulu’nun temel görevleri arasında bu alanda direktif organı olmak da bulunmaktadır. Başbakan’ın başkanlığında Adalet, Milli Savunma, İçişleri, Dışişleri, Ulaştırma, Ticaret ve Sanayi Bakanları ile Milli Güvenlik Kurulu Genel Sekreterliği, Genelkurmay Muhabere Elektronik ve Bilgi Sistemleri Başkanı, MİT Müsteşarı, TÜBİTAK ve Ulusal Bilgi Güvenliği Kurumu Başkanı’nın katılımıyla oluşması düşünülmektedir. Kurulun görevleri arasında, Ulusal Bilgi Güvenliğine yönelik tehdidi değerlendirmek, bu konudaki politikanın oluşturulması ve uygulamasıyla ilgili kararları almak ve bu konuda Ulusal Bilgi Güvenliği Kurumu’na direktif vermek, uygulamaları incelemek, değerlendirmek ve yönlendirmek ve konuya ilişkin yasa tekliflerini değerlendirmek bulunmaktadır. Görüldüğü gibi bilgi güvenliğine ilişkin olarak gerekli olan işlevlerin tümü büyük önem taşımaktadır. Güven Çalışma Grubu’nun oluşturduğu işlevlerin tamamının yerine getirilmesi gerekmektedir (TUENA Anaplanı Sonuç Raporu, 1999, s. 50).

Konunun milli boyutu ele alındığında diğer kurum, kuruluş ve üniversiteler ile özel sektörün yeterli bilgiye sahip olmadığı ve sorumluluklarının farkında olmadığı görülmektedir. Bilgi Savaşının tabanı olan eğitim alanında da büyük eksiklikler olduğu değerlendirilmektedir.

4.7. Bilgi Güvenliğine Stratejik Yaklaşım

Bu araştırmanın bütününde, yeni çağın temellerinin bir ülkenin güvenlik politikasını hangi kavramlar çerçevesinde şekillendirdiği ve bu altyapıların üstyapılar üzerindeki etkisi ele alınmıştır. Bu bölümde, bilgi güvenlik politikasının nasıl tanımlanması ve yeni doktrinleri hangi kurumsal çerçeveye oturtma çabasını göstermemiz gerektiği stratejik bir yaklaşımla ortaya konulacaktır. Dünyanın içinden geçtiği sürecin artıları ve eksileri değerlendirilerek, burdan çıkarılacak derslerle, geriden gelmenin nasıl bir avantaja çevrilebileceği incelenecektir. Önceki

bölümlerden elde edilen bilgilerin ışığında, Türkiye'nin bilgi çağında oluşturmaları gereken bilgi güvenliğine yönelik doktriner uygulamalar ile ilgili somut bir şablon önerilecektir (Gürçihan, 2002, s. 1-7).

Bilgi kürede oluşan yeni dengeler çerçevesinde, devletler, diğer devletlere karşı aktif güvenlik politikaları uygulamak zorunda kalacaklardır. Bilgi coğrafyasında yaşanan çatışmaların sessiz olma özelliği, bu coğrafyada devletlerin ve devlet dışı unsurların karşı tarafa saldırma ve zarar verme eğilimini artıran bir özellik olmasından dolayı, diğer coğrafyaların aksine bilgi coğrafyası, gelecekte dünyanın en gürültülü coğrafyası olma özelliğini kazanacak; devletler ve devlet dışı unsurlar birbirleri ile sürekli çatışma ve aktif savunma halinde olacaklardır.

Türkiye bu coğrafyanın bilincinde olarak, aktif bir savunma ve saldırı doktrini geliştirmeli ve bilgi çağınının bu yeni güvenlik anlayışını mevcut yapılara eklemek yerine, toplumsal yapılanmasını bu yeni güvenlik doktrini çerçevesinde oluşturmalıdır. Önerilecek olan bilgi çağı güvenlik şablonu aşağıdaki temel esaslara dayanmaktadır:

- Savunma ve Saldırı Politikası
- Yasal Çerçeve ve Toplumsal Mutabakat
- Kritik Altyapılar
- Sivil ve Askeri Siber Güçler
- Stratejik Sektör ve Ürünler

4.7.1. Savunma ve Saldırı Politikası

Bir ülkenin sınırlarına saldırı olduğunda o ülkenin nasıl karşılık vereceği, hangi senaryolara karşı hangi karşı senaryoların uygulanacağı savunma stratejileriyle nasıl tespit edilmiş ise, Türkiye söz konusu olan bu yeni coğrafya için de savunma ve saldırı prensiplerini belirlemek zorundadır. Sıradışı hareketlenme yaşanan bir yabancı birlik, komşu ülkede yaşanan toplumsal kaos, bölgemizde gelişen askeri, ekonomik ve politik paktlar, ülke güvenliği açısından farklı nicelikler ve nitelikler taşıyorsa, sanal coğrafyada yaşanan olayların benzer karşılıkları olacaktır. Bulunduğu coğrafyanın özelliklerini de gözönüne alarak, Türkiye'nin sanal coğrafyadaki konumu çok doğru bir şekilde tespit edilmeli ve karşı karşıya olduğu tehditler en küçüğünden, en büyüğüne kadar doğru şekilde sınıflandırılmalıdır.

Sanal coğrafyada neyin açık bir tehdit, neyin bireysel hareketlere eşdeğer olduğunun tespit edilmesinin ardından; bu tehditlere verilecek cevaplar büyük önem taşıyacaktır. Konu ile ilgili standartların belirlenmesi, sadece sanal coğrafyayı bir düzene kavuşturmak açısından değil, ülke güvenliğinin zaafa uğramaması açısından da büyük önem taşımaktadır. Türkiye, kategorilendirdiği tehditlere, tehdidin boyutu ile doğru orantılı olarak bir savunma ve saldırı politikası geliştirmelidir. Amacı olmayan gayretler sadece kaynakların gereksiz harcanmasına neden olmayacak, bu gayretin gerekli olduğu noktalarda da güvenlik şemsiyesinin incelenmesine neden olacaktır.

Sanal coğrafyada, tehdidin ne olduğu kadar, nerden kaynaklandığı da büyük önem taşımaktadır. Olayın yetenekli bir hacker mı, yoksa bir devlet veya devlet dışı kuruma bağlı olarak çalışan bir hacker ekibi tarafından mı, yoksa bizzat bir devletin resmi biriminin eylemi mi olduğu, verilecek karşılığın belirlenmesinde büyük önem taşımaktadır. Tehdidin boyutundan bağımsız olarak gerçekleştirilecek karşı savunma ve saldırı tedbirleri, karşı tarafın çok daha acımasız bir saldırı gerçekleştirebileceği ihtimali gözönünde tutularak hesaplanmalıdır. Türkiye, sanal coğrafyasına yönelik hangi saldırılar karşısında hangi karşı saldırıları gerçekleştireceğini açıkça beyan etmeli ve bu şekilde caydırıcı gücünün test edilmesini önlemelidir. Sanal ortamda ister devlet dışı unsurlar, ister devlet unsurları arasındaki dayanışmanın çok daha kolay ve esnek kurulabileceği gözönüne alınarak, sivil halka verilecek gereksiz zararlar da hesaplamalara dahil edilerek, tehdit ile doğru orantılı ve daha şiddetli karşı saldırılara yolaçmayacak bir karşı saldırı ve savunma taktiği geliştirilmelidir. Devletin politikaları çerçevesinde, hiç bir saldırı olmaksızın girişilecek siber operasyonların niteliği ve kapsamı ve bu konuda ülkenin kapasitesi ise hiç bir şekilde deşifre edilmemesi gereken bir politika olarak üst düzey gizliliğini korumalıdır.

4.7.2. Yasal Çerçeve ve Toplumsal Mutabakat

Bilgi kürenin sınırları ehil kişi ve kuruluşlar tarafından tanımlanmalıdır. Tanımlama süreci sırasında yapılabilecek eksik tanımlamalara dayalı olarak yasal çerçeve belirlenmeye kalkışılırsa kavram kargaşası artacaktır. Birimlerce oluşturulacak yasalar, bütün için, en iyi ihtimal ile yetersiz, en kötü ihtimal ile alakasız kalacaklardır. Kavramları, oyuncularını, dinamikleri ve diğer bir çok unsuru ile daha yeni yeni ortaya çıkan bir alanın doğal olarak meraklısı da çok olacaktır. Bu

meraklı kitlesi içinde, medyanın da çarpıtıcı etkisi ile, yanlışları en çarpıcı ifadelerle ortaya koyan birinin, doğruları sönük bir şekilde ifade edenler karşısında öne çıkma eğilimi yüksektir. En doğruyu söyleyenin değil, en çarpıcı şekilde söyleyenin prim yaptığı bu çerçevede, kavramları ve dinamikleri bilimsel olmayan bir şekilde tarif etmenin büyük sakıncaları olacaktır.

Türkiye, en başından itibaren, sanal dünya politikalarında ön plana, medyada bu konuda prim yapmış isimleri değil, akademisyenleri ve teorisyenleri çıkarmalıdır. Gazete köşelerinde, toplum karşısından İnternet gibi bir bilinmezi kullanarak kendilerine sosyal prim sağlayan isimlerin genelleyici, sansasyonel, medyatik ve bilimsellikten uzak tavırlarının ülke güvenlik politikasını etkilemesine izin verilmemelidir. Telekulak olaylarında da görüldüğü gibi, Türkiye’de yasalar zaman zaman etki tepki mekanizmaları ile şekillenmektedir. Suç örgütlerinin elektronik izlenmesine yönelik yasa ancak, polisin yasal olmayan metotlarla, başbakanın evinin telefon numaralarını izlemeye aldığıının manşetlere taşınması ile hız kazanarak meclisten çıkmıştır. Gazete manşetleri ile şekillenen bir yasal çerçevenin büyük sakıncaları olacağından, medyada İnternet uzmanı olarak prim yapan isimlere, sözkonusu milli politikalar olduğunda gereğinden fazla prim verilmemeli, bu isimlerle ilişkili çıkar çevreleri iyi tespit edilmelidir.

Türkiye konuyu baştan bütün hedefleri ile ayrıntılı tespit etmeli, hukukçular, akademisyenler, konunun profesyonelleri ve sivil toplum örgütlerinden bir grup oluşturarak, yeni çağın bilgiye dair yasal altyapısını, anayasal tanımlardan teknik ayrıntılarına kadar, medyatik yaklaşımlardan uzak tutulacak bu kurula hazırlatmalıdır.

Unutulmaması gereken nokta, yasaların yazılınca değil uygulanınca hayata geçen varlıklar olmaları dolayısı ile, bu yasal çerçeveyi benimseyen bilince sahip bir toplumun yaratılmasıdır. Yeni yasal çerçevenin getirdiği tanımlarla hayatı değişecek sokaktaki vatandaşın, bu yasaları meclisten geçirecek meclisteki vekiline kadar toplumdaki herkes dijital çağın gerekleri hakkında çocukluktan itibaren eğitilmelidir. Türkiye, henüz daha endüstriyel çağın vatandaşlık bilincini toplumuna kazandıramamış olsa da, hızla vatandaşlar, kurumlar ve devlet arasında bir mutabakat oluşturmali ve bu mutabakat çerçevesinde özellikle yeni nesle dijital vatandaşlık aşlamaya başlamalıdır. Yeni çağla birlikte bir toplumun kritik sınırları

dağlardan, ovalardan bireylerin beyinlerine taşındığından, vatandaşını güvenlik politikasının etkin bir parçası haline getirmeyen bir devlet çok büyük tehlikelere maruz kalacaktır. Türkiye, bu bağlamda, güvenlik politikası için en büyük ortanın müttefikleri değil, milleti olduğunun bilincine vararak, tepeden inen değil, alttan gelen ve gönülden benimsenen bir güvenlik çerçevesi oluşturmak zorundadır. Eğitim sistemi bireyleri bu çağın gerekleri ve bu gerekleri kullanma bilinci ile donatacak şekilde yeni baştan ele alınmalıdır.

4.7.3. Kritik Altyapılar

Türkiye, kendi coğrafi, kültürel ve ekonomik durumunu da gözönüne alan bir çerçevede, kritik altyapılarını milli bir ana plan çerçevesinde tespit etmelidir. Her bir altyapının bütün ile koordinasyonu, devletin güvenlik politikaları çerçevesinde geliştirilmelidir. Olası bir saldırıya karşı yapılandırılacak savunma önlemlerini, olası bir taarruz içinde en etkin şekilde kullanılabilmeleri için bütün olasılıkları gözönüne alan eylem planları oluşturmalıdır. Bütün bu unsurların yürütülmesinden ve denetlenmesinden sorumlu alt ve üst yapılar, önceden belirlenen ve en üst düzeyde takip edilen bir takvim çerçevesinde oluşturmalıdır. Kritik altyapıların belirlenmesi ve sözkonusu yapıların oluşturulması için görevlendirilerek komitelere sadece devlet ve özel sektör temsilcilerini değil, sivil toplum örgütlerini de katmalı, onları da etkin bir şekilde bu işin içine sokmalıdır. Radyolink istasyonlarını uluorta, her taraftan etkiye açık bir şekilde kuran, iletişim sektöründen tutun da, F-16'larının elektronik sistemlerini bile, etkili bir şekilde denetleyemediği, yabancılara yaptıran bir savunma sektörüne sahip bir ülkenin, sanal çağ ile ilgili teknik reformlardan çok düşünsel reformlara ihtiyacı vardır. Türkiye, savunma sanayindeki bağımlılığını sanal coğrafya için de gösterirse; telafi edilemeyecek şekilde kontrolü elinden kaybedecek ve geçmişini mumla aratacak bir bağımlılık sürecine girecektir. Bu süreç bugün oluşan bağımlılığı yarın iki misline çıkaran bir bağımlılık sarmalı olarak, artan bir şekilde yoğunlaşacaktır. Geçmişin bağımlılıklarının getirdiği zararları telafi etmek sadece bir zaman ve maliyet meselesi iken, yeni çağın bağımlılıkları, alınamayan silahlar, uygulanamayan stratejiler, atılmayan adımlardan ibaret olmayıp, bir ülkenin genç nüfusunun düşünce tarzına kadar müdahale eden cinsten olacağı için, telafi edilemez boyutlara varacaktır. Bu bağımlılık sarmalından kopmanın tek yolu, biz nasıl daha iyi yaparız yaklaşımını ortaya koymakla mümkündür.

Türkiye, önceden tespit edilen bir takvim çerçevesinde bütün toplum katmanlarının ortak katılımı ile öncelikle altyapısının ayrıntılı bir haritasını çıkarmalı ve daha sonra bu altyapıyı geliştirmek ve güvenlik politikasına entegre etmenin şablonlarını oluşturmalıdır. Körfez Savaşı sırasında Irak'ın iletişim altyapısının planlarını ABD'ne, Irak'ın telekomünikasyon altyapısını kuran AT&T şirketinin verdiği gerçeği unutulmadan, kritik altyapılar en üst düzeyde milli hassasiyetler içeren bir anlayışla oluşturulmalı, geliştirilmeli ve korunmalıdır.

Türkiye, iletişim çağında benimsenen teknik ve hukuki standartlardan bağımsız olarak, kendi milli standartlarını belirlemeli ve bu standartları gerektiği takdirde tek başına, gerektiği takdirde uluslararası sistem ile entegre şekilde çalışacak bir şekilde dizayn ederek, altyapılarını bu standartlar çerçevesinde inşa etmeli, geliştirmeli ve korumalıdır. Hiç bir şey dışarıdan, sorgulanmadan, incelenmeden, içinde kötü niyetli unsurlar taşıyıp taşımadığına bakılmadan ülkenin içine ve hele hele kritik altyapılarının bünyesine dahil edilmemelidir. Yeni çağın sanal güvenlik mekanizmalarının, Türkiye'nin değişken siyasi hareketlerinden etkilenmemesi için, sözkonusu güvenlik alt ve üst yapıları, hükümet politikalarını değil, devlet politikalarını temsil eden kurumlara bağlanmalıdır. Oluşturulacak bir kurul, bir genel sekreterlik mantığı ile sürekli çalışarak, bu mekanizmaların koordinasyonunu üstlenmeli ve doğrudan yürütmeye yönelik yetkilerle faaliyet göstermelidir.

4.7.4. Sivil ve Askeri Sanal Güçler

Yeni çağla birlikte, ülke güvenliğinde sivil ve asker. ayrımı gittikçe belirsizleşecektir. Teknolojinin gereklerinden veya çağın kültürel, sosyal ve ekonomik dinamiklerinden olsun, ülkelerin güvenlik sınırları beyinlere doğru kaydıkça, bu değişen anlayış, sivillerin ve askerlerin çok daha yoğun bir şekilde işbirliğine girmelerini şart koşacaktır. Büyük patlamalarla bozulan uzun süreli durgunluk dönemleri olarak şekillenen fiziki coğrafyalara ait güvenlik politikalarının aksine, sanal coğrafyanın güvenlik politikaları sürekli küçük sorunların yaşanacağı bir ortama göre hazırlanmak zorundadır. Bu durumda her küçük soruna karşı aktif önlem alınması, devlet güçlerini gereksiz yere bölecek, yıpratacak ve olası bir büyük sorun karşısında ülke savunmasını büyük zaafiyete uğratacaktır. İşte bu noktada, devletin sanal coğrafyadaki küçük sorunların bekçiliğini sivil güçlere bırakıp,

kendisinin bu güçlerin koordinasyonunun sorumluluğunu taşıması ve büyük depremlerin savaşçısı olma konumu koruması büyük önem taşımaktadır.

Sivillerin askeri disiplinden yoksunluğu, sözkonusu işbirliklerinin nasıl yürüyeceği konusunda ciddi kaygılar oluştursa da, bugünün handikaplarının aşılması, geleceğin politikalarını oluşturmak açısından hayati önem taşımaktadır. Dünyada henüz bu açıdan ortaya konulmuş sağlıklı bir örnek bulunmamaktadır. Kendi yetenekli hackerlerini hapishanelerde çürütürken, NSA bünyesinde çalıştırdığı bilgisayar dehaları ile sanal gücünü pekiştiren ABD; Savunma Bakanlığı sistemlerini kıran genci MOSSAD bünyesinde çalıştırmaya başlayan İsrail; komünist gelenekler çerçevesinde sanal güçlerini bile bir devlet departmanı olarak organize eden Çin ve usta bilgisayar korsanlarını mafya ilişkileri üzerinden kendi çıkarları için kiralayan Rusya örnekleri, kurumsallaşmada ders alınması fakat kesinlikle tekrarlanmaması gereken örneklerdir.

Türkiye'nin mevcut ordu geleneği, sözkonusu kaygıları da gözönüne alarak, sanal coğrafyaya doğru geliştirmelidir. Bu maksatla Türk Silahlı Kuvvetleri'nin koordinesi altında oluşturulacak yapı, sanal coğrafyanın büyük sorunları için, toplumun yönlendirilmesi görevlerinin yanısıra, üst düzey savunma ve saldırı yeteneklerini bünyesinde toplayan, askeri disiplinin güvenilirliği ile profesyonel disiplinin yaratıcılığını çok iyi şekilde harmanlamış bir çerçeve içinde hareket etmelidir. Bu oluşum, sanal coğrafyadaki küçük sorunlara karşı mobilize edilecek sivil güçleri, belirlenen filtreler çerçevesinde belli mesafelerde genel yapıya bütünleştirmeli, bir bakıma bu güçlerin standardizasyon ve onay makamı gibi çalışarak, gerekli koordinasyonu sağlamakla yükümlü olmalıdır. Türkiye'nin genç nüfusunun bilgi kürede elindeki en etkin silah olduğunu unutmamalıdır. Sanal dünyada amaçsızca gezinen bu gençler, ülkenin güvenlik politikasında kullanılmak üzere, belli şablonlar çerçevesinde eğitilmelidir. Bu açıdan, güvenlik sağlama sorumluluğunun gereği olarak koordinasyon makamını kuran devlet, sivil alanda ise, güvenilirliğini kanıtlamış, yazılı ve sözlü protokollerle devletin güvenlik politikasına katılan sivil kurumları, bünyesinde barındırdığı genç güçlerle birlikte aktif şekilde korumalı ve teşvik etmelidir. Bu sivil güçler, her aşamada, devletin sıklet merkezini dağıtmasına gerek kalmadan, sanal coğrafyada oluşacak küçük sorunlarla başedecek konuma ve bilince ulaşacaklardır. Yasal çerçeve, bu gerçeği gözönüne alarak

oluşturulmalıdır. Yasal ceza mekanizmaları, bilgi kürede merak içgüdüyle dolanan gençler üzerinde değil; devlete karşı ideolojik gündemlerini dayatma mücadelelerinde sanal coğrafyayı etkin ve yeni bir cephe olarak algılayan sanal düşmanlara karşı uygulanmalıdır.

4.7.5. Stratejik Sektör ve Ürünler

Bilgi kürenin oluşumuyla birlikte, bilgi egemen güçlerin belli sektörlerde yoğunlaştığı görülmektedir. Sanal coğrafyaya özgü olarak, çok geniş kitlelere bedava veya bedavaya yakın ucuzlukta sunulan hizmetlere rastlanmaktadır. Özellikle iletişim sektöründe görülen bu bedava ürünlerin arkasındaki mantık ekonomik olmaktan çok, sözkonusu iletişim ürünlerini kullanan kitlelerin üzerinden elde edilen bilgi ve istihbaratın politik ve kültürel değerinden kaynaklanmaktadır. Bilgi tuzakları sundukları kolaylıklarla tüketiciyi, yani çağdaş vatandaşı, avucunun içine alırken, aynı zamanda bu vatandaşın her türlü sosyo-politik davranışlarının takip edileceği elektronik bir kuyruğu da peşi sıra takmaktadır. Böyle bir ortamda, bir ülkenin vatandaşlarına dair bu tür bilgilerin, teknolojiye hakim ve egemen diğer ülkelerin kontrolü ve denetimine girmesi, sözkonusu ülkelerin stratejik çıkarlarının insiyatifine bırakılması büyük zaaf teşkil edecektir. Türkiye, özellikle iletişim sektöründe hızla uzmanlaşarak, eğitim sistemini gençliği bu alana yönlendirecek şekilde yapılandırmalıdır.

Milli ürün olmadığı, sermayenin renginin olmadığı gibi yaklaşımlara prim verilmeyerek, Türkiye konu ile ilgili kendi milli markalarını ve firmalarını yaratmak zorundadır. Bir coğrafyada yeralan madenler nasıl milli servet ise, aynı coğrafyada yaşayan vatandaşların ürettiği her bilginin stratejik, ekonomik ve sosyal değeri olduğu unutulmayarak, Türkiye kendi vatandaşının ürettiği bilgiyi bizzat kendisi derleyip, değerlendirip, koruyacak altyapıları ve üst yapıları oluşturmak zorundadır.

Türkiye sözkonusu stratejik sektörleri ve ürünleri geliştirirken, sadece kendi coğrafyası üzerindeki hakimiyetini değil, bölge coğrafyası üzerindeki hakimiyetini de geliştirmeyi gözönüne almalıdır. Dünyayı ellerinde tutan güçlerin, kritik sektörlerde geliştirdikleri ürünlerin içine, gerektirdiği takdirde kullanılmak üzere, o ürünlerin kendi çıkarları dışında kullanılmasını engelleyici tuzaklar yerleştirdikleri artık bilinen bir gerçektir. Bu gerçeğin ışığında, dışarıdan gelen her ürün ve hizmete,

ülke çıkarları doğrultusunda sağlıklı bir şüphencilik ile yaklaşmak ülke savunmasının bir gereğidir. Türkiye'nin, dışardan aldığı ve/veya yabancı ortaklarla içerde ürettiği, yeni çağın güvenlik politikaları açısından önem taşıyan her ürün ve hizmetin, ülke politikalarını zaafa uğratmayacak güvenilirlikte olduğunu tespit edecek teknik, idari ve hukuki konuma sahip olması gerekmektedir. Bu çerçevede, özellikle savunma ve iletişim sektöründe, ürünlerin ve hizmetlerin kabının Türk olması ile yetinilmemeli ve sözkonusu ürünlerin içeriğinin de Türk damgası taşımasına özen gösterilmelidir. GPS sistemlerinden tutun da, telefon santrallerine kadar her türlü sistem, önceden tespit edilen millilik kriterleri çerçevesinde test edilmeli ve bu testi geçemeyen hiç bir ürün, hizmet ve firmanın milli bilgi yapılanmasına eklenmesine izin verilmemelidir. Yabancı bir ülke tarafından yapılan bir yazılım herşeyi ile milli kontrol mekanizmaları ile denetlenebilir, fakat yazılımlarının içine neler gizlenip gizlenmediğini tam anlamı ile kontrol etmek zordur. Sözkonusu ürün, hizmet veya yapının milli kontrol altında olduğuna emin olmak imkansızdır. Türkiye bu nedenle, genç ve yetenekli beyinlerini her alanda kritik noktalara yerleştirerek, kurulabilecek tuzakları tespit edip, giderme yeteneğini geliştirmeli ve hiç bir zaman bu konudan taviz vermemelidir. Sözkonusu yetenekli beyinlerin yetiştirilmesi için, sanal çağın teknolojilerini ve bilimini teknik aşamadan, teorik aşamaya kadar verebilecek eğitim kurumları Türkiye'nin her bir yanına kurulmalı ve bu yönde her türlü teşvik uygulanmalıdır.

Yukarıda önerilen şablonun çimentosundaki millilik unsuru, belki Türkiye tarihinde hiç bir zaman önemli olmadığı kadar ciddiye alınması ve taviz verilmemesi gereken bir unsur olarak karşımıza çıkmaktadır. Bütün dostluk ve çıkar ilişkilerinden bağımsız olarak, Türkiye sanal coğrafyadaki güvenlik politikasını mutlaka ve mutlaka vatandaşları ile ortak bir mutabakat ve katılım çerçevesinde geliştirerek, her türlü senaryo ışığında, sözkonusu altyapı ve üst yapıları gerektiği takdirde tek başına ayakta durabilecek kapasite ve güvenilirlikte oluşturmak zorundadır. Yeni çağda bir devlet, ancak vatandaşı kadar özgür ve yaratıcı, bir vatandaşı ise ancak devleti kadar bağımsız ve güvenli olabilecektir. Herkesin bir ağ ile birbirine bağlandığı bu süreçte, ağın en zayıf ilmiği kadar güçlü olacağı unutulmamalıdır (Gürcihan, 2002, s.1-7).

4.8. Bilgi Savaşı Projeleri

Türkiye’de bilgi harbi kavramının Türk Silahlı Kuvvetleri yoluyla gündeme geldiğinden hareketle bu konudaki projelerin de yine aynı kurum tarafından savunma sanayi projeleri kapsamında gündeme getirildiğini ve hayata geçirildiğini görüyoruz. Bu bölümde Türk Silahlı Kuvvetlerinde bilgi harbiyle ilişkili olarak hayata geçirilen projeleri inceleyeceğiz:

4.8.1. TAFICS (Turkish Armed Forces Integrated Communication System)

TAFICS barış, gerginlik durumu ve savaşta stratejik ve operatif seviyedeki komutanlar arasındaki bilgi iletimi ihtiyaçlarını karşılamak için modern, süratli, emniyetli, beka kabiliyeti yüksek, elastiki, geniş kapasiteli, otomatik ve entegrasyona açık sayısal bir iletişim sistemini ifade etmektedir. Sistem aynı zamanda hükümetin de kriz zamanlarındaki ihtiyaçlarına cevap verecek şekilde tasarlanmıştır. İletişim ortamı Türkiye sathına yayılmış 8500 km. fiber optik kablo ve 107 radyo link istasyonu ile sağlanacak, 11 adet düğüm santralı vasıtasıyla ile sistem Ankara’da kurulacak olan ana kontrol merkezi ile yönetilecek, ayrıca yedek ana kontrol merkezi Eskişehir’de tesis edilecektir. TAFICS emniyetli ses, resim, data, yazı ve görüntü aktarma gibi çeşitli tele servisler sağlayacaktır. Proje 217 kullanıcıya yüksek kalite, kapasite, emniyet ve süratte haberleşme imkanı temin edecektir. Video konferans ve görüntülü telefon imkanlarına sahip olan sistemin emniyeti demet ve uç kriptoloji cihazları ile sağlanacaktır. TAFICS projesi günümüzde büyük kısmıyla hayata geçirilmiştir. Siemens/SIMCO ortak kuruluşu tarafından yürütülen proje tamamlanmıştır. Projenin sözleşmesi 1996 yılında imzalanmış olup, bedeli 200 milyon ABD dolarıdır (Savunma ve Havacılık, 2000, s.78-79).

4.8.2. Taktik Saha Muhabere Sistemleri (TASMUS) Projesi

Kara Kuvvetleri Komutanlığı’nın taktik sahadaki Komuta Kontrol ihtiyaçlarını elastiki, güvenilir, beka kabiliyeti yüksek iletişim sistemleri ile karşılamak amacıyla uygulanan proje Ordu seviyesinden Tabur seviyesine kadar olan birlikleri kapsamaktadır. TASMUS taktik sahada kullanıcılara ses, data ve görüntülü haberleşme imkanı sağlayacak ayrıca Taktik Harekat Merkezleri arasında video

telekonferans hizmeti verecektir. Her ordu bölgesinde en az üç yerde TAFICS'e entegre olacak sistem TAFICS'le birlikte düşünüldüğünde yeni bir Telekom ağına eşdeğer olacaktır. TASMUS projesi Kara Kuvvetlerinin iletişim ihtiyaçlarına yönelik temel bir projedir. Bu sistemi tamamlamak için, 9600 serisi frekans atlamalı telsizler, 4600 serisi telsizler, uydu yer terminalleri gibi çok sayıda iletişim sistemleri projesi eşzamanlı olarak yürütülmektedir (Savunma ve Havacılık, 2000, s. 78-79).

4.8.3. Türk Silahlı Kuvvetleri Uydu Muharebe Sistemi Projesi

Proje; TAFICS ve Türk Telekom A.Ş. imkanlarıyla iletişimin sağlanamadığı veya zayıf olduğu durumlarda emniyetli ve kaliteli ses, data, video, tele konferans desteğinin temin edilmesi maksadıyla kullanılacak uydu terminalleri ile TAFICS ve TASMUS'a alternatif iletişim ortamı sağlamayı amaçlamaktadır. Halihazırda Türk Silahlı Kuvvetleri uydu haberleşmesi yapmakta ve bu maksatla Türksat-1C uydusunun herkese açık olan ticari bandı (Ku-Bandı) kullanılmaktadır. Uydu Muharebe Sistemi Projesiyle Türksat 2-A uydusundan faydalanılacaktır. Türksat 2-A uydusu iki kısımdan oluşmaktadır: Ku-Band ve X-Band. Emniyetli bir iletişim ortamı sağladığından X-Band genellikle askeri hizmetler için kullanılmaktadır. Bu kısmın algoritması Türk Silahlı Kuvvetleri tarafından üretilmiş olup, başka bir ülke tarafından durdurulması, dinlenilmesi ve bastırılması imkanı yoktur. Yer terminalleriyle desteklenecek olan bu sistem TAFICS ve TASMUS'a entegre olabilmekte ve seyir halindeki savaş araçlarıyla da iletişime geçebilmektedir (Savunma ve Havacılık, 2000, s. 78-79).

4.8.4. Uzun Ufuk Projesi

Deniz Kuvvetlerinin Harpoon füzelerini en etkin şekilde kullanabilmesi için Ege Denizini 24 saat esasına göre izleyecek ve elde edilecek taktik resmin bu silahı taşıyan gemilere ulaştırılması maksadıyla uygulanan proje 10 adet gözetleme uçağı, karaya konuşlu 3 adet mikrodalga radar, 4 adet Elektronik Destek Tedbirleri sistemi, HF radar, 1 takım insansız hava aracı, deniz hava hareket merkezi ve 2 adet füzyon merkezinden oluşan bir hedef tesbit ve haberleşme sistemidir. Gerçek zamanlı olarak çalışacak sistem, milli imkanlarla üretilen düşman tanıma-tanıtma sistemine entegre edilecektir. Bu suretle otomatik olarak birbirlerini tanıma ve tanıtma yeteneğine sahip radar, gemi, füze ve uçaklar aynı sistemi kullanan ünitelerin kullandığı



sorgulama ağına dahil edilecek ve Ege Denizinde sisteme uyum sağlamayan platformlar düşman kabul edilecektir (Ulusal Strateji, 2000, s. 75-76).

4.9. Konseptin İfadesi

Konsept belirlenme aşamasından önce yapılan değerlendirmeler neticesinde ortaya çıkan gerçek, Türkiye'nin önümüzdeki dönem içerisinde de teknolojik bağımlılıktan kurtulamayacağı; buna karşılık savunma anlamında teknolojik boyutlu güvenlik sorunlarının artacağıdır. Özellikle Rusya Federasyonu ve Yunanistan'ın bilgi savaşı kapsamında açık ve belirgin tehdit oluşturduğu görülmektedir. Bununda ötesinde bilgi savaşının Sadece Silahlı Kuvvetlerin ilgi alanına giren bir husus olmadığı da aşikardır. Topyekün bir mücadeleyi öngören bilgi savaşının teknik ayrıntılarla dolu bir yapıda olduğu zannedilerek stratejik oluşumlardan uzak durulmamalıdır. Geleceğin savaşlarının en güçlü silahının bilgi olduğu yaptığımız değerlendirmenin belki de en kesin sonucudur. Öyleyse stratejik bir yaklaşımla önümüzdeki dönem içerisinde Türkiye'nin Bilgi Savaşı Konsepti şu şekilde ifade edilebilir:

Bilgi savaşları Türkiye'nin genel savunma stratejisi dökümanlarında önemi derecesinde yerini almalıdır. İthal ve transfer teknolojilere olan bağımlılık; milli güç unsurlarını etkileyen faktörlerden; savunma yapılanması (silahlı kuvvetler, savunma sanayi), iletişim altyapısı, ulaştırma altyapısı ve finans sektöründe özellikle yazılım temininde asgari düzeye indirilmeli veya bu yapılara devlet kontrollü teknoloji girişleri sağlanmalıdır. Teknolojide tek bir ülkeye ya da ülkeler topluluğuna (ABD, AB) yönelmekten vazgeçilmeli, Japonya, Kore, Singapur gibi Asya ülkeleri teknoloji temininde alternatifler olarak değerlendirilmelidir. Ulusal Bilgi Güvenliği Teşkilatı etkin hale getirilmeli, Ulusal Bilgi Güvenliği Yasası çıkarılarak; kurumsallaşma sağlanmalıdır. Bilim ve Teknoloji Yüksek Kurulu mevcut yapıyı değerlendirerek Bilgi Savaşına yönelik özel kapsamlı bir Bilim ve Teknoloji Politikası belirlemeli ve eğitim sistemiyle entegrasyon sağlanarak Türkiye bilgi savaşını yürütebilecek (savunma/taarruz) bir potansiyele sahip kılınmalıdır.



5. SONUÇ VE ÖNERİLER

Türkiye'nin temel stratejik hedeflerine ulaşmasının önkoşulu her şeyden önce milli karar mekanizmalarını harekete geçirmek ve dış tesirlerden mümkün olduğunca arınmış bağımsız politikalar uygulayabilmektir. Günümüzde küreselleşme süreci içerisinde ülkelerin kendi stratejilerini hayata geçirebilmek için bağımsız hareket edebilme serbestisi bir anlamda kısıtlanmaktadır. Ülkeler üzerinde dış yönlendirmeler ve baskı mekanizmaları her zamankinden daha yoğun ve etkilidir. Bu etkinin derecesini ise o ülkenin küreselleşmeyi hangi anlamda algıladığı ve bu sürece katılım derecesi belirlemektedir. Ekonomik anlamda küreselleşme sürecinin kazanımlarından fayda sağlayamayan ve rekabetçi bir yapı oluşturamayan toplumlar; bu hareketin öncülüğünü yapan ve global stratejiler üreterek menfaatlerini dünyanın her bölgesinde takip eden büyük güç odaklarının kimi zaman zorlamaya varan etkilerine maruz kalmaktadır. Dolaylı savaş ve cezalandırma savaşları ön plana çıkmaktadır. Bu güçler zaman, zaman isteklerini güç kullanarak kabul ettirmektedir. Bu kapsamda; henüz küreselleşme rüzgarını yakalayamayan, gerek ekonomik gerekse teknolojik olarak güç odağı konumundan uzakta olan Türkiye'nin bu etkilere karşı durabilme ve pasifize edebilme yeteneğine sahip olabilmesi için elinde tek bir güç kalmaktadır: Savunma gücü.

Genel anlamda bu gücün caydırıcı bir etkiye sahip olması; temel stratejilerin yönelik politikaların uygulanmasında ve milli karar mekanizmalarının bağımsız hareket edebilmesi için ülke açısından bir teminat niteliğindedir. Caydırıcılık özelliği olan, etkin bir savunma gücünün en temel koşulu ise milli savunma sanayine sahip olunmasıdır. Ancak kendi savunma sistemlerini, silah, araç ve gereçlerini üretebilen ve geliştirebilen ülkeler, herhangi bir kriz ortamında engelleme ve ambargolara maruz kalmadan, savunma gücünü ayakta tutabilirler. Sahip olunan savunma sistemlerinin gizliliği eğer o sistem ülke imkanlarıyla üretilmişse mümkündür. Türkiye son yirmi yıllık süreç içerisinde savunma sanayinde önemli bir atılım içerisine girmiştir. Önemli yatırımlara imza atılmış, yurtiçi potansiyelin harekete geçirilmesi maksadıyla dünyanın silah sistemi satan dev şirketleriyle ortaklığa gidilmiş ve küçümsenmeyecek bir insan gücü potansiyeli ile teknoloji birikimi elde edilmiştir. Ancak bugün bile Türkiye silah ithal eden ülkeler arasında Suudi Arabistan, ABD ve Mısır'dan sonra dünyada dördüncü sırada bulunmaktadır.

Savunma malzemeleri ihracaatında ise yirminci sıranın bile altında bulunmakta, aldığı savunma malzemelerinin parasının kırkta birini bu malzemelerin yurtdışına satışından kazanabilmektedir. Aradaki fark ise diğer ihraç ürünleri gelirlerinden veya borçlanma ile karşılanabilmektedir (Anlağan, 2000, s.76).

Savunma sanayindeki mücadelenin esasını temelde teknolojiye sahip olma oluşturmaktadır. Teknoloji temini, casusluk gibi istisnai durumları bir kenara bırakacak olursak, genelde;

- Silah veya silah sisteminin satın alınması,
- Teknoloji transferi,
- ARGE yoluyla teknoloji üretimi yollarıyla yapılabilmektedir.

Her üç yöntemin de birbirlerine oranla avantajlı ve dezavantajlı durumları vardır. Bazen malzemenin niteliği, miktarı, temin süresi gibi özel durumlar ve koşullar kriter olarak alınmakta; bu durumda bazen teknoloji üretmek yerine malzeme alımı tercih edilebilmektedir. Savunma alanında temin edilen ürünlerin birtakım ortak özellikleri vardır. Bu yüzden diğer sanayi ürünlerinin temin yöntemlerinden farklı usullerle malzeme temini yoluna gidilmektedir. En ileri teknolojilerin uygulanması, yüksek kaliteli ürün ihtiyacı, ürünlerin emniyetli güvenilir ve özelliklerinin gizlilik gerektirmesi, dışa bağımlılığın az olmasının istenmesi, alım kararlarında siyasi kriterlerin de göz önünde bulundurulması, savunma silah ve sistem ürünlerinin temin özelliklerinden bazılarıdır. Diğer taraftan yüzyılın son çeyreğinde, dünyadaki gelişmeler, silahlı kuvvetler harcamalarının kısılarak ekonomik gelişmeye katkı sağlanması yönünde olmuştur. Geçmişin sayısal üstünlüğe dayalı hantal orduları terkedilmiş; teknolojik üstünlük, bilgi üstünlüğü, nitelik üstünlüğü, eğitim üstünlüğü, komuta kontrol üstünlüğü gibi kriterler tam/yarı profesyonel orduların teşkilatlanmasında esas teşkil etmiştir. Buradan tasarruf edilen maliyetin ise ekonomilere kaynak olarak aktarılması planlanmıştır (Anlağan, 2000, s. 77).

Bilgi ve teknolojinin hızla gelişmesi ve çok çeşitli olması, bu bilgi ve teknolojiye her zaman egemen olmayı imkansız hale getirmektedir. Ülkeler için bilim ve teknolojinin hangi alanlarına öncelik verileceği, bu alanlarla ilgili yönlendirme, planlama, eğitim altyapısının oluşturulması hususlarını içeren bilim ve teknoloji politikalarının tesbiti zorunlu hale gelmiştir. Güvenlik sorunlarının tüm temel

stratejileri etkilediği günümüzde savunma sanayi ve bilim ve teknoloji politikaları birbiriyle iç içe geçmiş iki kavram haline gelmiştir.

Yirmi birinci yüzyılda tüm hareketlerin temel taşı Bilgi Savaşı olacağından Silahlı Kuvvetlerin tüm silah ve güdüm sistemlerinin bu esasa göre tasarlanması ve üretilmesi, milli sistemin oluşturulmasının en önemli aşamasını oluşturmaktadır (Ayhan, 2002, s. 162).

Nitekim BTYK üçüncü toplantısında alınan 16 numaralı karar, doğrudan Türkiye'nin savunma yapılanmasıyla ilişkilidir: "Genelkurmay Başkanlığı'nın Türk Savunma Sanayinin geliştirilmesi, desteklenmesi ve önünün açılması yönündeki görüş ve önerilerinin değerlendirilmesi" (Gök, 1999, s. 47).

Özellikle 16 nolu kararın; "Kurulumuz, ulusal savunma stratejimizin önceliklerini ve ulusal savunma sanayinin bu önceliklere yanıt verecek biçimde ve özellikle de teknoloji yeteneği açısından geliştirilmesi gereğini, ülkenin bilim ve teknoloji yeteneğini bir bütün olarak yükseltme gereğinin ayrılmaz bir parçası sayar ve savunma önceliklerinin bu bütün içinde çözülmesi gerektiğini teyit eder" şeklindeki ifadesi milli bir savunma sanayinin oluşturulmasının ülkenin bilim teknoloji yeteneğine yapacağı katkının yanısıra bir güç birliği anlamı da içermektedir (Gök, 1999, s. 41).

Diğer yandan Milli Savunma Bakanlığınca hazırlanan ve 1998 yılında yürürlüğe konan, "Türk Savunma Sanayi Politikası ve Stratejisi Esasları" konulu Bakanlar Kurulu Kararı yüksek teknolojiye sahip harp ve silah sistemlerine sahip olunması gerektiğini ifade etmekte ve bu sistemlerin mutlaka milli gizlilik dereceli tesis güvenlik belgesine sahip yerli sanayi tesislerinde üretilmesi öngörülmektedir. Hatta bu çalışmalara katılacak milli firmalara ihalelerde yüzde 15'e kadar fiyat farkı avantajı da tanınmaktadır. Bu dökümanda savunma sanayi ürünleri ve bunlarla ilişkili teknolojilerden; milli olması zorunlu sistem ve teknolojilerin, kesinlikle yurtiçinden milli imkanlarla temini; kritik sistem ve teknolojilerin ise ancak uzun vadede yurt içi imkanlarından faydalanılarak temin edilememesi durumunda ortak üretim ile temini hükmü bulunmaktadır.

Türk Silahlı Kuvvetleri, MİT ve diğer mevcut kamu kurum ve kuruluşlarının Bilgi Savaşı unsurlarını etkin, koordineli, uyumlu ve çağın teknolojilerinden azami

faaydalanarak kullanmasının, milli ıkarlarımızın kollanması ve saėlanmasında ok nemli olduėu, “Blc terr rgt bařının Kenya’da yakalanması” operasyonunda, devletin iine sızmış etelerin ortaya ıkarılmasında, uyusturucu kaakılıėının nlenmesi faaliyetlerinde, szde Ermeni soykırımı iddialarına ve blc rgtn fikirlerine destek veren web sitelerinin kertilmesi ile diėer benzeri pek ok uygulama ile teyit edilmiřtir.

Milli bazda konu ile alakalı en nemli oluřum olan Ulusal Bilgi Gvenlik Teřkilatı alıřmalarını srdrmekte olup, dokman seviyesinde yeterli hazırlıėa sahiptir. Ancak unutulmamalıdır ki sorumluluk sadece bu kuruluř deėil milli bilgi unsurlarıyla iřlem yapan tm Trkiye Cumhuriyeti kamu ve zel kurum ve kuruluřlarını kapsamaktadır.

Devlet apında eėitim faaliyetlerine vakit geirmeden bařlanmalı ve Ulusal Bilgi Gvenlik Teřkilatı’nın nerdiėi kanun ve ynetmelikler hayata geirilmeli ve alıřtırılmalıdır. Uygulamaya geirilmesi nerilen Ulusal Bilgi Gvenliėi Teřkilatı ve Grevleri Hakkındaki Kanunun genel gerekesi bu gereėi bir kez daha gzler nne sermektedir:

Gnmzde bilgi; tarih boyunca olduėundan sratle iletilmekte, buna baėlı olarak da retilen bilginin saklanması, kullanılması, bir yerden diėer bir yere nakledilmesi ve imhası iin klasik usullerin dıřında, geliřen teknolojiyen sonuna kadar yararlanma gereėi ortaya ıkmıřtır. Teknolojiye ve bilgiye olan bu baėımlılık, lkeleri, bilginin korunması iin yeni usuller geliřtirmeye ve yasal dzenlemeler yapmaya mecbur bırakmıřtır.

Bilgi teknolojisine giderek artan baėımlılıėın sonucu olarak, merkezi kontrol, devlet ynetimi, ekonomik ve toplumsal hayatın her ynnn ortak bileřeni bilgi altyapısının kt niyetli kiřilere, terrist faaliyetlere ve doėal afetlere karřı korunması nem kazanmıřtır. Kamu ve zel kurum ve kuruluřların kendi yapılarına uygun farklı bir gvenlik nlemleri almaları ve bu konuda milli bir politikanın olmayıřı, lkemizin milli gvenliėini hassas hale getirmektedir. Bilgi gvenliėi konusundaki milli politika ile; motivasyonları ve grev alanları farklı olan kamu ve zel sektrn, gerek kendi iřlerinde, gerekse karřılıklı iliřkilerinde her trl tehdit ve

hassasiyete karşı bilgi güvenliğini tam olarak sağlayacak ilke ve önceliklerin tespiti gerekmektedir.

Milli bilgi güvenliğine yönelik tehdidin milli bilgi altyapımızı etkilemek, zarar vermek ve taarruz etmek için birçok farklı seçeneği vardır. Altyapıya karşı saldırılar teknik yeteneklerden, motivasyona kadar birçok değişiklik arz ederek, veri tabanını karıştırması veya programların uygulamalarını bozma yada fiziksel olarak yok edecek biçimde çatışma seviyesine (barış, kriz ve savaş) uygun olarak yapılır. Nispi barış periyodu sırasında dahi tehdidin, değişik seviyelerde devamlı olarak mevcut olduğunu unutmamak gerekir. Tehdidin kaynakları bireylerden (muhabir ve yetkisiz kullanıcılar) karmaşık milli organizasyonlara (yabancı istihbarat servisleri ve askeri istihbarat unsurları) kadar geniş bir yelpaze olarak ortaya çıkmaktadır. Bu gruplar arasındaki sınırlar belirsiz olduğundan, genellikle olayın kaynağını tespit etmek oldukça zordur.

Türkiye Cumhuriyeti Devleti'nin milli ve ekonomik güvenliğini etkileyen milli bilgi altyapısının, bugünkü haliyle güvenilirlik ve hizmete hazır olma kriterleri açısından, ihtiyaçları tam olarak karşılamadığı değerlendirilmektedir. Altyapının tehdide ve hassasiyetlere karşı yetersiz oluşu, altyapıda muhtemel kesintilere ve olabilecek kötü niyetli saldırılara karşı hassasiyeti arttırmaktadır. Bu nedenle, bu tür tehditleri ortaya çıkarmak ve gerekli önlemleri almak üzere merkezi bir yönetim birimine ihtiyaç duyulmaktadır.

Bu çerçevede, Devletin kamu ve özel tüm kurum ve kuruluşlarının endüstriyel, politik, ekonomik ve sosyal alanlarda kaçınılmaz olarak etkileşim içinde olduğu hususu dikkate alınarak, ortak olarak kullandıkları altyapının, Devletin milli ve ekonomik çıkarları için güvence altına alınması amaçlanmıştır. Öngörülen ana esaslar çerçevesinde sorunun; milli güvenlik politikasından sorumlu üst organın direktiflerine uygun olarak, gecikmeksizin çözümlenmesi için merkezi bir milli bilgi güvenliği yönetim yapısının oluşturulması ihtiyacı ortaya çıkmıştır. Bu bağlamda, Hükümet seviyesinde milli güvenlik ihtiyaçları doğrultusunda genel prensipleri belirleyen bir üst organ; direktifleri ve yasalarda verilen görevleri uygulayacak ve milli bilgi güvenlik sistemini işletecek bir yönetim birimi teşkili yoluna gidilmektedir. Taslak ile; "Milli güvenliği ilgilendiren bilgilerin korunması ve devletin bilgi güvenliği faaliyetlerinin geliştirilmesi, gerekli stratejilerin

(politikaların) üretilmesi ve belirlenmesi, kısa ve uzun dönemli planların hazırlanması, kriter ve standartların saptanması, ihracat ve ithalat izinlerinin ve sertifikaların verilmesi, bilgi sistemlerinin teknolojiye uyumunun sağlanması, uygulamanın takip ve denetimi, kamu ve özel kurum ve kuruluşları arasında koordinasyonun sağlanması amaçlarını gerçekleştirmek üzere oluşturulan teşkilatın görevlerine ilişkin esas ve usuller ile bunlara ilave olarak, bu yasal düzenleme ile kamu ve özel bütün kurum ve kuruluşlarda, bilgi güvenliğini sağlayacak gerekli yapılanmaya geçilmesi” hususu düzenlenmektedir.

Yürütülen her türlü bilgi sistem projesinde ihtiyaç duyulan kriptoloji ve yazılım ihtiyaçlarının tamamı, bu konuda ihtisas sahibi milli kurum ve kuruluşlardan tedarik edilmeli; projelere milli firma ve girişimcilerin katılımı için azami gayret gösterilmeli ve teşvik edilmelidir.

Yakın geçmişte gerçekleşen Körfez Savaşı ile sürekli gündemde olan, sanal ortamda yayılan virüsler göz önüne alındığında, strateji belirlerken bilgi savaşına da en az diğer savaş faktörlerine gösterilen hassasiyetin gösterilmesi gerektiği gerçeği ile karşılaşılacaktır. Asıl dikkat edilmesi ve gözden uzak tutulmaması gereken nokta ise bilgi savaşının sadece askeri bir tehdit olmayıp, kişisel, ekonomik ve psikolojik boyutlara da sahip olmasıdır. Toplum huzuru ve güvenliği için son derece dikkatle takip edilip, gerekli önlemlerin alınması gerekmektedir. Bu tedbirleri almakla sorumlu olanlar ise bilgi sistemlerini aktif olarak kullanmakta olan her kamu-özel, asker-sivil; her kesimden kullanıcıdır. İstenmeyen sonuçlarla karşılaşmamak için en alt seviyede şahsi veya kurumsal olarak uyulması gereken hususları şu şekile sıralamak yerinde olacaktır (Ünal, 2000, s. 36).

- Kesinlikle korsan yazılım kullanılmamalı, önemli bilgiler içeren sistemlerin İnternet gibi çoklu erişim ortamlarına girmeleri önlenmelidir.

- Gerek kendi bilgi sistemimizde, gerekse çalışmakta olduğumuz kuruluşa ait bilgi sistemlerine disket ya da CD gibi sanal yardımcılardan bilgi transferi yapacaksa, mutlaka güncelleşmesi tam olarak yapılan virüs programlarını kullanmalıyız. Bunu bir alışkanlık haline getirmeliyiz.

- Eğer dış ortamlardan CD ve disket gibi sanal yardımcılarla veri transferini çok yapıyorsak belli zaman dilimlerinde, periyodik olarak bilgi sistemimizi yedeklemeli ve sistemi yeniden formatlamalıyız.

- Eğer bir kuruluşun sahibiysek, bilgi sistemimizi korumak üzere koruyucu yazılımlar temin etmeli ve zamanla oluşabilecek gediklere karşı yeni yazılımların temini veya geliştirilmesi için kaynak ayırmalıyız.

Konuyla ilgili Ulusal Bilgi Güvenlik Teşkilatı, Emniyet Teşkilatı, Milli İstihbarat Teşkilatı ve Silahlı Kuvvetler gibi kuruluşların AR-GE projeleri karşılaştırılmalı, kaynak israfı ve duplikasyonlar önlenmeli ve projeler TÜBİTAK'ın ilgili bölümlerine devredilerek tasarruf sağlanmalıdır.

Bilgi savaşının tabanı olan eğitim çalışmaları tek elden sağlanmalıdır. Bu konuda ilgili kurumlarda görev yapacak uzman personel ihtiyacı süratle karşılanmalıdır.

Silahlı Kuvvetleri'in gelecekteki yapılanmasında "Teknik Üstünlük" kriteri mutlaka göz önünde bulundurulmalıdır. Bu kriter zamanla avantaja dönerek, personel ve silah indirimine gidilebilir, ülke kaynaklarının kalkınmaya yönlendirilmesi sağlanabilir.

Bilgi ve teknoloji gücü artık milli gücün bir unsuru olarak stratejik değerlendirmelerde yerini almalıdır.

Devlet kurumları içerisinde askeri, teknik, ekonomik ve politik konularda birbirleriyle iletişim halinde bulunan tüm unsurların bilgi savaşlarına altyapı teşkil edecek ve bilginin temini, saklanması, kullanılması safhalarında bilgi güvenliğini sağlayacak faaliyetleri düzenleyecek temel ihtiyaçlar şunlardır:

- Ortak politika ve konsept belirlenmesi,
- Kurum içi bilgi güvenlik kuruluşlarının tesisi ve üstyapıya entegrasyonu,
- Eğitim ihtiyaçlarının giderilmesi,
- Tüm kurumların uygulayabileceği standart bir bilgi güvenliği mevzuatı,
- Yasal düzenlemeler,
- Milli yazılım ve kripto ihtiyaçlarının giderilmesi

Bu temel ihtiyaçların giderilmesine yönelik vakit geçirmeksizin alınması gereken tedbirleri ise;

- Bilim ve Teknoloji Yüksek Kurulunca özel kapsamlı bilgi savaşları politikası ve konseptinin belirlenmesi,

- Ulusal Bilgi Güvenlik Teşkilatının kurulması,
- Anayasal hakları zedelemeyecek şekilde kişisel haberleşme hürriyeti ve haberleşme gizliliği ile milli güvenliği ortak olarak gözetecek bilgi güvenlik yasasının çıkarılması,
- Kurumlar arasında Milli Bilgi Ağının kurulması; bu ağın güvenli bilgi sınırlarının belirlenmesi ve ağa yapılacak giriş ve çıkışları gerçek zamanlı olarak denetleyecek bilgi güvenlik sistemlerinin temini,
- Stratejik faaliyet gösteren her kurumun kendi iç bilgi güvenlik teşkilatını kurması; standart bilgi güvenlik kriterlerinin, bu teşkilatların personeline, tek bir eğitim kurumundan verilecek eğitimle enjekte edilmesi olarak sayılabilir.

Bilgi savaşı ile ilgili yapılanmayı ortaya koyarken hiçbir zaman aklımızdan çıkarmayacağımız husus; “küreselleşen dünyada millilik, bağımsızlığın vazgeçilmez temel taşıdır “ilkesi olmalıdır (Gürcihan, 2002, s.1-7).

Yayılmacılığın yeni boyutlarıyla ortaya çıktığı günümüzde, Türkiye Cumhuriyeti’nin milletiyle birlikte bölünmez bütünlüğüne yönelik saldırılar da şekil değiştirmiştir. Geçmişte yaşandığı gibi, gelecekte de bu saldırıların süreceği öngörülmektedir. Çünkü; menfaatler, emeller ve niyetlerde bir değişiklik olmamıştır. İdeolojilerini bile değiştirebilen ülkelerin, Türkiye’ye yönelik politikalarında hiçbir değişiklik yaşanmadığı görülmektedir. Jeopolitik ve jeostratejik önemi, herhangi bir ülkeyle kıyaslanmayacak kadar belirgin olan Türkiye; geleceğini, bu gerçeklerin farkında olarak şekillendirmelidir.

Emperyalizm yeni savaş oyuncağını bulmuştur: Bilgi. Ancak, Türkiye cephesinden bakacak olursak, henüz hiçbir şeyde geç kalınmamıştır. Bilgi, günümüzde, herkesin ulaşabileceği yakınlıktadır. Önemli olan, bilginin işlenip, “bilimsel bilgi” haline getirilmesi; elde edilecek hasılanın ise, toplumun refahı, huzuru, güvenliği ve bekası için kullanılmasıdır. Sürdürülebilir kalkınmanın temeli bu düşünce olmalıdır.

Türkiye’nin yeni yüzyılda vizyonu; “çağdaş uygarlık düzeyine ulaşmaktır”. Ülke geleceği şekillendirilirken, içte ve dışta pek çok engelle karşılaşılacağı, bilinen bir gerçektir. Bu engellerin üstesinden gelmenin tek yolu; devlet-millet dayanışmasını ortaya koyarak, bilinçli bir arayış içerisinde olmaktır.

Belirsizliklerin fırsatları da beraberinde getirdiği fikrinden hareketle; günümüzün belirsizliklerle dolu ortamında, Türkiye'nin adeta zorunluluğu olan "lider ülke" sıfatına kavuşması boş bir hayal değildir. Bunu başarmak için, gerekli tarihsel birikim ve güç unsurları Türkiye'de mevcuttur. Asıl olan, bu tecrübe ve gücün, milli menfaatler doğrultusunda, stratejik bir yaklaşımla kullanılmasıdır.



KAYNAKLAR

- 1- ANLAĞAN, Ömer, Türkiye'nin Teknolojik Hedeflerinde Savunmanın Yeri ve Ekonomik Yaklaşımlar, Savunma ve Havacılık Dergisi, Mönch Türkiye Yayıncılık, 2000, cilt 14, sayı 79, sayfa 76-77
- 2- AYHAN, Ahmet, Dünden Bugüne Türkiye'de Bilim-Teknoloji ve Geleceğin Teknolojileri, Beta Basım Yayım Dağıtım A.Ş., 2002, 455 sayfa
- 3- ----- Başbakanlık Genelgesi, Yıl 1993, Sayı 13
- 4- BÜTÜN, Olcay, Türkiye Geleceğini Bulmalı , Ulusal Strateji Dergisi, 2000, sayı 15, CNR Uluslar arası Fuarçılık, sayfa 56-58
- 5- CAMPEN, D. Alan, DEARTH, H. Douglas, GOODDEN, R. Thomas, Cyberwar: Security, Strategy and Conflict in the Information Age, May 1996, Afcea International Press, 312 sayfa
- 6- CAŞIN, Mesut Hakkı, İleri Teknoloji ve ARGE Gücünün 2000'li Yılların Uluslar arası Stratejilerine Etkileri , MSB Araştırma ve Teknoloji Faaliyetler Bülteni, 1999, MSB Yayınları, sayı 9, sayfa 17-26
- 7- ÇÖREKÇİ, Ahmet, MGK'dan İstenen Yeni Rol, Ulusal Strateji Dergisi, 2001, CNR Uluslar arası Fuarçılık, sayfa 41-47
- 8- DUNA, Cem, Türkiye Mucizesi İçin Vizyon Arayışları ve Asya Modeli, Türkiye İş Bankası Kültür Yayınları, 1996, 370 sayfa
- 9- ERKAN, Hüsnü, Bilgi Toplumu ve Ekonomik Gelişme, Türkiye İş Bankası Kültür Yayınları, 1998, 251 sayfa
- 10- ----- Enformatik çalışma Grubu Raporu, TÜBİTAK Bilim ve Teknoloji Politikaları Tartışma Platformu, 1995, 41 sayfa
- 11- ESENERGÜL, Hüseyin, Türk Savunma Sanayinde Yabancı Ortaklı Şirket Olmak, Savunma ve Havacılık Dergisi, Mönch Türkiye Yayıncılık, 2000, cilt 14, sayı 79, sayfa 71-73
- 12- European Parliament Report on the Existence of Echolon, Temporary Committee on the Echolon Interception System, 2001, 194 sayfa
- 13- ----- Field Manual 100-5 Operations, Headquarters Department of the Army, 1993, 49 sayfa
- 14- ----- Field Manual 100-6 Information Operations, Headquarters Department of the Army, 1993, 162 sayfa

- 15- GÖK, Emin, Türkiye’de Bilim Teknoloji ve Savunma ARGE Politika ve Stratejisi, MSB ARGE Semineri, 1999, MSB ARGE Dairesi Başkanlığı, sayfa 37-48
- 16- GÜRCİHAN, Behiç, Bilgi Kuvvetleri Komutanlığı-III , www-dikey8 com, 2002, 7 sayfa
- 17- ----- Harp Akademileri Komutanlığı (1996), Uzman Sistemler ve Yapay Zeka, 172 sayfa
- 18- ----- Harp Akademileri Komutanlığı (1999), TSK Bilgi Harbine Nasıl Hazırlanmalıdır?, 210 sayfa
- 19- HAYDEN Michael B., Electromagnetic Attack: Is Your Infrastructure and Data at Risk?, 10 Ağustos 2001, Indiana University of Pennsylvania, Sans White Papers, 3 sayfa
- 20- İLYASOĞLU, Eyüp (1997), Türk Bilgi Teknolojisi ve Gümrük Birliği,Türkiye İş Bankası Kültür Yayınları, 90 sayfa
- 21- KAHYA, Göksel, Stratejik Felç , MSB Araştırma ve Teknoloji Faaliyetler Bülteni, 1999, MSB Yayınları, sayı 9, sayfa 49-50
- 22- KAYMAKÇALAN, Ömer (1999), Bilim ve Teknoloji Türkiye İçin Örnekler ve Öneriler, Teknoloji Yönetimi Derneği Yayınları, 121 sayfa
- 23- KIVRIKOĞLU, Hüseyin, Genelkurmay Başkanlığı isimli Mülakat, Savunma ve Havacılık Dergisi, Mönch Türkiye Yayıncılık, 1998, cilt 12, sayı 70, sayfa 8-19
- 24- ----- Komuta ve Kontrol, LSE Pamphlet 1-2, (1997), 63 sayfa
25. LIBICKI, Martin, What is Information Warfare, National Defense University, 1996, 104 sayfa
- 26- Malezyalı Hacker Irak İçin Vuracak, Akşam Gazetesi Dış Haberler Servisi, 01 Ocak 2003
- 27- ORÜN, Sıtkı Sunday, Savunma Sanayinde Gelişmeler, Savunma ve Havacılık Dergisi, Mönch Türkiye Yayıncılık, 2000, cilt 14, sayı 79, sayfa 84-85
- 28- ÖZCAN, Mehmet, Siber Terörizm ve Ulusal Güvenliğe Tehdit Oluşturma Boyutu, www.dikey8. com, 2002, 24 sayfa
- 29- ÖZKAYA, Ömer, CIA Belgeleriyle Zihin Kontrolü, IQ Yayıncılık, 2002, 448 sayfa
- 30- ÖZKİL, Altan, Konsept Geliştirme Esasları ve Konseptte Dayalı İhtiyaçlar Sistemi (KDİS) , MSB ARGE Semineri, 1999, MSB ARGE Dairesi Başkanlığı, sayfa 21-27

- 32- SALCAN, Olay, Bilgi Güvenliği , Silahlı Kuvvetler Dergisi, 2001, Genelkurmay Askeri Tarih ve Stratejik Etüt Başkanlığı, sayı 370, sayfa 54-67
- 33- ŞENOĞUL, Nahit, 21 nci Yüzyılın İlk Çeyreğinde Türkiye'nin Genel Vizyonu, Politikası ve Stratejisi , Savunma ve Havacılık Dergisi, Mönch Türkiye Yayıncılık, 1999, cilt 13, sayı 76, sayfa 20-30
- 34- ----- TAFICS Hayata Geçiyor , Savunma ve Havacılık Dergisi , Mönch Türkiye Yayıncılık, 2000, cilt 14, sayı 79, sayfa 78-79
- 35- TATAR, Ali, Bilgisiz Harp Olmaz , Ulusal Strateji Dergisi, 2001, sayı 16, CNR Uluslar arası Fuarçılık, sayfa 73-79
- 36- TOFFLER Alvin ve Heidi, 21-Yüzyılın Şafağında Savaş ve Savaş Karşısı Mücadele, 1995, Sabah Kitapları, 384 sayfa
- 37- TOPTAŞ, Ergüder, Stratejinin Yorumu, Silahlı Kuvvetler Dergisi, 2001, Genelkurmay Askeri Tarih ve Stratejik Etüt Başkanlığı, sayı 370, sayfa 75-79
- 38- ----- Türk Silahlı Kuvvetleri'nin Modernizasyon Projeleri , Ulusal Strateji Dergisi, 2000, sayı 15, CNR Uluslar arası Fuarçılık, s-75-76
- 39- ----- Türkiye Ulusal Enformasyon Altyapısı (TUENA) Anaplanı Sonuç Raporu, 1999, Türkiye Ulusal Enformasyon Altyapısı Proje Ofisi, BİLTEN, 93 sayfa
- 40- ÜNAL, Ahmet Naci, Düşman E-mail İle Gelebilir , Ulusal Strateji, 2000, sayı 15, CNR Uluslar arası Fuarçılık, sayfa 73-79
- 41- WALLER, Douglas, Onward Cyber Soldier , TIME Dergisi, 21 Ağustos 1995, sayfa 26-34
- 41- ----- www.carlisle.army.mil
- 42- ----- www.infowar.com
- 43- ----- www.psycom.net
- 44- ----- www.raven1.net
- 45- ----- www.tubitak.gov.tr

ÖZGEÇMİŞ

1966 yılında Elbistan-K.MARAŞ'ta doğan Eşref ÖZDEMİR, İlkokul ve Ortaokulu Menemen-İZMİR'de bitirdikten sonra 1980 yılında girdiği Kuleli Askeri Lisesinden 1984 yılında mezun olmuştur. 1984 yılında başladığı Kara Harp Okulu'ndan 1988 yılında Levazım Teğmen olarak mezun olduktan sonra bir yıl süreyle Levazım Okulu-İSTANBUL'da mesleki eğitim görmüştür. Sırasıyla 1 nci Komando Tugayı-KAYSERİ, 5 nci Komando Alayı-GÖKÇEADA ve 7 nci Kolordu Komutanlığı-DİYARBAKIR ve Lv. Mly. Okl. ve Eğt. Mrk. K.lığı - İSTANBUL'da; Takım Komutanlığı, Saymanlık, Levazım Müdürlüğü, Bölük Komutanlığı, Genel Taktik ve Askeri Kültür Öğretmenliği görevlerinde çalışmıştır. Görev yaptığı yıllarda İç Güvenlik Harekatı ve K.İrak'ta icra edilen sınır ötesi harekatlara katılmıştır.

Halen Levazım Maliye Muharebe Laboratuvar Başkanlığında Proje Üretim ve Yönetim Şube Müdürü olarak görev yapmaktadır. 1999 yılında ABD'de Savunma Dil Enstitüsünde İngilizce öğrenimi, 2001 yılında ise yine ABD'de Havadan İkmal Kursu görmüştür. Mesleki alanda; yayınlanmış kitapları ve çeşitli askeri dergilerde makaleleri vardır.

Harp Okulu yıllarından başlayarak lojistik, taktik, strateji, siyasi tarih, jeopolitik, yönetim gibi konulara ilgisinden dolayı Gebze Yüksek Teknoloji Enstitüsü Strateji Anabilim Dalı Bilim ve Teknoloji Stratejileri Bölümünde Yüksek Lisans Programını takip etmiştir.

Dr.Zeynep İlknur ÖZDEMİR ile evli olup, bir çocuğu (L.Egehan) vardır. İngilizce bilmektedir.

EKLER

Ek 1. Ulusal Bilgi Güvenliđi Teřkilatı ve Grevleri Hakkında Kanun Tasarısı Taslađı

EK-1**ULUSAL BİLGİ GÜVENLİĞİ TEŞKİLATI VE
GÖREVLERİ HAKKINDA KANUN TASARISI
TASLAĞI****BİRİNCİ BÖLÜM****Amaç, Kapsam ve Tanımlar****Amaç**

Madde 1- Bu Kanunun amacı; ulusal güvenliği ilgilendiren bilgilerin korunması, Devletin bilgi güvenliği faaliyetlerinin geliştirilmesi, gerekli politikaların üretilmesi ve belirlenmesi, kısa ve uzun dönemli planların hazırlanması, kriter ve standartlarının saptanması, ihracat ve ithalat izinlerinin ve sertifikalarının verilmesi, bilgi sistemlerinin teknolojiye uyumunun sağlanması, uygulamanın takip ve denetimi kamu ve özel kurum ve kuruluşların arasında koordinasyonun sağlanması amacıyla bir teşkilatın kurulması ve görevlerine ilişkin esas ve usulleri düzenlemektir.

Kapsam

Madde 2- Bu Kanun, ulusal güvenliği ilgilendiren bilgiye işlem yapan kamu ve özel kurum ve kuruluşları ile yerel yönetimleri, kamu kurumu niteliğindeki meslek kuruluşlarını, üniversiteleri, bu yerlerde çalışan personeli, diğer tüzel ve gerçek kişileri, bilgi güvenliğinden faydalananları ve faydalananacak durumda olanları kapsar.

Tanımlar

Madde 3- Bu kanunda geçen deyimlerden;

a) Ulusal Bilgi Güvenliği; Ulusal güvenliği ilgilendiren, yetkisiz ellere geçtiği takdirde devletin güvenliğini tehlikeye sokabilecek veya devlet aleyhine



EK-1 (Devam)

kullanılabilecek her türlü bilgiyi, üretim, kullanım, işleme saklanma , nakledilme ve imha sırasında yetkisiz kişilerin erişimine ve olası her türlü fiziksel ve elektronik müdahaleye karşı korumaya; bilgiye erişim ve kullanıma ait usulleri açık şekilde belirlemeye ve bilgiyi gerektiğinde hazır bulundurmaya yönelik tedbirleri,

b) Haberleşme Güvenliği: Ulusal güvenliği ilgilendiren bilginin özellikle telekomünikasyon kanallarından gönderilmesi sırasında yetkisiz kişiler tarafından elde edilmesinde ve içeriğinin açığa çıkarılmasına ve diğer her türlü müdahaleye karşı alınan tüm tedbirleri,

c) Fiziki Güvenlik: Ulusal güvenliği ilgilendiren bilgiyi ihtiva eden ya da bu bilgiye işlem yapan cihaz, malzeme ve tesisi, yetkisiz kişilerin erişimine karşı korumak üzere alınan fiziksel tedbirleri,

d) Personel Güvenliği: Ulusal güvenliği ilgilendiren bilgiye yalnızca yetki verilen kişilerin, bilmeleri gerektiği oranda erişebilmeleri için alınan tüm tedbirleri,

e) Teknik Güvenlik: Yurt içinde ve yurt dışında personel, araç, donanım ve binalarda dinleme ve gözetleme amacıyla yapılan teknik yerleşmelere karşı alınan tüm güvenlik tedbirlerini,

f) TEMPEST: Tüm elektronik teçhizattan ve bunların kuruluşundan iletkenlik ve ışıma yoluyla istem dışı yayılan bilginin önlenmesine ilişkin alınan tedbirleri,

g) Güvenlik Hali: Bilginin güvenliğinin bilerek veya istenmeyerek yapılan herhangi bir işlem nedeni ile tamamen ya da kısmen ortadan kaldırılmasını,

h) Kripto: Birbirleriyle haberleşen iki tarafın, haberleşmesi esnasında üçüncü tarafa bilgi sızdırmamak amacıyla bilginin gizlenmesini sağlayan sistemleri,

i) Kriptoloji: Kriptografi ve kripto analiz konuları ile ilgilenen bir bilim dalını,

j) Kripto Sistemleri: Şifreleme ve şifre çözme etkinliklerinden birisini veya



EK-1 (Devam)

ikisini birden yerine getirmeye yarayan, bu sistemler kapsamında veri iletişimi de dahil olmak üzere her türlü iletişim sistemlerinde kullanılan sistemleri

k) Kriptografik Algoritma: Bir bilginin gizlenmesi için yapılan matematiksel bir işlemi,

l) Ulusal Bilgi Ağı: Kamu ve özel kuruluşlarda ulusal güvenliği ilgilendiren bilgiye işlem yapan mevcut terminalleri, bilgi teatisi maksadıyla birbirine bağlayan ağı,

m) Üst Kurul: Ulusal Bilgi Güvenliği Üst Kurulunu

n) Kurum: Ulusal Bilgi Güvenliği Kurumu Başkanlığını ifade eder

İKİNCİ BÖLÜM

Kuruluş ve Görevler

Kuruluş

Madde 4- Ulusal bilgi güvenliğinin sağlanması amacıyla başbakanlığa bağlı Ulusal Bilgi Güvenliği Üst Kurulu ile tüzel kişiliğe sahip katma bütçeli Ulusal Bilgi Güvenliği Kurumu Başkanlığı kurulmuştur.

Ulusal Bilgi Güvenliği Üst Kurulu

Madde 5- Ulusal Bilgi Güvenliği Üst Kurulu ; Ulusal bilgi güvenliği alanında genel direktif organı olup, başbakanın başkanlığında; Adalet, Milli Savunma, İçişleri, Dışişleri, Ulaştırma, Sanayi ve Ticaret Bakanları ile Milli Güvenlik Kurulu Genel Sekreteri, Genelkurmay Muharebe Elektronik ve Bilgi Sistemleri Başkanı, Milli İstihbarat Teşkilatı Müsteşarı, Türkiye Bilimsel ve Teknik Araştırma Kurumu ile kurum başkanından oluşur. Başbakanın katılmadığı hallerde üst kurula, Adalet Bakanı başkanlık eder. Üst kurulun daimi üyeleri tarafından ihtiyaç duyulduğu hallerde, diğer bakanlar ile kamu ve özel kurum ve kuruluşlarının temsilcileri de üst



EK-1 (Devam)

kurul toplantılarına katılabilir. Üst Kurulun toplantı yeter sayısı daima üyelerin ikisidir. Kararlar, toplantıya katılan daimi üyelerin oy çokluğu ile alınır. Toplantılara katılmaları uygun görülen diğer kişilerin oy hakkı yoktur. Üst Kurul, Nisan ve Ekim aylarında olmak üzere, yılda iki defa olağan olarak toplanır. Üst Kurulun gündemi, Başbakan tarafından belirlenir. Başbakan, daimi üyelerden birisinin talebi üzerine, Üst Kurulu olağanüstü toplantıya çağırabilir. Üst Kurulun sekreteryası hizmetleri, kurum tarafından sağlanır.

Ulusal Bilgi Güvenliği Kurumu Başkanlığı

Madde 6- Ulusal Bilgi Güvenliği Kurumu Başkanlığının teşkilatı, aşağıda isimleri belirtilen ana hizmet birimlerinden oluşur:

- a) Plan Program ve Koordinasyon Daire Başkanlığı,
- b) Bilgi Güvenliği Daire Başkanlığı,
- c) Kriptoloji Daire başkanlığı,
- d) Bilgi Destek Daire Başkanlığı,
- e) Denetleme ve Bilgilendirme Daire Başkanlığı,

Kurumun danışma birimi, Uluslararası İlişkiler ve Hukuk Müşavirliği; yardımcı birimleri ise, Ulusal Bilgisayar Güvenliği Merkezi Müdürlüğü ve Genel Sekreterliktir. Kurumun teşkilatı Ek'li cetvelde gösterilmiştir.

Ulusal Bilgi Güvenliği Üst Kurulunun Görevleri

Madde 7- Ulusal Bilgi Güvenliği Üst Kurulunun görevleri aşağıda belirtilmiştir:

a) Ulusal bilgi güvenliğine yönelik tehdidi değerlendirmek, ulusal bilgi güvenliği siyasetinin tayini, tespiti ve uygulamasıyla ilgili kararları almak ve kuruma bu konuda direktif vermek,

b) Tespit edilen ulusal bilgi güvenliği siyasetine ilişkin kararlar doğrultusunda yapılan uygulamaları incelemek, değerlendirmek ve yönlendirmek,

EK-1 (Devam)

c) Ulusal bilgi güvenliğine ilişkin mevzuat değişikliği tekliflerini değerlendirmek.

Ulusal Bilgi Güvenliği Kurumu Başkanlığının Görevleri

Madde 8- Ulusal Bilgi Güvenliği Kurumu Başkanlığının görevleri aşağıda belirtilmiştir:

a) Ulusal bilgi güvenliğine karşı yurt içi ve yurt dışı tehdidin tespit edilmesini sağlamak, gerekli tedbirleri almak ve alınmasını sağlamak,

b) Ulusal bilgi güvenliği sistemini oluşturmak için politika, konsept, ilke, standart ve usulleri tespit etmek ve geliştirmek,

c) Ulusal bilgi güvenliğinin sağlanmasına esas olarak bilginin gizlilik, bütünlük ve kullanıma hazır olmasını sağlayacak tedbirleri belirlemek, uygulamak, uygulanmasını sağlamak ve kontrol etmek,

ç) Ulusal bilgi güvenliği risk yönetimi ve değerlendirmesini yapmak ve yapılmasını sağlamak,

d) Ulusal bilgi güvenliği alt yapısını korumak amacıyla gerekli görülecek ulusal bilgi güvenliği sistemi esaslarını tespit ederek kurmak ve geliştirmek,

e) Ulusal bilgi güvenliği sisteminin mimarisinin oluşturulmasında caydırma, koruma, ikaz, tespit, onarım ve tedbir unsurlarını belirlemek,

f) Ulusal bilgi güvenliği ile ilgili uluslararası mevzuat ve teknolojiye gelişmeleri takip etmek,

g) Güvenlik hassasiyeti gösteren personel, yazılım, donanım, kripto, iletişim ortamlarını ve iletişim ağlarını her türlü tehdit kaynağına karşı maliyet etkin

EK-1 (Devam)

tedbirlerle koruma altına alınmasını sağlamak, bu tedbirleri uygulamaya sokmak ve kontrol etmek,

h) Ulusal bilgi güvenliğine ilişkin güvenlik kategorilerini ve sistemin minimum güvenlik ihtiyaçlarını belirlemek, uygulamasını sağlamak,

i) Tüm gizlilik dereceli ve tasnif dışı hassas bilgiye işlem yapacak birimler ve sebekeler için onay vermek,

j) Ulusal güvenliği ilgilendiren bilgiye işlem yapacak donanım ve yazılım ihtiyaçlarına ait güvenlik değerlendirmesini yapmak ve değerlendirilmiş ürün listelerini hazırlamak ve yayımlamak,

k) Haberleşme güvenliği sistemlerinin tehdit analizi ve hassasiyet değerlendirmelerini yapmak,

k) Hassas ve gizlilik dereceli bilgiyi korumak üzere, anahtarlama materyali üretim esaslarını belirlemek,

l) TEMPEST standartlarını hazırlamak ve onay işlemlerini gerçekleştirmek,

m) Kripto sistemlerinde kullanılacak materyal ve anahtarları üretecek teçhizatı onaylamak, kripto anahtarlarının dağıtılmasına ilişkin standartları ve yöntemleri belirlemek ve denetlemek,

n) Ulusal bilgi güvenliği gerekleri, ihtiyaçlar, ticaret ve gizlilik arasında uygun bir denge kurarak kriptolojik malzemelerin ihracat ve ithalatıyla ilgili Genelkurmay Başkanlığı ve Dışişleri Bakanlığı'nın uygun görüşleri alınarak gerekli lisansları vermek,

o) Ulusal bilgi güvenliği ile ilgili mevzuat değişikliklerine ilişkin teklifleri Üst Kurula sunmak,

EK-1 (Devam)

- ö) Bilgi çağının gerektirdiği çağdaş güvenlik tedbirlerini belirleyerek Üst Kurula teklif etmek,
- p) Üst Kurulun almış olduğu karar ve direktifleri uygulamak,
- r) Ulusal bilgi güvenliği amacıyla, Genelkurmay Başkanlığı ve Dışişleri Bakanlığı ile koordineli olarak diğer ülkelerle ve uluslararası kuruluşlarla işbirliği yapmak, sistemlerin, nihai sistem güvenlik kriterlerini belirlemek ve onay işlemlerini yapmak.
- s) Ulusal bilgi güvenliği konusunda eğitim standartlarını belirlemek, plan ve programları yapmak,
- t) Ulusal bilgi güvenliği konusunda araştırma ve geliştirme faaliyetlerini sağlamak,
- u) Kamu ve özel kurum ve kuruluşlar için gizlilik dereceli bilgi veya kripto cihazlarına ilişkin her türlü yetki belgesi (klerans) düzenlemek ve onay yöntem ve usullerini belirlemek, uygulanmasını sağlamak,
- ü) Ulusal bilgi güvenliği konusunda üretim yapan kamu ve özel kurum ve kuruluşlarını bir program çerçevesinde denetlemek ve üretilen ürünleri onaylamak.

Uluslararası İlişkiler ve Hukuk Müşavirliği

Madde 9- Uluslararası İlişkiler ve Hukuk Müşavirliği, Kurum Başkanına doğrudan bağlı olup görevleri aşağıda belirtilmiştir :

- a) Uluslararası Bilgi Güvenliği politikasının oluşturulmasında uluslararası ilişkileri ve gelişmeleri takip etmek, değerlendirmek, koordine etmek ve önerilerde bulunmak, gerekli kanun tasarısı taslaklarını hazırlamak,
- b) Ulusal bilgi güvenliği konusunda Kurum tarafından hazırlanan veya

EK-1 (Devam)

Başbakanlık, Bakanlıklar ve kuruluşlardan gönderilen kanun, tüzük ve yönetmelik Taslaklarını hukuki açıdan inceleyerek, görüş bildirmek,

c) Ulusal Bilgi Güvenliğine ilişkin konularda altyapı teminat modelinin oluşturulması ve altyapının güvenilirliğinin sağlanarak kullanıma hazır tutulması için gerekli yasal düzenlemeleri ve sözleşmeleri hazırlamak,

d) Bireysel mahremiyeti koruma ve birey için gerekli kamu bilgisine erişimi sağlayıcı yasal düzenlemeleri belirlemek,

e) Uluslararası bilişim güvenliğine ilişkin suçların mevzuatımızda yer alması için gerekli kanun tasarısı taslaklarını hazırlamak,

f) 4353 sayılı kanun hükümlerine göre adli ve idari davalara ilişkin gerekli bilgileri hazırlamak, Maliye Bakanlığı Başhukuk Müşavirliği ve Muhakemat Genel Müdürlüğünü ilgilendirmeyen idari davalarda kurumu temsil etmek,

g) Uluslararası Bilgi Güvenliği tehdide uğradığı hallerde ekonomik kısıtlama, diplomatik yanıt gibi tedbirlerin kullanımını Dışişleri Bakanlığı ve ilgili Bakanlıklarla koordine etmek ve önerilerde bulunmak,

h) Kurum tarafından verilen diğer görevleri yapmaktır.

Ulusal Bilgi Güvenliği Merkezi

Madde 10- Ulusal Bilgi güvenliği merkezinin görevleri aşağıda belirtilmiştir :

a) Güvenli bilgi sistemlerinin geniş bir şekilde, kullanımını teşvik etmek,

b) Endüstri ve Kamu tarafından geliştirilmiş sistemlerin, teknik koruma yeteneklerini değerlendirmek,

c) Bilgi güvenliği konusunda faaliyet gösteren, kamu ve endüstri gruplarının teknik desteğini sağlamak,

EK-1 (Devam)

- d)** Bilgi sistemlerinin değerlendirilmesi için, gerekli teknik kriterleri geliştirmek,
- e)** Ticari sistemleri değerlendirmek,
- f)** Bilgisayar ve Ağ Güvenlik teknoloji araştırmalarını icra ve yönlendirmek,
- g)** Güvenli Bilgi Sistemlerini geliştirme ve test etmede kullanmak için, gerekli modifikasyon ve analiz techizatını geliştirmek ve bilişim emniyetini sağlamak,
- h)** Bilgi güvenliği sahasında eğitim vermek,
- i)** Kamu ve Endüstrinin diğer bölümlerine bilgi güvenlik bilgisini dağıtmak,
- j)** Tehdidin türüne göre geliştirilen karşı tedbirleri gerektiğinde uygulamaya koymak,

Genel Sekreterlik

Madde 11- Genel Sekreterliğin Görevleri Aşağıda Belirtilmiştir :

- a)** Kurum Başkanının resmi ve özel yazışmalarını yürütmek,
- b)** Kurumun idari, bakım-onarım ve idame hizmetlerine ilişkin görevlerini yürütmek,
- c)** Kurumun maliye ve satın alma hizmetlerini sağlamak,
- d)** Kurumun güvenlikle ilgili hizmetlerini yürütmek,
- e)** Üst Kurulun sekreteryasını yapmak,

ÜÇÜNCÜ BÖLÜM

ANA HİZMET BİRİMLERİ VE GÖREVLERİ

Plan, Program ve Koordinasyon Dairesi Başkanlığı

EK-1 (Devam)

Madde 12- Plan, Program ve Koordinasyon Dairesi Başkanlığının Görevleri aşağıda belirtilmiştir :

a) Telekomünikasyon ve Bilgi sistemleri ortamındaki değişimlere uyum sağlayacak Ulusal bilgi güvenliği politikasının oluşturulması için gerekli verileri hazırlamak, prensipleri belirlemek,

b) Ulusal Bilgi güvenliği ile ilgili olarak görev alanına ilişkin planlama ve programlama faaliyetlerinde bulunmak, gerekli mevzuatı düzenlemek,

c) Ulusal Bilgi güvenliği altyapı esaslarını ortaya koymak yapılmış olan risk analizleri neticelerine göre altyapıyı iyileştirici tedbirleri belirlemek

d) Uyuşum standartları ve kriterlerini ortaya koymak,

e) Ulusal Bilgi güvenliği konusunda bilgilendirme ve eğitim faaliyetlerini planlamak,

f) Kamu ve özel sektöre Ulusal bilgi güvenliğine ilişkin danışmanlık ve teknik yardım sağlamak,

g) Kurumun personel faaliyetlerini yürütmek ve koordine etmek,

h) Ulusal Bilgi Güvenliği Başkanlığının bütçe düzenleme faaliyetlerini yürütmektir.

Bilgi Güvenlik Dairesi Başkanlığı

Madde 13- Bilgi Güvenlik Dairesi Başkanlığının görevleri aşağıda belirtilmiştir:

a) Ulusal bilgi Güvenliği ihlallerine karşı alınacak tedbirleri belirlemek, ihlallere karşı gerekli tedbirleri almak ve ilgili makamlarla koordineli olarak uygulanmasını sağlamak,

b) Ulusal Bilgi güvenliği açısından Personel güvenliğine, fiziki güvenliğe ve

EK-1 (Devam)

donanım ve yazılım güvenliğine ilişkin usul, kriter ve prensipleri belirleyerek dökümantasyonunu hazırlamak,

c) Kurumun, ulusal bilgi ağı TEMPEST, haberleşme güvenliği ve teknik güvenliğine ilişkin usul, kriter ve prensiplerini belirleyerek dökümantasyonunu hazırlamak,

d) Elektronik kriptu dışında ihtiyaç duyulacak kod ve parola sistemlerini belirlemek, geliştirmek ve üretmek,

e) İletişim ortamları, donanım ve ağlar için tehdidi ve zafiyeti dikkate alarak risk analizleri yapmak, ve risk yönetim usullerini belirlemek, risk analizleri sonucunda belirlenmiş koruyucu tedbirleri uygulamaya koymak,

f) Yazılım güvenlik, kriter ve standartlarını belirlemek,

g) Ulusal ve uluslararası iletişim ağlarına ilişkin olarak ulusal bilgi güvenliği açısından güvenlik, usul, kriter ve prensipleri belirlemek, dökümantasyonunu sağlamak,

h) Güvenlik denetimlerine ilgi alanı itibariyle katılmak, alt kurullara sekreteryahizmeti vermek ve görev alanına ilişkin mevzuat değişikliklerine ilişkin teklifleri hazırlamaktır.

Kriptoloji Dairesi Başkanlığı

Madde 14- Kriptoloji Dairesi Başkanlığının görevleri aşağıda belirtilmiştir :

a) Kriptografik algoritma, ihtiyaçlarını belirlemek, üretiminin denetimini yapmak ve kütüphanesini oluşturmak,

b) Kripto cihaz ve kriptografik bilginin ihracat ve ithalatında Genelkurmay Başkanlığı, Dışişleri Bakanlığı ve gerektiğinde ilgili diğer bakanlıklarla koordineli olarak esas ve usulleri belirlemek, lisans belgesi vermek,

Kaynak: ttnet web sitesi (www.ttnet.net)

EK-1 (Devam)

c) Risk analizleri ve risk azaltma planları yapmak , kabul edilebilir riski tespit etmek,

d) Kripto merkezlerinin sağlaması gereken kriterlerini ve denetleme usul ve esaslarını belirlemek, denetleme raporlarını değerlendirerek onay vermek, kripto anahtar üretimi ve dağıtımını yapmak, gerektiğinde kurum ve kuruluşlara kendi kripto anahtar üretimi ve dağıtımını konusunda yetki vermek,

e) Gizlilik derecesiz uygulamalarda da kripto kullanım esaslarını belirlemek, uygulamaları teşvik etmek ve denetlemek,

f) Kripto cihaz ve dökümantasyonu için, kripto saymanlık, işletme, bakım ve onarım usullerini belirlemek,

g) Kripto ihlallerine karşı alınacak tedbirleri belirlemek ve gerekli tedbirleri almak,

h) Her tür kriptografik yöntem ve teçhizata ilişkin sertifikasyon ve onay usullerini belirlemek,

i) Kripto hizmetlerinde çalıştırılacak personele kripto yetki belgesi verilmesi esas ve usullerini belirlemektir.

Bilgi Destek Dairesi Başkanlığı

Madde 15- Bilgi Destek Dairesi Başkanlığının görevleri aşağıda belirtilmiştir;

a) Ulusal bilgi güvenliği altyapısına karşı iç ve dış tehdidi teşhis etmek, tanımlamak, genel tehdit değerlendirilmesi yapmak ve Üst Kurula sunmak,

b) Ulusal bilgi güvenliğine karşı tehdidin teknik özelliklerini ve muhtemel etkilerini belirlemek, karşı tedbirleri geliştirmek,

EK-1 (Devam)

- c) İstihbarat üreten kurum ve kuruluşlar ile bilgi güvenliğine ilişkin istihbarat bilgisi değişimi için protokoller yapmak,
- d) Mevcut ve tasarlanan iletişim ortamları, donanım ve ağlar için tehdidi ve zafiyeti dikkate alarak risk analizleri yapmaktır.

Denetleme ve Değerlendirme Dairesi Başkanlığı

Madde 16- Denetleme ve Değerlendirme Dairesi Başkanlığının görevleri aşağıda belirtilmiştir;

- a) Ulusal bilgi güvenliği açısından kriptoloji, bilgi güvenlik ve TEMPEST denetleme kriter ve usullerini belirlemek ve geliştirmek,
- b) Kriptoloji denetleme programlarını hazırlamak, kriptoloji merkezlerinin kriterlere uygunluğunun denetlemesini sağlamak, gerektiğinde denetlemek ve denetleme raporlarını değerlendirmek,
- c) Ulusal bilgi güvenliği sistemlerine karşı yapılan saldırıları ve güvenlik ihlallerini değerlendirmek,
- d) Eğitim, öğretim ve biçimlendirme ihtiyaçlarını tespit etmek,
- e) Genel değerlendirme raporu hazırlayarak Üst Kurula sunmak,
- f) İletişim ortamları, şebeke, yazılımlara ait güvenlik sistemleri ile ilgili denetleme usul ve kriterlerini belirlemek, geliştirmek, denetleme yapılmasını sağlamak, gerektiğinde denetlemek ve denetleme raporlarını değerlendirmek,
- g) TEMPEST standartlarını hazırlamak ve onay işlemlerini gerçekleştirmek,
- h) Ulusal bilgi güvenlik alt yapısına ait sistemlerin nihai sistem güvenlik kriterlerini belirlemek ve onay işlemlerini yapmak.

EK-1 (Devam)

DÖRDÜNCÜ BÖLÜM

Çeşitli Hükümler

Gizlilik Dereceleri

Madde 17- Bilgi güvenliğinin sağlanmasından kullanılacak gizlilik dereceleri ile hangi makam tarafından ne şekilde verileceği hususları Kurum tarafından çıkartılacak yönetmelikte düzenlenir.

Kamu ve Özel Kurum ve Kuruluşlarının Yükümlülüğü

Madde 18- Tüm kamu ve özel kurum ve kuruluşları, ulusal güvenliği ilgilendiren bilginin korunması için kendi idari yapıları içerisinde gereken organizasyonu kurmak veya değişiklikleri yapmak ve gerekli tedbirleri almak konusunda sorumludurlar.

Ulusal bilgi güvenliği, tüm kamu ve özel kurum ve kuruluşlarda bir bütün olarak değerlendirilir ve gerekli koordinasyon Kurum tarafından sağlanır. Bu amaca yönelik tüm kaynaklar yerinde, zamanında ve en etkin bir şekilde kullanılır. Kamu ve özel kurum ve kuruluşları, Kurum tarafından bu Kanunun uygulanmasına ilişkin olarak yayımlanan esas ve usullere uymak zorundadır.

Kurum, gerekli gördüğü ulusal bilgi güvenliğinin sağlamaya ilişkin bilgileri, bu Kanun kapsamına giren kamu ve özel kurum ve kuruluşlardan doğrudan istemeye yetkilidir. Bu konuda istenen gizlilik dereceli her türlü bilgi, makam onayı ile en kısa zamanda verilir. Özel kanunlardaki hükümler saklıdır.

Kişi ve Kurumların Hizmetlerinden Yararlanma

Madde-19 Genel ve katma bütçeli idareler, kamu iktisadi teşebbüsleri ile bunlara bağlı kuruluşlar ve müesseselerde çalışanlar, Kurumda sözleşmeli olarak istihdam edilebilirler. Bu personel kurumundan aylıksız izinli sayılır. İzinli oldukları sürece

EK-1 (Devam)

memuriyetleri ile ilgili özlük hakları devam ettiği gibi bu süreler terfi ve emekliliklerinde hesaba katılır. Kurumda çalıştıkları sürece bunların sicilleri Kurum tarafından verilir ve bu sicillere göre kendi kurum ve kuruluşlarınca terfileri yapılır. Bu personelin, çalışma usul, esas, ücret ve sayılarına ilişkin hususlar, Bakanlar Kurulu Kararıyla tespit edilir. Ancak bu personelin aylıkları, hiç bir halde kendi kurum ve kuruluşlarında aldıkları aylıklardan az olamaz.

Birinci fıkrada belirtilen kurum ve kuruluşlarda görevli personel, gerektiği hallerde aylık, ek gösterge, ödenek, her türlü zam ve tazminatlar ile diğer mali ve sosyal hak ve yardımları kendi kurumlarınca ödenmek tabi oldukları kanun hükümleri çerçevesinde geçici olarak Kurumda görevlendirilebilirler.

Kadrolar ve Personel

Madde 2- Kadroların tespit, ihdas, kullanım ve iptali ile kadrolara ait diğer hususlar, 190 sayılı Genel Kadro ve Usulü Hakkında Kanun Hükmünde Kararname hükümlerine göre düzenlenir.

Kurumda başkan, başkan yardımcıları, hukuk müşavirleri, daire başkanları, şube müdürleri, mühendisler ve yüksek öğrenim görmüş olanlar, kadro karşılık gösterilmek kaydıyla 657 sayılı Devlet Memurları Kanunu ve diğer kanunların sözleşmeli personel hakkındaki hükümlerine bağlı olmaksızın sözleşmeli olarak çalıştırılabilir. Kurumda başkan, başkan yardımcıları ve daire başkanları olarak atanacak personelde bu sahada en az lisans düzeyinde eğitim yapmaları ve kamu kurum ve kuruluşlarında Kurumun ilgi alanını oluşturan görevlerde en az 10 yıl görev yapmış olmaları şartı aranır.

Bu şekilde çalıştırılacak sözleşmeli personelin sayısı, sözleşme usul ve esasları Başbakanlıkça tespit edilir. Sözleşme ile çalıştırılacak personel, istekleri üzerine Türkiye Cumhuriyeti Emekli Sandığı ile ilgilendirilir.

Atama

Madde 21- Kurum Başkanı, başkan yardımcıları, birinci hukuk müşaviri ve daire başkanları sözleşmeli olarak çalıştırılmadıkları takdirde, haklarında 657 sayılı Devlet Memurları Kanununun istisnai memuriyete ilişkin hükümleri uygulanır. Bunlardan Başkan, Başbakan'ın onayı ile; diğer personel ise, Başkanın onayı ile atanır.

Sözleşme ile Araştırma, Etüd, Proje ve Program Yaptırma

Madde 22- Kurumun hizmetlerine ilişkin araştırma, etüd, proje ve program işleri, üniversiteler ile gerçek ve tüzel kişilere sözleşme ile yaptırılabilir.

Kurumun gelirleri

Madde 23- Kurumun gelirleri aşağıda belirtilmiştir;

- a) Genel bütçeden yapılacak hazine yardımı
- b) Döner sermaye gelirleri

Döner Sermaye İşletmesi

Madde 24- Kurumda, bu Kanunda öngörülen faaliyet temel ve sürekli görevlere bağlı olarak ortaya çıkan üretim ve hizmet fazlasının değerlendirilmesi amacıyla döner sermaye işletmesi kurulabilir.

Döner sermaye işletmesinin sermaye limiti 2.5 trilyon Türk Lirasıdır. Tahsis edilen sermaye miktarı, Maliye Bakanlığının uygun görüşü üzerine Bakanlar Kurulunca on katına kadar artırılabilir. Bu suretle artırılan sermaye, elde edilen gelirle karşılanır.

Döner sermaye, Başbakanlık bütçesine konulan ödenekle, Hazinece verilecek aynı yardımlar, döner sermaye gelirinden elde edilecek karlar, bağış ve yardımlardan oluşur.

Ödenmiş sermaye tutarı, tahsis edilen sermaye tutarına ulaştıktan sonra elde

Kaynak: ttnet web sitesi (www.ttnet.net)

EK-1 (Devam)

edilen karlar, hesap dönemini izleyen yılın Şubat ayı sonuna kadar Hazineye gelir kaydedilmek üzere Kurum saymanlığına yatırılır.

Döner sermaye faaliyetlerinin gerektirdiği giderler ile Bütçedeki ödenekten karşılanamayan kiralama, satın alma, araç, gereç, araştırma ve benzeri diğer ihtiyaçlar döner sermayeden karşılanır.

Döner sermaye işletmesinin faaliyet alanları, gelir kaynakları, mali ve idari işlemlerine ilişkin usul ve esaslar Maliye Bakanlığı ile Sayıştay'ın görüşleri alınarak hazırlanacak yönetmelikle düzenlenir.

Döner sermaye işleri 1050 ve 832 sayılı Kanunların vizeye ilişkin hükümlerine tabi değildir. Ancak gelir ve giderler için bütçe yılı sonundan itibaren 3 ay içinde düzenlenecek yıllık bilançolar ve ekleri gelir ve gider belgeleri ile birlikte Sayıştay Başkanlığına, tasdikli birer sureti de Maliye Bakanlığına gönderilir.

Ceza Hükümü

Madde 25- Kamu ve özel Kurum kuruluşların yöneticisi durumunda olan personelden, bu kanunun 18. maddesinde belirtilen yükümlülükleri yerine getirmeyenler, bu fiilleri başka bir suça vücut verse bile ayrıca bir yıldan beş yıla kadar hapis cezası ile cezalandırılırlar. Failin bu fiilden kendisi veya bir başkası yararına bir menfaat temin etmesi veya fiilin bir zarara sebebiyet vermesi halinde hapis cezası iki yıldan az olamaz.

Geçici Madde 1- Üst Kurul ile Kurumun çalışma usul ve esasları dairelerin alt birimlerinin kuruluş ve görevlerine ilişkin usul ve esaslar, Döner sermaye işletmesine ilişkin usul ve esaslar ile Kanunun uygulanmasında ihtiyaç duyulacak usul ve esaslar, Kanunun yürürlüğe girdiği tarihten itibaren bir yıl içinde Kurum tarafından hazırlanacak ve Bakanlar Kurulu kararıyla yürürlüğe konulacak yönetmeliklerde gösterilecektir.

EK-1 (Devam)



Geçici madde 2- Ekli (1) sayılı listede belirtilen kadrolar ihtas edilerek 190 sayılı Kanun hükmünde Karanamenin (1) sayılı cetveline "Ulusal Bilgi Güvenliği Üstkurulu ile Ulusal Bilgi Güvenliği Kurumu Başkanlığı" bölümü olarak eklenmiştir.

Geçici Madde 3- Bu Kanunun kabulü ile asgari ihtiyaçları karşılayacak çekirdek kadro ile faaliyete geçirilecek kendi ihtiyaçları doğrultusunda azami üç yıl içinde nihai teşkilatını kuracaktır.

Yürürlük

Madde 26- Bu Kanun yayımı tarihinde yürürlüğe girer.

Yürütme

Madde 27- Bu Kanun hükümlerini Bakanlar Kurulu yürütür.

EK-A DEVAMI EK (1) SAYILI CETVEL

ULUSAL BİLGİ GÜVENLİĞİ KURUMU BAŞKANLIĞI TEŞKİLATI

i) BAŞKANLIK

Başkan

ii) DANIŞMA BİRİMLERİ

Uluslar arası İlişkiler ve Hukuk Müşavirliği

iii) ANA HİZMET BİRİMLERİ

1. Plan Program ve Koord. D.Bşk.lığı

2. Bilgi Güvenlik D.Bşk.lığı

3. Kriptoloji D.Bşk.lığı

4. Bilgi Destek D.Bşk.lığı

5. Denetleme ve Değerlendirme D.Bşk.lığı

iv) YARDIMCI BİRİMLER

1. Ulusal Bilgisayar Güvenlik Merkezi Müdürlüğü

2. Genel Sekreterlik

EK-1 (Devam)

MADDE GEREKÇELERİ

Madde 1- Madde ile, Kanunun düzenlenme amacı belirtilmektedir.

Madde 2 - Madde ile, Kanunun kapsamı belirtilmektedir.

Madde 3 - Madde ile, Kanunda yer verilen deyimlerden ulusal bilgi güvenliği, haberleşme güvenliği, fiziki güvenlik, personel güvenliği, teknik güvenlik, TEMPEST, güvenlik ihlali, kriptoloji, kriptoloji, kriptoloji sistemleri, algoritma, ulusal bilgi ağı, üst kurul, kurum terimleri açıklanmaktadır.

Madde 4 - Madde ile Ulusal Bilgi Güvenliği Üst Kurullu ile Başbakanlığa bağlı olarak Ulusal Bilgi Güvenliği Kurumu Başkanlığının kuruluşu düzenlenmektedir.

Madde 5 - Madde ile, Ulusal Bilgi Güvenliği Üst Kurulunun asil üyelerinin kimlerden oluştuğu, Üst Kurula başkanlık usulü, diğer kamu ve özel kurum ve kuruluşların temsilcilerinin katılım durumu, oy verme ve karar yeter sayısı, olağan toplantı tarihleri, gündem, olağanüstü toplantıya çağrı usulü, sekreter ya hizmetleri düzenlenmekte ve üst Kurulun çalışma usul ve esaslarının daha sonra çıkarılacak Yönetmelikle düzenleneceği belirtilmektedir.

Madde 6- Madde ile, Ulusal Bilgi Güvenliği Kurumu Başkanlığının alt birimlerini oluşturan daire başkanlıkları ile uluslararası ilişkiler ve hukuk müşavirliği, ulusal bilgisayar güvenlik merkezi ve genel sekreterliğin kuruluşu düzenlenmekte ve dairelerin alt birimlerinin kuruluş şekillerinin ve görevlerinin çıkarılacak Yönetmelikle düzenleneceği belirtilmektedir.

Madde 7- Madde ile, Ulusal Bilgi Güvenliği Üst Kurulunun görevleri düzenlenmektedir.

Madde 8- Madde ile, Ulusal Bilgi Güvenliği Üst Kurumu Başkanlığının görevleri düzenlenmektedir.



EK-1 (Devam)

Madde 9- Madde ile, Uluslararası İlişkiler ve Hukuk Müşavirliğinin görevleri düzenlenmektedir.

Madde 10- Madde ile, Ulusal Bilgisayar Güvenliği Merkezinin görevleri düzenlenmektedir.

Madde 11- Madde ile , Genel Sekreterliğin görevleri düzenlenmektedir.

Madde 12- Madde ile, Plan Program ve Koordinasyon Başkanlığının görevleri düzenlenmektedir.

Madde 13- Madde ile, Bilgi Güvenliği Dairesi Başkanlığının görevleri düzenlenmektedir.

Madde 14- Madde ile, Kriptoloji Dairesi Başkanlığının görevleri düzenlenmektedir.

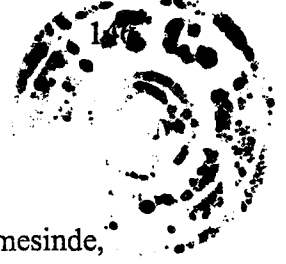
Madde 15- Madde ile Bilgi Destek Dairesi Başkanlığının görevleri düzenlenmektedir.

Madde 16 -Madde ile, Denetleme ve Değerlendirme Dairesi Başkanlığının görevleri düzenlenmektedir.

Madde 17- Madde ile, bilgi güvenliğinde kullanılacak gizlilik dereceleri ile hangi makam tarafından ne şekilde verebileceğinin Kurum tarafından çıkarılacak bir Yönetmelikle düzenleneceği belirtilmektedir.

Madde 18- Madde ile, ulusal bilgi güvenliği, tüm kamu ve özel kurum ve kuruluşlarda bir bütün olarak değerlendirildiğinden, her kurum ve kuruluşun kendi bünyesinde gereken organizasyonu oluşturması ve ulusal bilgi güvenliği konusunda belirtilen önlemlerin alınması için yükümlülük düzenlenmektedir. Belirtilen hükümlülüklerin yerine getirilmesinde özel kanunlara tabi kurum ve kuruluşlara ilişkin hükümler saklı tutulmaktadır.

EK-1 (Devam)



Madde 19- Madde ile, oluşturulan teşkilatın görevlerinin yerine getirilmesinde,

diğer kurum ve kuruluşlarının ihtiyaç duyulan hizmetlerinden ve personelinden yararlanma esasları ile söz konusu personelin mali ve sosyal hakları saklıdır.

Madde 20- Madde ile, oluşturulan teşkilatın kadroları ve bu kadrolarda görevlendirilecek personelin yasal dayanağı, sözleşmeli olarak çalıştırılacak personel, Emekli Sandığı ile ilgilendirilme ve özel uzmanlık gerektiren işlerde uzman personel çalıştırabilmesi hususları düzenlenmektedir.

Madde 21- Kurum Başkanı, daire başkanları ve birinci baş hukuk müşavirleri hakkında istisnai memurluk statüsünün uygulanması ve personelin atama onay usulü düzenlenmektedir.

Madde 22- Madde ile, oluşturulan teşkilatın yaptıracığı araştırma, etüt, program ve proje işlerinin sözleşmeyle yaptırabilmesi hususu ve ihaleyle ilgili esaslar düzenlenmektedir.

Madde 23- Madde ile, Ulusal Bilgi Güvenliği Kurumu Başkanlığının gelirleri düzenlenmektedir.

Madde 24- Ulusal Bilgi Güvenliği Kurumu Başkanlığının faaliyet alanına giren konularda gerçek ve tüzel kişilere verilecek hizmetlerin yerine getirilmesine araştırma-geliştirme faaliyetleri için gerekli olan kaynağın elde edilmesine yönelik olarak bir döner sermaye işletmesi kurulması ve bunun işletilmesi esasları düzenlenmektedir.

Madde 25- Ceza hükmü düzenlenmektedir ve kanunda belirtilen yükümlülükleri yerine getirmeyenler hakkında caydırıcı nitelikte hükümler düzenlenmektedir.

Madde 26- Yürürlük maddesidir.

Madde 27- Yürütme maddesidir.