Karadeniz Araştırmaları
XIV/55 - Güz 2017 - s.131-146
Makale gönderim tarihi: 18.04.2017
Yayına kabul tarihi: 27.07.2017

ULUSLARARASI İLİŞKİLERDE GÜVENLİĞİN DÖNÜŞÜMÜ ÇERÇEVESİNDE BİLGİ GÜVENLİĞİ VE SİBER SAVAŞ

Uğur GÜNGÖR*
Oğuzhan GÜNEY**

ÖZ
Bu makalenin amacı güvenliğin dönüşümü çerçevesinde bilgi güvenliği ve siber savaşı incelemektir. Makalenin ilk bölümünde uluslararası ilişkilerde bilgi ve güvenlik ilişkisi çerçevesinde bilginin önemi, bilgi hiyerarşisi ve bilgi güvenliğinin prensipleri ele alınmıştır. Makalenin ikinci bölümünde, savaş olgusunun geçirdiği değişim incelenmiş, bu değişimde bilgi savaşının yeri vurgulanmıştır. Üçüncü bölümde siber güvenlik ve siber savaş konusunda bilgi verilerek, siber savaşın iki önemli örneği olan Estonya ve Gürcistan siber savaşları açıklanmıştır. Makalenin sonucunda siber savaşların milli güvenliği tehdit edecek boyutlara ulaştığı ve bir güvenlik meselesi haline geldiği, bilgi güvenliğinin savaşlarda ağırlık merkezi haline geleceği vurgulanmıştır.
Anahtar Kelimeler: Bilgi Güvenliği, Siber Güvenlik, Siber Savaş, Estonya, Gürcistan

ABSTRACT
The purpose of this article is to analyse information security and cyber war within the context of transformation of security in international relations. The first part of the article examines the importance of knowledge, information hierarchy, and the basic principles of information security. The second part highlights the evolution of warfare and the place of information warfare in its evolution. This paper also investigates cyber security and cyber wars and discusses the cyber wars in Estonia and Georgia. It concludes that cyber wars will high likely threaten the national security, become a national security issue and information security will become a center of gravity in the future wars.
Keywords: Information Security, Cyber Security, Cyber Warfare, Estonia, Georgia

* Doç. Dr., Başkent Üniversitesi, İletişim Fakültesi, ORCİD: 0000-0001-5074-5949, ugungor@baskent.edu.tr
** Lisansüstü öğrenci, ogzgny@gmail.com

Uluslararası ilişkilerin dünya siyasetinde nasıl şekillendiği ve oluşan karmaşık yapıyı açıklamak için bilimsel disiplin içerisinde teorilere ihtiyaç duyulmaktadır. Teorilerin ortaya çıkması ile doğrular ile yanlışlar zaman ilerledikçe farklılaşmakta ve sağlam bir alt yapı oluşturulmaktadır. Teorik güvenlik yaklaşımları da reel dünyada olanları sadece açıklamak veya tahminler yürütmekle kalmaz, aynı zamanda olaylar ve ilişkiler ile ilgili alternatif yollar sunarak düşünsel ve pratiksel olarak ufkumuza yön verirler.

İnsanlık tarihinin başlangıcından günümüze kadar insanın doğası gereği en zeki canlı olarak kendisini görmesi en iyinin kendi olduğu fikrine kapılarak kibir sarmalına düşmesi insanlar arasındaki karşılıklı rekabet hissini oluşturan temel sebep olarak görülebilir. Pratik hayatta bu davranışsal biçim ise güvensizlik ortamına zemin hazırlar ve insanoğlunun karşılıklı amansız mücadelesi insanın olumsuz doğası gereği harekete geçer. Realizmin temel varsayımlarından birisi olan karşılıklı rekabet, insanın güvensizlik sarmalının içinde kalmasının önemli bir nedenidir.

Güvenliğin birçok alanda konuşulan olgu olması itici güç olan bilginin de güvenliğini gündeme taşımıştır. Bilgi ve teknolojiye dayanan bu hızlı dönüşüm, toplumsal koşulların değişimine neden olmuş ve bilgi güvenliği kavramının tanımlanması gerektiği tartışmalarını hızlandırmıştır. Özellikle yaşadığımız çağ için Bilgi Çağı tanımlaması yapmak doğru gibi gözükmektedir. Çünkü bireyler, kurumlar ve devletlerin bilgiyi üretmesi ile gücün doğru orantılı olarak artışı analiz edildiğinde AR-GE faaliyetlerine önem veren birey, kurum ve devletlerin gelişmişlik seviyesinin yüksek olduğu görülmektedir. Bu nedenle gelişmişlik seviyesinin sürekli zirvede tutulması adına üretilen bilginin güvenliği ön plana çıkmaktadır.

Devletlerin ve özelde bireylerin güvenliği sağlıklı toplum inşasında temel gereksinim olarak göze çarpmaktadır. Maslow piramidinde fizyolojik ihtiyaçları karşılayabilen insanın güvenlik aşamasına geçmesi güvenliği zorunlu ihtiyaca dönüştürmüştür. Aynı zamanda ihtiyaca dönüşen güvenlik algısı günümüz bilgi iletişim teknolojilerinin oluşturduğu sanal ortamlarla küresel topluma dönüşümü için güvende olma hissini zorunlu kılmaktadır. Dolayısıyla güvenlik hayatımızın her anına ve her aşamasına yerleşmiş reel bir olgudur.

Uluslararası ilişkilerde güvenlik algısı Soğuk Savaş sonrası hızla değişime uğramıştır. Geleneksel realist görüş güvenliği sadece çıkar kapsamında değerlendirirken, günümüz gelişmeleri güvenliğe daha geniş perspektiften bakan ve ulusal güvenliğe yönelik tehditleri, askeri nitelikli olmayan tehlikeleri de içeren yeni güvenlik yaklaşımlarını ortaya çıkarmıştır. Bu yaklaşım sonucu uluslararası örgütler, ulus ötesi birimler, sivil toplum kuruluşları, uluslararası şirketler ve hatta toplumun hücresel parçası bireyler de uluslararası ilişkiler analizlerinde yer bulmuştur. Aynı zamanda ekonomik, teknolojik, çevresel ve sosyal süreçlerin güvenliğe etkileri de inceleme alanları arasına girmiştir.

Bu etkileşim içerisinde akışkanlığı sağlayan ve uluslararası ilişkilerde güvenliğe doğrudan etki eden bilgi ve güvenliğinin yeni yaklaşımlar içeri-

sinde önemli etkileri olduğu gözlenmiştir. Bilgiyi veren yargıyı belirler ilkesi gereği enformasyon savaşının toplumun gerçekliği ve devletlerin yönlendirilmesinde ciddi etkileri olmaya devam edeceği beklenmektedir.

1. Bilgi ve Güvenlik İlişkisi

Bilgi, günlük hayatımızda çok kullandığımız bir kavramdır. Buna rağmen bilginin tanımını yapmak oldukça zordur. Çünkü bilgi önceleri felsefenin ilgi ve tartışma alanında yer alırken, günümüzde tüm bilim dallarının konusu haline gelmiştir. Her bilim dalı bilgiyi kendi çalışmalarına göre tanımlamaktadır. Buna karşın bilgi sadece bilim dallarına göre değil, zamana ve değişen koşullara göre de farklılaşan bir kavramdır. Önceleri bilgi insanı şekillendiren, haber değeri taşıyan bir olgu iken günümüzde bilgi bir üretim faktörüdür ve alınıp satılma özelliğine sahiptir. Genel olarak bilgi, bir seçim yapmamız söz konusu olduğunda gereksinim duyduğumuz şeydir. Değeri sürekli artan bir olgunun önemi arttıkça gizliliği bütünlüğü ve güvenliğe olan ihtiyacı da o oran da artmaktadır. Bilgi her zaman kendini güvende hissetmelidir.

a. Bilginin Tanımı ve Bilgi Hiyerarşisi

Bilgi nedir, sorusuna cevaben Russell (1970: 20-26), bilgi ve bilmek kavramlarını bir araya alıp incelemiş, bu alanda kesin bir tanım yapmanın zor ve neyin bilgi olduğu sorusu üzerinde yoğunlaşmanın gerektiğini söylemiştir. "Bilgi, kâğıt veya başka ortamlar üzerine kaydedilmiş, anlaşılabilen ve iletilebilen veriler topluluğudur" (Information, 1987: 14) veya "Zihnin herhangi bir biçimde resmi veya gayri resmi olarak iletilen, kaydedilen, yayınlanan fikirlerin gerçek ve hayali ürünleridir" (Information, 1980: 48)

"Bilgi" temel üretici güç olarak kabul edilir. Bilgi ve teknolojiye da-yanan gelişmeler, toplumsal koşulların hızlı değişimine neden olmuş güvenli-ğin tanımlanması gerektiği tartışmalarını da hızlandırmıştır. Çünkü bilgi de-ğeri sürekli yükselen bir madendir. Enformasyon ve iletişim teknolojilerindeki büyük değişim, yeni bir devrimle, "enformasyon devrimiyle tanımlanmıştır. Öne sürülen bu devrimin gerçekleştiği ortam ise "bilgi ekonomisi" kavramıyla somutlaştırılmıştır. Bilgi ekonomisi temel olarak; bilginin üretilmesine, dağıtılmasına, bilgi ve enformasyonun ekonomide kullanılmasına, ileri teknoloji yatırımlarına dönüşmesi ile birlikte bilgi güvenliği sorunsalını da beraberinde getirmiştir.

Bilginin veriler topluluğundan oluştuğu düşünüldüğünde "akıl" seviyesine gelmeden önce geçirdiği bir takım basamaklar bulunmaktadır. Bu basamaklar bilgi hiyerarşisi olarak da nitelendirilerek açıklanmaktadır. Bilgi, "karar verme, planlama, karşılaştırma, değerlendirme, analiz, tahmin, tanı vb. hayatın her alanına dayanak oluşturacak fiillerin temelini teşkil eder" (Çapar, 2003: 422). Gerek örgütsel gerekse de bireysel olarak üretilen bilginin, farklı süreçlerden geçerek bilgi halini aldığını açıklayabilmek için Waltz (1998: 50) bilgi hiyerarşisini Veri-Enformasyon-Bilgi-Akıl olarak dört basamaktan oluşturmuştur (Şekil-1). Dolayısıyla üretilen bilginin hazır hale gelme aşamasına kadar ve bilgi ekonomisi sürecinde verilerin güvenliğinde

süreklilik oluşmaktadır. Çünkü üretilen bilginin siyasi, askeri, kültürel, toplumsal, ekolojik ve ekonomik değerlemesi açısından yüksek olması bilginin güvenliğini ön plana çıkarmaktadır.

Şekil-1: Bilgi Hiyerarşisi

İçinde bulunduğumuz zaman dilimine "bilgi toplumu/çağı" olarak ismini veren bilgi olgusu, aynı zamanda çeşitli boyutlarıyla ele alınabilecek bir durumdur. 19. yüzyılın son çeyreğinden itibaren yarı iletkenlerin bilgisayara dayalı teknolojilerle entegre edilmesi, günümüzde uzay teknolojisinin de kullanıldığı sayısı her geçen gün artan yeni iletişim teknolojilerinin geliştirilmesine zemin hazırlamıştır (Atabek, 2001: 59). Hayatımızın her alanında yerini alan çeşidi ve miktarı gün geçtikçe yaşamın hemen her alanında pratik çözümler sunan bilgi teknolojileri, sağladıkları pek çok faydayla birlikte güvenlik sorunsalını da birlikte taşımıştır. Kullanım alanlarına göre güvenlik açısından devletler, politikalarını etkileyecek zeminler oluşturması kimi zaman bir saldırı aracı, kimi zaman da söz konusu saldırılara maruz kalan bir hedefin nasıl savunulacağının niteliğini ortaya koymaktadır.

Bilginin milli gücün önemli bir unsuru olduğu kabul edilmeli mi? Bilgi ve bilgi çağı teknolojilerinin giderek artan önemi, ulus devletlerarasındaki davranış süreçlerinde kültürel devrim ve değişiklikleri yaratıyor mu? Bu soruların cevabı, komuta-kontrol ve çağdaş bilgi savaşlarını ve bu yönlerini incelemek adına operasyonel sorumlulukları olan ve üst düzey analist, akademisyen ve teknik uzmanların yanı sıra, askeri operatörleri, planlamacıları, araştırmacılar ve analistleri (Wheatley ve Hayes, 1996: 26) bir araya getirmiştir. Özellikle ABD Silahlı Kuvvetlerinin Misyon Yeteneklerini geliştirmek ve desteklemek için Milli Stratejik Araştırmalar Enstitüsü(INSS) İleri Kavramlar Teknolojiler Müdürlüğü ve Bilgi Stratejileri (ACTIS) tarafından düzenlenen çalıştay ve yuvarlak masa toplantılarının sonucu bilgi gücünün önemli bir unsur olduğu herkes tarafından kabul edilmiştir. Bilgi ve bilgi çağı teknolojilerinin giderek artan önemini göstermesi ve bilginin ulus devletler arasındaki davranış süreçlerinde kültürel devrim ve değişiklikleri ortaya çıkarmasını katılımcıların %80'i kabul etmiştir (Wheatley ve Hayes, 1996: 16).

Bilgi milli gücün ayrı bir unsuru olarak görülebilir mi? sorusuna (Tablo-1) katılımcıların %80'i evet cevabını verirken %20'si ise iktidar gücünden bağımsız bilginin her yerde bulunabilen yaygın bir unsur olduğunu varsaymıştır (Wheatley ve Hayes, 1996: 17).

Bilgi ulusal gücün ayrı bir unsuru olarak görülebilir mi?	
EVET	**HAYIR**
❖ Bilgi güçtür. ❖ Bilgi, ulusal gücün tüm diğer unsurlarını destekler ve kendi önemi ile ortaya çıkar. ❖ Bilgi, uluslararası rekabet ve çatışmanın anahtarıdır. ❖ Milli güç unsurları olarak belirli bilgi kategorilerini belirlemek gerekir.	❖ Bilgi her yerdedir ve yaygındır. ❖ Bilgi sadece devlet kurumlarında ortaya çıkar. ❖ Bilgi sadece veri korelasyonu göstermektedir; önemli veya önemsiz olabilir. ❖ Bilgi saldırıları ve suçları mevcut yasalar kapsamındadır.

Tablo 1: Çalıştay Fikirleri Özet Tablosu

b. Bilgi Güvenliğinin Temel Prensipleri

Güvenliğinin sağlanması beklenen bilgi; fiziksel bir ortama kaydedilmiş, düzenlenebilen, saklanabilen herhangi bir iletişim aracıyla başkalarına iletilebilen anlamlı veriler topluluğudur. (Dura ve Atik, 2002: 114). Bilgi güvenliği, bilginin yetkisiz kişilerce kullanımının önlenmesi, doğruluk ve bütünlüğünün korunması ve yetkisi olan bireyler tarafından erişilmesini sağlamak şeklinde tanımlanmaktadır (Canbek ve Sağıroğlu, 2006: 169; Marks, 2007: 50).

Şekil-2: Bilgi Güvenliğinde Gizlilik, Bütünlük ve Kullanılabilirlik

Bilgi güvenliği birçok zaman bilişim güvenliği gibi algılansa da bilişim güvenliği bilgi güvenliğinin kısmi bir parçasını ifade etmektedir. Bilgi güvenliği sadece bilginin başkasının eline geçmesi yani gizliliğinden ibaret değildir. Bilgi güvenliğinin tanımı konusunda genel bir fikir birliği bulunmamakla birlikte, klasik tanımı oldukça kısa ve basit olup, McCumber Bilgi Güvenliği Modeli'ne göre (McCumber, 1991) bilginin karakteri, "gizlilik", "bütünlük"

ve "kullanılabilirlik" (confidentiality, integrity, availability) olarak isimlendirilen üç temel unsurdan oluşur (Şekil 2).

İlk özelliği ya da ilkelerden olan gizlilik; bilginin yetkisiz kişiler tarafından erişilmez hale getirilmesini sağlamak için yapılan uygulamalardır (Önel ve Dinçkan, 2007:6). Diğer bir özelliği ise bütünlük ilkesidir. Bu özelliği ile göndericiden alıcıya iletilen bilginin değiştirilmeden ya da bozulmadan alıcıya ulaşımını sağlamaya yönelik uygulamaları kapsar. Üçüncü ilkesi olan erişilebilirlik ya da süreklilik ilkesi ise sistemin kullanıcıları tarafından zarar verilmeden kullanılmasını ve sürekliliğinin korunmasını sağlayan uygulamaları ifade eder.

2. Savaşın Değişen Niteliği ve Bilgi Savaşları

William S. Lind, Keith Nightengale, John Schmitt ve Joseph Sutton'un 1989 yılında ABD Deniz Piyadeleri Gazetesinde yazdıkları "Savaşın Değişen Yüzü: Dördüncü Nesil Savaşa Doğru" başlıklı makalede savaşın gelişimi nesillere ayrılarak incelenmiştir. Bu yaklaşıma göre Birinci Nesil Savaşlar (1648-1830) Avrupa'da ulus devletlerin oluştuğu 1648 Westphalia Barış Antlaşmasından Napolyon Savaşlarının da dahil olduğu dönemi kapsayan "klasik ulus devlet savaşlarıdır". İkinci Nesil Savaşlar (1830-1918) ise Topyekün Endüstri Savaşları olmuştur. Bu dönemde endüstri devriminin nimetleri savaş alanlarına uygulanarak savaş stratejileri teknoloji tarafından belirlenmiştir. Üçüncü Nesil Savaşlar (1918-1948) ise ikinci nesil savaşlar olan 'mevzi savaşları' anlayışının önemini yitirmesi sonrasındaki dönemi kapsamış ve 'manevra savaşları' olarak adlandırılmıştır. İki Çinli askeri stratejist olan Albay Qiao Liang ve Wang Xiangshui (1999: 22) savaş olgusunun gelişimi üzerinde çalışmış ve 1991 Körfez Savaşını Üçüncü nesil savaşın zirvesi olarak nitelendirmiştir. Lind ve Arkadaşları (1989: 22-26) Dördüncü Nesil Savaşları 'Savaş ile barış dönemleri arasındaki ayrımın bulanıklaştığı, mücadelenin belirlenmiş muharebe sahaları dışına taştığı, sivil ve askerler arasındaki farkların ortadan kalktığı ve asimetrik özellikleri de içeren askeri, yarı askeri ve bazen de sivil gayretler bütünü' olarak tanımlamışlardır. Dördüncü Nesil Savaş ortamında cephe kavramı artık mekânsal bir olgu olmaktan çıkarak siber uzay da en önemli savaş cephelerinden biri haline gelmiştir.

Savaş olgusunun geçirdiği değişimi; Lind ve arkadaşları 'nesillere', Çinli stratejistler 'evrelere' ayırırken, Alvin Toffler (1993: 14) tarım toplumu, sanayi toplumu ve bilgi toplumu olmak üzere 'dalgalara', Martin Van Creveld (1999: 32) aletler çağı, makineler çağı, sistemler çağı ve otomasyon çağı olmak üzere 'çağlara' ayırarak açıklamaya çalışmışlardır. Gerek Toffler'ın bilgi toplumu, gerekse Creveld'in otomasyon çağı, bilgi ve iletişim sistemlerinin kullanımındaki yoğunluğu ve bu sistemlere olan bağımlılığı ortaya koymaktadır.

Günümüzde bilgi sistemleri ve iletişimin hayal edilemeyecek noktalara ulaşması bilgi-güvenlik ilişkisini de farklılaştırmış güvenliğin sadece ordular ile teşkil edilmesini olanaksız kılmıştır. Bilginin getirdiği değişim ile

Buzan'ın bütünsel açıdan değerlendirilmesi gereken geniş kapsamlı güvenlik olgusunu gündeme taşımıştır. Barry Buzan, siyasi, ekonomik, sosyal, çevresel ve askeri boyutları analizine dâhil etmiş ve güvenliği daha geniş bir uluslararası çerçevede tanımlamıştır (Buzan, 1983: 214-242).

Bilgi savaşı denilen enformasyon savaşı bir realite olmakla birlikte ve aynı zamanda hızlı gelişim süreci içerisinde olmasına rağmen yerleşmiş bir doktrinin olmaması belirli inanç/kavramlar çerçevesini net olarak çizememiştir. Öncelikli olarak "bilgi savaşı" birçok şeyi ifade etmek için kullanılır, ancak çoğu zaman askeri etki alanı veya bilgisayarlar tarafından hâkim siber savaş etkilerine odaklanmıştır. Bu dar tanım rekabet ve çatışma ile ilgili geniş politika alanlarındaki sorunlara cevap bulmakta yetersiz kalmaktadır. Bilgi savaşı gerçekte geniş ve çeşitli alanlarda yer aldığı için analizi de açıkça her uygulamada tanımlanmış olmalıdır. Seçilen elemanların net olarak belirlenmiş ve odaklanılmış olması önemlidir. Genel olarak, anlamsız genellemeler ile geniş bir yelpaze de ele alınmıştır (Wheatley ve Hayes, 1996: 5).

Bazı askeri altyapı sistemleri hariç, ulusal, kamusal ve özel bilgi sistemlerinin tamamının birbirinden izole edilmesi günümüzde imkânsız hale gelmiştir. Kamu ve özel sektörün bilgi sistemleri geniş alanlarda birbirine bağlıdır ve bu bağlantı büyümeye devam edecektir. Ulaşım sistemleri, hava kontrol sistemleri, enerji kontrol sistemleri, sağlık sistemleri, medya sistemleri ve bankacılık sistemleri vb. bilgi sistemlerini bir bütünsel olarak potansiyel bir hedefe dönüştürmüştür (Wheatley ve Hayes, 1996: 5).

Bilgi Savaşı, toplumlar ve sistemler ve zihinler üzerinde kontrol sağlama ile gerçekleştirilen bir mücadelenin farklı bir yöntemidir. Etkileri açısından sadece askeri değil, bütüncül nitelik taşır. Bilgi Savaşı alanlarını tanımlamak için üç görece bağımsız boyutuyla ele alınmalıdır. İlki çatışma / işbirliği derecesi, ikincisi somut odak (siyasi, askeri, sosyal, ekonomik ve benzeri) ve son olarak aktörlerin (bireyler, özel kuruluşlar, ulus devletler, uluslararası örgütler, genel halk, medya, vb.) doğasıdır (Wheatley ve Hayes, 1996: 5).

Bilgi alanı içerisindeki üç farklı düzlem; bilgi alanı, etkileşim alanları ve etkileşim seviyesi içerisindeki üç boyutu bir araya getirildiğinde ortaya çıkan temel varsayım bilgi hâkimiyetidir. Bilgi savaşları çok kısa anlamda, "ulusal ve bu amaçla çatışmaların gerçekleşmesi için bilginin kullanılması" olarak ifade edilmektedir (Wheatley ve Hayes, 1996: 5).

Bilgi savaşı içerisinde her çeşit bilgi ve bilgi kaynağı üzerinden türetilecek yeni bilgilerle karar alma mekanizmalarına etki edecek bir biçimde müdahale etmeye saldırı amaçlı bilgi savaşı, müdahaleyi durdurmaya yönelik hareketlere ise savunma amaçlı bilgi savaşı denilmektedir (Denning, 1999: 12).

Bilgi savaşında öncelikli husus, ülkenin kendi bilgi alt yapısının güvenliğini sağlamak ve rakiplerinin bilgi sistemlerini, bilgi kaynaklarını ve bilgi alt yapısını imha etmek için eylemlerde bulunmaktır (Sağsan, 2002: 213-232). Önceleri bilgi savaşı sadece orduların komuta-kontrol-iletişim ve is-

tihbarat sistemleri ile ülkenin bütün iletişim sistemini elektronik anlamda hedef alan savaş biçimini ifade ederken sonraki dönemlerde ise sivilleri de kapsayan her çeşit bilgi üzerinde kurulmaya çalışılan hâkimiyet enformasyon savaşının kapsamına girmiştir. Bilgi savaşlarında en güçlü silâh, bilgi/enformasyon ve dezenformasyondur (Özdağ, 2012).

Bu bağlamda stratejik bilgi savaşları da gündeme taşınmıştır. Bilgi savaşının tanımlayıcı özelliklerinden yola çıkarak şöyle bir sonuç çıkartılabilir. Geleneksel savaşların planlaması içerisinde yer alan stratejik savaşlar, bilgi teknolojilerinin de yer aldığı biçim olarak stratejik bilgi savaşlarını ön plana çıkarmıştır. Bu stratejiler ile bilgi savaşları daha da az maliyetle, tahrifat gücü daha fazla olan bir savaş modeline dönüşmüş hatta bilgi savaşlarını dahi gelenekselleştirmiştir. Bu nedenle, teknolojik yeterliliği yüksek ülkeler bilgi savaşı aşamasını tamamladıktan sonra bir üst seviye olan stratejik bilgi savaşlarını uygulamaya koymuşlardır (Sağsan, 2002: 213-221).

3. Siber Güvenlik ve Siber Savaş

Kullanılma amacı iletişim olan internette temel felsefe bilginin ulaşılabilirliğini ve paylaşımını kolaylaştırmaktır. Başlangıçta kullanıcı sayısının azlığı nedeniyle güvenlik kaygısı olmamasına rağmen günümüzde sistemi kullananların sayısının hızla artmış olması ve bilgisayarların ve akıllı cep telefonların her eve her cebe girebilecek kadar yaygınlaşması tehlike boyutlarını hem artırmış hem de farklılaştırmıştır. İlk zamanlarda yaşanan tehditler internetin devamlılığı için fiziksel altyapıya karşı oluşurken şimdilerde zararlı kodlar ve virüslerin üretilmesi ve yaygınlaşmasıyla birlikte bu tehditler ikinci plana itilmiştir (Öğün ve Kaya, 2013: 150).

Zamanla ekonomik sistemlerin, ticaretin ve bilgi sistemlerinin internetle bütünleşik hale gelmeleri ve siber alanda yaşanan gelişmelerin sistemlere yetkisiz girişe, bilgi hırsızlığına ve hatta fiziksel zararlar vermeye kadar imkân tanıması siber alanda güvenliği büyük bir problem sahasına dönüştürmüştür. Aynı zamanda internetin ulusal ve uluslararası yapısına fiziksel olarak sınırlama konamaması bireyler ve toplumlar üzerindeki etkileri de düşünüldüğünde uluslararası ilişkiler alanında yerini almaması düşünülemez (Öğün ve Kaya, 2013: 150).

Siber teknolojiler hızlı bir biçimde toplumları ve bireyleri dönüştürmeye devam etmektedir. Siber tehditlerin boyutları devletlerarası krizlere yol açacak kadar büyümesi ve devletlerin siber alanı bir hâkimiyet unsuru olarak görmeye başlamaları gibi durumlar günümüzde bilgi güvenliği ve siber güvenlik alanlarını birbirinden farklılaştırarak daha bağımsız bir hale dönüştürmüştür. Bilgi güvenliği daha çok kurumların ilgilendiği, statik, sınırları belli bir disiplin iken siber güvenlik daha dinamik bir kavram olmuştur. Çünkü ağ üzerinden yapılabilecek bilgi hırsızlığı gibi bir kavramdan siber saldırı gibi tüm entegre sistemlere fiziksel zarar verebilecek bir noktaya gelinmiştir. Dolayısıyla daha kapsamlı bir kurumsal boyutun yanı sıra siber savaş, siber istihbarat, siber suç gibi toplumsal, ulusal ve uluslararası boyutlara ulaşmıştır.

Genel anlamda hedef seçilen ülke ve ülkelere yönelik ticari, politik veya askerî amaçlı şahıs, şirket, kurum, örgüt, gibi yapıların bilgi sistemlerine veya iletişim altyapılarına yapılan planlı ve koordineli saldırılara siber savaş denilebilir. Ancak siber güvenlik sadece bir saldırı ve bunun sonucunda verilecek bir zarar veya elde edilecek haksız bir kazanç anlamına gelmez. Aynı zamanda siber teröristlerin sanal ortamı iletişim ve propaganda aracı olarak kullanılması da siber güvenlik konusu içerisine girmektedir (Öğün ve Kaya, 2013: 152). Dünyada ilk defa enformasyon savaşları deyimini kullanan John Arquilla (1999: 384), günümüz teknolojisiyle kitlesel ölçekte yıkıcı eylemlerin gerçekleştirilebileceğinin bilindiğini, ancak Stuxnet gibi virüslerle birlikte sadece enformatik değil fiziki tahribatın da verilebileceğinin anlaşıldığını söylemektedir. Siber saldırılarla bir ülkenin trafik ışıklarından güç şebekelerine, kara, deniz, hava yollarına kadar her şeyi felç etmek, aynı zamanda bu tahribatları dünyanın herhangi bir yerinden internete bağlı bir bilgisayar ile gerçekleştirmek mümkün hale gelmiş ve istihbarat birimlerinin işlerini de fazlasıyla kolaylaştırmıştır.

Örneğin Beyaz Saray Siber Güvenlik Uzmanı Richard Clarke casusluğun çok kolaylaştığını söylüyor. Eskiden Washington'daki Rus Elçiliği'nde çalışan bir KGB ajanının bir FBI ajanı ayartması çok zordu. Ama şimdi Moskova'da oturuyorsun. Ve hiçbir risk olmadan binlerce sayfa çalabiliyorsun. Eskinin casuslarına artık gerek yok. Hem istihbarat örgütlerindeki insan kaynağı, hem de altyapı farklılaştı: "Eskiden Sinop'ta büyük bir kulemiz vardı. Rusya'daki konuşmaları dinliyorduk. Ama şimdi buna ihtiyaç yok. Amerikalı askerin Sinop'a gitmesine gerek kalmadan her işini masasından halledebiliyor." Kimse radyo frekansı kullanmıyor. Ulusal Güvenlik Ajansı'nın (NSA) Maryland'deki kampüsünden bütün dünyadaki internet trafiğini izlenebiliyor (Tanış, hürriyet, [web], 2012).

ABD, İran'a kendi kendini kopyalayan bir yazılım olan Stuxnet ile saldırı düzenledi. Stuxnet, Haziran 2010'da fark edilen ve İran'ın Natanz nükleer tesisine saldırmak için geliştirilmiş olan bir siber silahın adıdır. Stuxnet, siber savaşın ve siber silahların, bir dönem tartışılan uzay savaşları gibi sadece sanal veriler üzerinde kalmayacağını ispatladı. Siber saldırılar, hedef sistemdeki sistem açıklarını bularak içeri sızar. Stuxnet'de ise, "zero-day" yani sıfırıncı gün açıkları olarak isimlendirilen, sistem açıkları piyasalarda yüz binlerce dolarlık bütçelerle yapılabilmektedir. Anlaşıldığı üzere Stuxnet'in tasarlanması milyon dolarlık bütçelerle oluşturulmuştur. Bu durum Stuxnet'in basit amatör birey veya gruplarca olmadığını ve arkasında bir devlet bütçesi ve mühendislik ile üretilmiş olduğunu bize göstermektedir. Yazılım öncelikle motorları ve sıcaklığı kontrol eden merkezi kontrol birimlerini ele geçirdi. Böylece sistemin kontrol eden diğer yazılımları da birer birer kolaylıkla elimine edilebildi. Özellikle nükleer yakıt zenginleştirme tesislerini hedef alan bu saldırı santrifüjlerin dönüş hızlarını etkileyerek kullanım ömürlerini azaltmak suretiyle zenginleştirme sürecine zarar vermeyi hedefledi ve santrifüjlerin çılgınca dönmesine yol açtı ve ciddi fiziki zararlar verdi. İran başlangıçta ne olduğunu tam olarak kavrayamasa da

sonraları durumun vahametini anladı ve en yetkili ağızdan bizzat Ahmedinejad tarafından İran'ın bir siber saldırıya uğradığı doğrulandı (Alkan, 2012).

Türkiye'de de farklı zamanlarda bilişim güvenliği açısından tehdit oluşturmuş olaylar yaşanmıştır. Örneğin milli olmayan Batman Hidroelektrik Santrali yazılımının kilitlenmesi elektrik üretim faaliyetlerini durdurmuştur. Atatürk Havalimanında aksamalara sebep olan virüsün dış hatlar terminalinde gidiş ve geliş katlarında yolcuların "check-in", "boarding" ve "bagajlama" işlemlerinin etkilenmesi ile faaliyetler manüel olarak yapılmak zorunda kalınmış, yolcular için birçok aksama meydana gelmiştir (Habertürk, [web], 2009). Diğer bir yaşanan olay ise 2011 yılında Gümrük Müsteşarlığı'ndaki Merkezi Bilgi İşlem Sistemi'nin veri tabanında oluşan arıza bir milyar dolarlık dış ticareti durdurmuştur (Hürriyet, [web], 2011). Gümrük sistemlerinin çökmesi gibi meydana gelen aksamalar ilk akla gelen örnekler arasındadır (Öğün ve Kaya, 2013: 162).

Yaşanıldığında acı tecrübelerle siber tehditlere karşı devlet, kurum ve bireylerin tedbirlerini artırma zorunluluğu doğmaktadır. Özellikle bu konuda devletler bazında yasal düzenlemeler, tedbirler ve siber olaylara müdahale birimleri kurulmaya başlanmıştır. Bu faaliyetler; Siber Güvenlik Eylem Planları, Ulusal Bilgi Güvenliği Programı, Ulusal Bilgi Güvenliği Kapısı, Yasal Çalışmalar, Siber Güvenlik Müdahale Ekipleri ve Birimleri, Siber Güvenlik Tatbikatları, Konferanslar ve Çalıştaylar ve de 2012 yılı içerisinde TSK bünyesinde MEBS ve Siber Savunma Komutanlığı olarak teşkilatlanmaya gidilmiştir (Öğün ve Kaya, 2013: 165). Ayrıca TCK'ya "Bilişim Alanında İşlenen Suçlar" başlığı altında eklenen 243. ve 244. maddeler ile aşağıda yer alan kanun, yönetmelik, genelge ve tebliğler çıkarılmıştır.

1. Ulusal Siber Güvenlik Stratejisi Eylem Planı
2. Kurumsal SOME (Siber Olaylara Müdahale Ekibi) Kurulum ve Yönetim rehberi
3. SOME (Siber Olaylara Müdahale Ekibi) tebliğ
4. 23.01.2004_5070 Sayılı Elektronik İmza Kanunu
5. 24.07.2006_Kamu Sertifikasyonu Merkezi İle İlgili Genelge
6. 23.05.2007_5651 Sayılı İnternet Ortamında Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun
7. 01.11.2007 İnternet Toplu Kullanım Sağlayıcıları Hakkında Yönetmelik
8. 30.11.2007_İnternet Ortamında Yapılan Yayınların Düzenlenmesine Dair Usul ve Esaslar Hakkında Yönetmelik
9. Lisanslı Yazılım Kullanılması İle İlgili Genelge
10. 20.07.2008_Elektronik Haberleşme Güvenliği Yönetmeliği
11. 10.11.2008_5809 Elektronik Haberleşme Kanunu
12. 07.01.2010_İnternet Alan Adları Yönetmeliği
13. 26.10.2007_Kamu Kurumları İnternet Sitesi Kılavuzu

14. 24.07.2012_Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmelik

a. Siber Savaşlarda Estonya Örneği

Siber saldırı konusunda en çarpıcı örnek olarak Avrupa'nın en gelişmiş bilgi sistemlerine sahip olan, internet erişiminin temel insan hakkı olduğunu ilan eden ve bilgi sistemlerinin yoğun kullanımından dolayı kendisini 'E-stonia' olarak tanımlayan Estonya verilebilir.

Saldırılar 27 Nisan 2007 tarihinde başlamış ve Estonya'nın başta finans merkezlerini, bankalarını, parlamentosunu, bakanlıklarını, güvenlik ve ulaşım alt yapısını hedef almıştır. Bu saldırı ile insanlık tarihinde ilk kez bir devlet üç hafta süreyle sistematik ve çoklu bir siber saldırıya maruz kalmış ve 1.4 milyonluk bu ülkede devlet otoritesi oldukça sarsılmıştır (Traynor, 2007).

"Avrupa'nın en kablolu devleti" olmakla ün yapmış Estonya, internet kullanımının en yüksek düzeyde olduğu ülkelerden birisidir. Örneğin Skype'ın hazırlanmasında kullanılan yazılım, Estonya menşeiliydi. Estonya, dünya üzerinde internet kullanarak yapılmış olan ilk yerel seçimlere de 2005 yılında ev sahipliği yapmıştır (Katri, 2003: 4-7). 2010 yılı verilerine göre, Estonya'nın 1.46 milyonluk nüfusun yüzde 75'i internet kullanıcısıdır. Her vatandaşın devlet kurumlarına ve bankalarına internet üzerinden bağlanmasına imkân veren bir dijital kimliğe sahip olduğu ülkede, 355 devlet kuruluşu sanal dünyada yer almaktadır. Ernsdorff ve Berbec (2007: 171) araştırmalarında Estonya'nın e-devlet yapılanmasında Orta ve Doğu Avrupa'da lider ve dünyada üçüncü sırada yer aldıklarını belirtir.

İkinci Dünya Savaşı esnasında Estonya, Sovyetler Birliği ile birlikte, Almanya'ya karşı cephe açmıştı. Savaştan sonra Estonya'nın başkenti Tallinn'e Kızıl Ordu'nun girişinin ifadesi olarak 1947 yılında yapılmış olan Estonya'nın Nazilere karşı savunulmasını ve Sovyetler Birliği'nin verdiği mücadeleyi sembolize eden "Tallinn'in Kurtarıcısı Heykeli" ya da popüler adıyla "Bronz Asker" heykeli dikilmişti. 2007 yılında heykelin yıkılmasını isteyenler ile yer değiştirmesi gerektiğini savunanlar arasında yürüyen tartışma sonucunda heykel, 26 Nisan 2007'de hükümetin kararıyla Tallinn'deki askeri mezarlığa taşındı. Heykelin kaldırılmasını istemeyen ve ülke nüfusunun yaklaşık %25' ini oluşturan Rus kökenli vatandaşlar, ülkenin çeşitli yerlerinde özellikle başkent Tallinn'de gösteri yapmaya başladı. Protesto gösterileri devam ederken 27 Nisan gece yarısından sonra ülkenin siber altyapısını hedef alan saldırılar başladı ve giderek hız kazandı. 27-29 Nisan 2007 tarihleri arasında devletin internet sayfaları siber saldırılara maruz kalmış; ulusal e-posta sunucularına ve haber portallarına siber saldırılar düzenlenmişti. Dördüncü günden itibaren, özellikle 30 Nisan-18 Mayıs tarihleri arasında daha fazla organize saldırılar yapılmış ve ulusal bilgi sistemlerine, internet sağlayıcılarına ve bankalara büyük zararlar veren siber saldırılar gerçekleştirilmiştir (bilgiguvenligi.gov.tr.[web], 2015).

Estonya'da devlet otoritesinin sarsılmasının yanı sıra belki de en önemli sonuç, Batılı ülkeler nezdinde yaşanmıştır. Estonya'ya karşı yapılan siber saldırılar, NATO'nun siber güvenliğe bakışının şekillenmesinde önemli rol oynamıştır. Saldırıların ilk başladığı andan itibaren Estonyalı yetkililer NATO uzmanlarından büyük destek almıştı. Tallinn'e gelen NATO uzmanları, ülkenin saldırılara karşı geliştirdiği savunma mekanizmalarında önemli rol oynadılar. Siber savunma kapasitesini bir merkezde toplayarak harekât kabiliyetini daha artırmak isteyen NATO, bununla yetinmeyerek 2008 Ağustos ayında Estonya Tallinn merkezli bir NATO Siber Savunma İşbirliği Mükemmeliyet Merkezi (Cooperative Cyber Defence Centre of Excellence–NATO CCD COE) kurmuştur.

b. Siber Savaşlarda Gürcistan Örneği

Enformasyon savaşlarına önemli örneklerden bir diğeri de 2008 yılında Rusya ile Gürcistan arasındaki savaşta gerçekleşmiş, siber uzay, savaşın önemli bir cephesi haline gelmiştir. Gürcü köylerine yapılan füze saldırısına karşılık veren Gürcistan, Güney Osetya'nın başkentini bombalamış ve 7 Ağustos 2008'de bölgeyi işgal etmiştir. 8 Ağustos 2008'de Rus ordusu işgalci güçleri Güney Osetya'dan çıkartmış, bununla da kalmayıp siber savaşçılarını devreye sokmuştur. Gürcistan'ın dış dünya ile bağlantılarını kesmek için Gürcü medyasına ve devletin web sitelerine saldırmıştır. Saldırı silahı olarak DDoS'u kullanmıştır. Gürcistan'ın CNN ve BBC web sayfalarına girişini engellemiştir. Rusya siber savaşçıları Gürcistan'a trafiği destekleyen tüm yönlendiricileri ele geçirmiştir. Dışarıdan haber almayan Gürcistan, dışarıya da e-posta bile gönderememiştir.

Gürcüler 8 Ağustos'da Güney Osetya'yı bombalarken Güney Osetya'daki tüm veri sistemleri ve internet siteleri siber saldırı ile kapatılmıştır. Ruslar ise askeri harekâtın başladığı tarihten itibaren Gürcistan internet sitelerine yönelik saldırıları artırmıştır. İnternet sitelerine erişim engellenmiş ve birçoğunun site içerikleri değiştirilmişti. Bu saldırılar fiziksel olarak bir zarar oluşturmamış ancak çatışmaların önemli bir evresinde Gürcistan hükümetini zayıf düşürmeye yönelik adımlar olmuştur. Bunlardan en çarpıcı olanı Gürcistan Devlet Başkanlığı resmi sitesine Mikhail Saakasvhili'nin resminin yerine Adolf Hitler'in resminin konulmasıdır. Böylelikle dünya kamuoyu psikolojik olarak etki altına alınarak, Gürcistan'a yönelik saldırıların haklı olduğuna yönelik imaj çizilmeye çalışılmıştır (bilgiguvenligi.gov.tr.[web], 2015).

Gürcistan'ın internet hatlarının yarısının Rusya üzerinden dünyaya açılmakta oluşu, Gürcistan'ın internet bağlantısını engellemeyi ve ülkeyi dünyadan izole etmeyi kolaylaştıran önemli bir faktör olmuştur (Mirzaoğlu, 2011: 20).

Sonuç

Güvenlik uluslararası ilişkilerin birincil konularından birini oluşturur. Güvenliğin sübjektifliği, toplum ve bireylerin yaşam biçimlerindeki değişim ile birlikte farklılaşmaya devam edecektir. Günümüzde de güvenlik algılamala-

rı, bilgi ve teknolojiye dayanan gelişmeler, iktisadi ve toplumsal koşulların hızlı değişimi ile birlikte küreselleşme süreci içerisinde yeniden tanımlanması gerektiği tartışmalarını doğurmuştur. Güvenlik insan hayatını doğrudan etkileyen olguları barındırdığından geleneksel yaklaşımlar günümüz güvenlik kavramsalını anlamlandırmada yetersiz kalmaktadır.

21. yüzyıl içerisinde güvenlik kavramı ve ulusal güvenlik anlayışları özellikle II. Dünya Savaşı sonrasında çok önemli bir değişim süreci yaşamıştır. Ulus-devlet yapısı içerisinde devletler, tehdit ve düşman tanımlamalarını daha açık ve belirgin bir şekilde ortaya koymuş kendi imkânlarınca mücadele şartlarını oluşturmuşlardı. Özellikle 1990 ve sonrasında yapılar daha girift ve tek başına mücadele edebilecek boyutları fazlasıyla aşmıştır. Bunun getirdiği farklılıklardan yola çıkılarak ulusal savunma stratejileri de değişikliğe uğramaya devam etmiştir.

Küreselleşmenin getirdiği sonuçlar itibari ile toplumsal düzlemde bir değerler dizisi değişikliği yaşanmaktadır. Günümüzde, özellikle üretim koşullarının yaşadığı yapısal değişim toplumun her alanında yansımasını bularak yeni bir toplum düzeni ortaya çıkarmıştır. Toplumların "Teknoloji" ve "bilgi" zemininde biçimlenmesine "Bilgi Toplumu" denilmektedir. Bilgi toplumu; her türlü bilgiyi üreten, bilgi ağları oluşturan, hazır bilgilere nüfuz eden ve bu bilgileri her alanda değerlendirebilen özelliklere sahip toplumsal düzey seviyesi olarak da tanımlanabilir (İlhan, 1993: 62-67).

Bilgi temel üretici güç olarak kabul edilir. Modern kapitalizm yerini maddesiz denilen "bilgi sermaye", "zeka sermaye" olarak değişime uğramakta bilgi ve teknolojiye dayanan gelişmeler, toplumsal koşulların hızlı değişimine neden olmakta güvenliğin yeniden tanımlanması gerektiği tartışmalarını da gündeme çıkarmaktadır. Çünkü bilgi değeri sürekli yükselen bir madendir. Enformasyon ve iletişim teknolojilerindeki büyük değişim, yeni bir devrimle, "enformasyon devrimiyle" tanımlanmıştır. Üretilen bilginin siyasi, askeri, kültürel, toplumsal, ekolojik ve ekonomik değerlemesi açısından yüksek olması bilginin güvenliğini ön plana çıkarmaktadır. Çünkü sanal olarak üretilen bilginin hazır hale gelme sürecinde verilerin güvenliliği sürekli olmalıdır. Geçmişte devletleri dış tehditlerden korumak için askerler kullanılırken günümüzde sanal güvenlik birimleri de yerini almıştır.

Teknolojik ve bilgi zeminli küreselleşme, ulusal ve uluslararası düzeyde tehditlerin değişimini ve yeni aktörlerin ortaya çıkışına neden olmuştur. Bu nedenle çağın yeni aktörleri arasında devlet dışı örgütler, şirketler, uluslararasılaşmış yapılara bürünmüş terörist gruplar ve organize suç örgütleri de yerini almıştır. Teknolojiyi devletlerin kullandığı kadar bu yapı ve örgütlerin de kullanması bilgi güvenliği alanındaki paradigmanın zemini içerisindedir.

Devletlerin ve diğer aktörlerin kendi çıkarları doğrultusunda yeni stratejiler belirlemesi ve güç oluşturma çabası da doğaldır. Bu stratejilerin uygulama alanlarındaki stratejilerin çakışması ile yeni rekabet sahaları oluşacaktır. Uluslararası ilişkilerdeki gittikçe karmaşıklaşan bu karmaşık yapı

aktörlerin farklı stratejik davranışlar belirlemesine ve kendileri için hedeflenen yeni çıkarlara yöneltecektir.

Askeri kapalı devre altyapı sistemleri hariç, ulusal, kamusal ve özel bilgi sistemlerinin tümünün birbirinden izole edilmesi günümüzde imkânsız hale gelmiştir. Özellikle kamu ve özel sektörün de bilgi sistemlerinin çok geniş alanlarda birbirine bağlı olması tehlikenin boyutlarını çok daha dramatik boyutlara ulaştırmıştır. Bilgi sistemlerinin bütünsel olarak potansiyel bir hedefe dönüşmesi nedeniyle bu alanlarda oluşacak zafiyetler devletin tüm kurumları gibi Türk Silahlı Kuvvetleri'ni de doğrudan etkileyecektir.

Bilgi güvenliğinin devlet düzeyinde koordinesi sağlanması, alınacak tedbirler ve hızlı karar verme mekanizmalarının oluşturulması çok önemlidir. Çünkü bilgi tüm hızıyla üretilmekte ve akışkanlığı da bir o kadar süratle devam etmektedir. Bilişim teknolojileri ile oluşturulmuş alt yapı, ulaşım, enerji gibi hayati öneme haiz sistemler tüm toplum yaşamını doğrudan etkileyebilmektedir. Özellikle devletlerin belirlediği stratejiler için oluşacak zaman kayıpları ülkeleri dezavantajlı konuma düşürebilmektedir. Dolayısıyla bilişim teknolojilerindeki güvelik unsurları devletler için ön plana çıkmaya devam etmektedir.

Bilgi iletişim teknolojilerinin siyasal ve toplumsal hayatın her aşamasında yerini alması ve bu teknolojilerin kendilerini hızlı bir şekilde sürekli yenilemesi, etkin ve güvenilir nitelikli kullanıcı personele olan ihtiyacı doğrusal oranda artırmaktadır. Güvenlik açıklarının öncelikli olarak insan faktörü ile başladığı düşünülürse bu alana yapılacak yatırımların getirileri çok daha fazla olacaktır.

KAYNAKLAR

ALKAN Mustafa (2012). "Siber Güvenlik ve Siber savaşlar", *Bilgi Güvenliği Derneği Koferans:* Mayıs 2012
https://www.tbmm.gov.tr/arastirma_komisyonlari/bilisim_internet/docs/sunumlar/BILGI%20GUVENLIGI%20DERNEGI/09_05%20-%20Bilgi%20Guvenligi%20Dernegi.pptx
ARQUILLA John (1999). "Ethics and Informatıon Warfare", in *Strategic Appraisal: The Changing Role of Information in Warfare* (Zalmay Khalilzad, John P. White, and Andrew Marshall eds.), Santa Monica, CA: RAND
ATABEK Ümit (2001). *İletişim ve Teknoloji: Yeni Olanaklar Yeni Sorunlar,* Ankara: Seçkin Yayıncılık.
BUZAN Barry (1983). *People, States and Fear: The National Security Problem in International Relations,* Brighton, Harvester Books, Chapel Hill, University of North Carolina Press, , s. 214–242.
CANBEK Gürol ve SAĞIROĞLU Şeref (2006). "Bilgi, Bilgi Güvenliği ve Süreçleri Üzerine Bir İnceleme", *Gazi Üniversitesi Politeknik Dergisi*, 9 (3): 165-174

ÇAPAR Bengü (2003). "Bilgi yönetimi: Nasıl bir insan gücü?" T. Büyükakın ve F. Büyükakın (yay. hazl.) *II. Ulusal Bilgi, Ekonomi ve Yönetim Kongresi bildiriler kitabı* içinde (ss. 421-432). İstanbul: Beta.

DENNING, E. Dorothy (1999). *Information Warfare and Security*, New York

DURA Cihan ve ATİK Hayriye. (2002). *Bilgi toplumu, bilgi ekonomisi ve Türkiye*, İstanbul, Literatür Yayınları.

ERNSDORFF Mark ve BERBEC Adriana (2007). "Estonia: The Short Road to E-government and E-democracy", P. Nixon ve V. Koutrakou (Der.), *E-government in Europe*. Abingdon, Routledge. s.171.

HABERTÜRK Ajans İnternet Sitesi, Atatürk Havalimanı'nda Virüs Kabusu, <http://www.haberturk.com/yasam/haber/125013-ataturk-havalimanindavirus-kabusu>, 14.04.2017.

'Information', (1987). Harrod's librarians glossary of terms used in librarianship, documentation and bookcrafts, Aldershoot, Gower, 14.

'Information', (1980). The ALA glossary of library and information science, Chicago, Amerikan Library Assocation, , s. 48.

KATRI Kerem (2003). *Internet Banking in Estonia*, Tallinn, Praxis Center for Policy Studies, s.4–7.

KESİCİ İlhan (1993). "Bilgi Toplumunun Özellikleri", *Bilişim*, Mayıs, 62–67.

McCumber, John (1991). "Information systems security: A comprehensive model". *Proceedings 14th National Computer Security Conference*. Baltimore: National Institude of Standarts and Technology.

ÖĞÜN, M.Nesip ve Kaya Adem (2013). "Siber Güvenliğin Milli Güvenlik Açısından Önemi ve Alınabilecek Tedbirler", *Stratejik Araştırmalar Enstitüsü Güvenlik Stratejileri Dergisi*, 9(18):145-181

ÖNEL, Dinçer ve DİNÇKAN Ali (2007). *Bilgi Güvenliği Yönetim Sistemi Kurulumu.* TÜBİTAK UEKAE (Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü), http://docplayer.biz.tr/3155080-Bilgi-guvenligi-yonetim-sistemi-kurulumu.html:Erişim:14.04.2017

ÖZDAĞ, Ümit (2012). "Stratejik İletişim ve Algı Yönetimi" *Enformasyon Savaşı*, B.Senem Çevik-Ersaydı, Rifat Serav İlhan (Ed.), Ankara, Ankara Üniversitesi Politik Psikoloji Ar. ve Uyg. Merkezi Yayını

RUSELL, Bertrand (1970). "Knowledge, Error and Probable Opinion", C. Landesmen (ed). *The Foundation of Knowledge*, New Jersey: Prentice Hall, 20-26

SAĞSAN, Mustafa (2002). "Bilgi Savaşı: Siperlerden Klavyelere Taşınan Harekâtın Anatomisi" *Avrasya Dosyası, İstihbarat Özel*, 8(2):213-232.

STEIN, George J. (1995). "Information Warfare", *Airpower Journel, Spring* 1995<http://www.au.af.mil/au/afri/aspj/airchronicles/apj/apj95/spr95_files/stein.htm: Erişim:14.04.2017

TANIŞ, Tolga (2012). "Türkiye siber savaşa hazır mı?" 29 Nisan 2012< http://www.hurriyet.com.tr/turkiye-siber-savasa-hazir-mi-20442751: Erişim:14.04.2017

WALTZ, Edward (1998). *Information warfare: Principles and operations.* London: Artech House,

WHEATLEY, Gary ve HAYES Richard (1996). *Information Warfare and Deterrence*, NDU Press Book December