Kara Harp Okulu Bilim Dergisi
Science Journal of Turkish Military Academy
Haziran / June 2018, Cilt/Volume 28, Sayı/Issue 1, 73-108.
ISSN (Basılı) : 1302-2741 ISSN (Online): 2148-4945

BİLGİ VE İLETİŞİM TEKNOLOJİLERİNE DAYALI OLUŞUMLAR İLE BU OLUŞUMLARIN ULUSLARARASI İLİŞKİLERE GÜVENLİK BAĞLAMINDAKİ ETKİSİ: SİBER TERÖRİZM

2016-2019 Ulusal Siber Güvenlik Strateji Belgesi Kapsamında Türkiye İncelemesi

Mahir TERZİ*

Öz

Sembollerin işlenen nesne olduğu 21. Yüzyıl; Bilgi Toplumu, Bilgi Tabanlı Ekonomi, e-Devlet, FTP tarzı örgütlenme, para yerine geçenler ve uluslararası sivil toplum örgütleri olarak kategorize edilebilecek farklı bir toplum yapısı ve toplumsal örgütlenme modeli ile ortaya çıkmaktadır. Bilgi ve İletişim Teknolojilerinin gelişimine bağlı olarak ortaya çıkan bu unsurlar, beraberinde yeni bir tehdit olan siber tehditleri getirmektedir. Söz konusu tehditler, öncelikle bilgi ve iletişim teknolojilerine dayalı toplum ve ekonomik yapısı olan gelişmiş ve gelişmekte olan ülkeler için tehdit oluşturmaktadır. Bu çalışmada, siber tehditlerin başında gelen siber terörizm incelenmiştir ve siber terörizmle mücadele için konsensüse varılmış bir tanıma ve uluslararası iş birliğine ihtiyaç olduğunu söylemek mümkündür. Uluslararası iş birliği, terörizmle mücadelede olduğu kadar etik kodların nasıl geliştirilebileceğine ilişkin kaygıları da taşımalıdır. Türkiye örneğinde, Ulusal Siber Güvenlik Strateji Belgesi (2016-2019) dikkate alındığında, genel itibariyle söz konusu belgenin iyi oluşturulduğu ifade edilebilir. Ancak uluslararası iş birliğine yapılan vurgu ve referans zayıftır. Bununla birlikte uluslararası iş birliğine ilişkin esasların ne olabileceği ve etik kodların nasıl geliştirebileceğine ilişkin etütler açısından da söz konusu belgenin geliştirilmeye ihtiyacı vardır. Belgede tamamlanmaya ihtiyaç duyan diğer bir husus ise siber saldırı sonrası ortaya çıkan özellikle maddi zararın telafisine ilişkin mekanizmalara yer verilmemesidir.

Anahtar Kelimeler: *Bilgi Tabanlı Ekonomi, Bilgi Toplumu, BİT, E-*

* Dr., Kültür ve Turizm Bakanlığı, mahirterzi@yahoo.com, ORCID: 0000-0003-1308-2060

Devlet, Etik Kodlar, FTP, Siber Terörizm, Siber Uzay, Türkiye, Uluslararası İşbirliği.

The Formations Based on Information and Communication Technologies and the Effects of These Formations on the International Relations in the Context of Security: Cyber Terrorism

The Case of Turkey in the Scope of 2016-2019 National Strategy Document for Cyber Security

Abstract

21st century that the symbols are processed comes on the scene with a different society structure and social model of organisation which are categorised as information society, knowledge-based economy, e-government, FTP style organization, money substitutes and international non-governmental organisations (NGOs). These elements, which arise due to the development of Information and Communication Technologies, bring along with new threats like cyber threats. These threats pose a threat especially to the developed and developing countries, which are primarily socially and economically based on information and communication technologies. This study examines cyber terrorism as one of the chief cyber threat, and it explores that a consensus-based recognition on the definition of cyber terrorism and international cooperation for combating terrorism are needed at international level. International cooperation should also be concerned with how to develop ethical codes as well as combating terrorism. Taking into account the National Cyber Security Strategy Document (2016-2019) in the case of Turkey, it can generally be said that the document is well established. However, the emphasis and reference to international cooperation are weak. Moreover, the document needs to be advanced in terms of what can be the basis and content of this international cooperation and how ethical codes can be developed. Another thing that needs to be considered in the document is the fact that there is no mechanism to compensate for the financial damage in particular caused by the cyber attack.

Keywords: *Information Based Economy, Information Society, ICTs, E-Government, Ethical Codes, FTP, Cyber Terrorism, Cyber Space, Turkey, International Cooperation.*

GİRİŞ

Ülkeler, toplumlar ve kişiler arasındaki fiziksel sınırların bilgi ve iletişim teknolojileri aracılığıyla siber ortamda anlamını kaybetmesi, olası siber tehditlere karşı ortak bir geleceğin küresel düzeyde kendini hissettirmesi, göz ardı edilemeyecek bir gerçektir. Bu anlamda siber tehditler ve bunun özel bir biçimi olan siber terörizm ile mücadele; uluslararası iş birliğini, ulusal düzeyde ise kapasite geliştirme kaygısı ve farkındalığını gerektirmektedir.

Bu çalışma, Bilgi ve İletişim Teknolojilerine dayalı ekonomik, kurumsal, araçsal ve örgütsel oluşumların, siber ortam aracılığıyla, uluslararası ilişkilere güvenlik bağlamındaki etkisine dikkat çekmektedir.

Söz konusu oluşumlar, bilgi ve iletişim teknolojileri bağlamında; Bilgi Tabanlı Ekonomi, Bilgi Toplumu, e-Devlet, FTP tarzı örgütlenme, Para Yerine Geçenler ve Uluslararası Sivil Toplum Kuruluşları olarak kategorize edilmiştir.

Çalışma, bilgi ve iletişim teknolojileri ile siber tehditlerin özel bir formu olan siber terörizmin, illa da ölüm gibi bir sonucu doğurmaksızın, gündelik hayatın gidişatı üzerine yapabileceği tesirin potansiyeli ve önemi ile bu çerçevede yapılması gerekenler hakkında bilgi vermeyi amaçlamaktadır.

Bu bağlamda öncelikle 21. yüzyılda bilgi ve iletişime dayalı oluşumlar tanımlayıcı-istatiksel metot ile mevcut çalışmada ortaya konmuş, ardından bilgi ve iletişime dayanan söz konusu oluşumların uluslararası ilişkilere etkisi, güvenlik bağlamında incelenmiştir. Son olarak Türkiye örneğinde 2016-2019 Ulusal Siber Güvenlik Strateji Belgesi incelenmiş olup, farkındalık açısından Türkiye'nin mevcut tehditlere hazır olup olmadığı değerlendirilmiş, eksikliklere ilişkin tespitler yapılmıştır.

21. Yüzyılda Bilgi ve İletişime Dayalı Oluşumlar

Bu başlık altında bilgi tabanlı ekonomi, bilgi toplumu, e-Devlet, FTP örgütlenme modeli ve hibrit mekânlar ile para yerine geçenler ve

uluslararası sivil toplum örgütleri hakkında bilgilere değinilecektir. Bunlardan uluslararası sivil toplum örgütleri hariç diğer bütün kavramlar teknolojiye ilişkin olup, uluslararası sivil toplum örgütlerinin bunlarla ilişkisi; teknolojinin birlikte getirdiği şeffaflık, yüksek farkındalık yaratma ve hızlı harekete geçme imkânı sağlaması yönünden, yeni dayanışma ve hak arama araçları geliştirmesiyle ilgilidir. Ancak aradaki ilişki karşılıklıdır; çünkü bilgi ve iletişim teknolojilerinin gelişmesinde sivil toplum örgütleri de rol oynamaktadır (www.un.org).

Bilgi Tabanlı Ekonomi

Küreselleşmeye hız veren teknolojinin gelişimiyle ilgili olarak üç endüstriyel devrim vardır. Birinci endüstriyel devrim, buhar makinesinin sanayiye uygulanması aracılığıyla 18. yüzyılda İngiltere'de gerçekleşti. Bu devrim iletişim hızı gibi yeni icatlara neden oldu. İkinci endüstriyel devrim, içten yanmalı motorların ve elektrik enerjisinin sanayide kullanılmasıyla, 19. yüzyılda gerçekleşti. Bu devrim, üretim ve taşıma maliyetlerinin düşmesine ve kitle üretimine geçilmesine dayanak oldu. Üçüncü sanayi devrimine gelince; bu devrim, mekanik ve elektromekanik sistemlerin elektronik sistemlere dönüşümü olarak tanımlanmaktadır. Bu son devrimin temel unsuru bilgi ve bu bilginin yayılmasıdır (Kılıç, 2002: 74–75).

Bununla birlikte teknoloji küreselleşmeye yön verirken küreselleşmenin de teknolojiye yön verdiğini söylemek yanlış olmayacaktır. Birleşmiş Milletler Avrupa Ekonomik Komisyonu'nun Bölgesel Raporu'nda, küresel gelişme dönemiyle ilgili olarak dönüm noktasının 1990'larda gerçekleştiği ifade edilmektedir (www.unece.org).

> "20. yüzyılın son 10 yılı küresel gelişme sürecinde bir dönüm noktasını temsil etmektedir. Günümüz dünyasında sosyal, ekonomik ve kültürel gelişimin motoru bilgidir. Bilgi tabanlı ekonomik faaliyetler, önde giden ülkelerde stratejik önemi olan üretim faktörüdür. Ayrıca bilgi tabanlı faaliyetler, 21. yüzyılda daha ileri ekonomik ve kültürel büyüme için her bir ülkenin gelişme ve hazırlıklılık düzeyinin temel göstergesidir." (www.unece.org).

Bugün Küreselleşmeye yön verme süreci, Bilgi Tabanlı Ekonomi ile ortaya çıkmaktadır. Teknik açıdan ifade etmek gerekirse; Net Ekonomi, Ağırlıksız (Weightless) Ekonomi ve Görsel Ekonomi (Daugeline, 2004) olarak da adlandırılan Bilgi Tabanlı Ekonomi, bilgi ve iletişim teknolojilerine dayanan ekonomiyi kastetmektedir.

Çarpıcı olan diğer bir tanıma göre ise Bilgi Tabanlı Ekonomi, yeni düşünceler, fikirler, süreçler ve ürünler yaratma ve icat etme ve bunları

ekonomik değer ile refaha dönüştürme kapasitesi ve yeteneğidir (Toft, 2002). Bununla birlikte bilginin değişen önemiyle ilgili tanımlar da ileri sürülebilir. Smith (2002), bilginin değişen önemini hesaba katarak dört kategori içinde Bilgi Tabanlı Ekonomiye yönelik yaklaşımları açıklamaktadır.

Birinci kategoride bilgi bir şekilde ürün olarak şimdiye kadar olduğundan daha önemli hale gelmiştir. Diğer bir ifadeyle, insanoğlu artık bilgi ürünlerinin ticaretine dayanan yeni tür faaliyetlere tanıklık edecek. İkinci kategori, bilginin girdi olarak bir şekilde niteliksel ve nicelikse olarak öncekinden daha önemli hale geldiğini vurgulamaktadır. Yani bilgi eğer girdi olarak önemliyse bu bilginin Bilgi Tabanlı Ekonomi için önemli olacağını ifade eder. Üçüncü kategori, kodlanmış bilginin bir şekilde ekonomik olarak uygun bilgi temellerinde daha önemli bir bileşen olacağını ifade eder. Bilgi ve İletişim Teknolojileri ürünleri kodlanmış bilgi ürünleri üzerine inşa edilir. Keza böyle bir mülk, Bilgi ve İletişim Teknolojilerinin teknolojisiyle uyumludur. Son kategori ise doğrudan Bilgi ve İletişim Teknolojilerindeki teknolojik gelişmeleri işaret eder.

> "Şimdi bile Bilgi ve İletişim Teknolojisi devrimini Bilgi Tabanlı Ekonomi'nin gelişi ile sinonim olarak değerlendirmiyorsak da her iki fenomen güçlü bir şekilde ilişkilidir. Bilgi ve İletişim Teknolojisi Sistemi, Bilgi Tabanlı Ekonomi'ye bilginin üretim ve dağıtımı için olduğu kadar üretim sistemine kendini eşleştirmek için koşulları radikal bir şekilde değiştiren yeni ve farklı bir teknolojik taban sunar." (Smith, 2002: 7–8).

Yukarıda ifade edilen dört kategoride bütün tanımlar bilginin farklı bir yönünü vurgulayarak nihayetinde örtüşmektedir. Diğer bir ifadeyle, bütün tanımlar bilginin kendisiyle sonuçlanan yeni bir değer olarak ortaya çıktığını belirtmektedir.

Kapital, emek, ham madde ve girişimcilik dört üretim faktörü iken (Dinler, 1995: 15) günümüzde teknoloji, beşinci üretim faktörü olarak diğer üretim faktörlerine eklenmiştir (Alkin, vd., 2003: 463).

Fakat teknolojiyi üretim kaynaklarının beşincisi olarak değerlendirmek Bilgi Tabanlı Ekonomiyi tanımlamak için yeterli olmayabilir. Bilginin kendisi kendinde değer olarak görülmektedir. Örneğin Drucker (2004), kendi kitabı Kapitalist Toplum Sonrası'nda, günümüz toplumlarında değer üretmek için bilginin önemini vurgulamaktadır.

Bilgi Tabanlı Ekonomi, günümüz ekonomilerinin temel yapısı olarak görülmektedir. Hızlı ilerleme kaydeden bilgi, en önemli üretim faktörü

olarak telaffuz edilmektedir (Avrupa Toplulukları Komisyonu, 2002). Bilgi kendini üreten bir değer olarak kabul görmektedir (Drucker, 2004).

Günümüzde bilgi sadece her şey değil aynı zamanda ticaretin de bir aracı olmaktadır. Böylece bilgi yoğun ürünler, üretilen mal ve hizmetler yahut ihraç edilen ürünler başlığı altında ülkelerin gayri safi milli hasılası içinde önemli bir kalem olarak ortaya çıkmaktadır.

Birleşmiş Milletler Avrupa Ekonomi Komisyonu Bölgesel Raporu'nda, Bilgi Tabanlı Ekonominin özellikleri aşağıdaki gibi sıralanmıştır.

- Bilgi Tabanlı Ekonomi çok kuvvetli teknoloji güdümlü bir güçtür. Her üç dört yılda bir Bilgi ve İletişim Teknolojilerinin yeni bir jenerasyonu ortaya çıkmaktadır. Bugün Bilgi ve İletişim Teknolojisi Şirketleri en geniş kurumlar arasındadır. Bilgi ve İletişim Teknolojisi, en hızlı büyüyen ekonomi sektörleri arasındadır.
- Bilgi ve İletişim Teknolojilerinin hızlı büyümesi tarafından harekete geçirilen telekomünikasyon ve ağ yapıları insan faaliyetlerinin her siperini etkilemiştir ki bunu da insanları tamamen yeni tarzlarda çalışmaya zorlayarak ve yeni alanlar yaratarak yapmıştır.
- Kültürel ve ruhsal değerler tarafından desteklenen bilgi, bağımsız bir güç olmuştur ve sosyal, ekonomik, teknolojik ve kültürel dönüşümün sonucunu belirleyen en önemli faktördür.
- Bilgi Tabanlı Ekonomi, öncü ülkelerin gelişimini hızlandırarak büyük entelektüel ekonomik kaynakların hızlı bütünleşmesine Avrupa entelektüel havuzuna geçişte imkân vermiştir.
- Ortaya çıkan bilgi tabanlı ekonomi, ülkelerde karşılıklı olarak kurumsal ve yenilik sistemleri ile insan kaynakları gelişimini de içeren toplumsal faaliyetin bütün alanlarını etkilemiştir. Bilgi tabanlı ekonomi, her ülkede ilerlemenin motoru olmuştur. Eğer bir ülke gelişmişse bunun anlamı gelişmiş bir bilgi tabanlı ekonomiye sahip olduğudur. Eğer bir ülke geride kalmışsa bunun anlamı da bilgi tabanlı ekonominin o ülke ekonomisinde küçük bir parça oluşturduğudur (www.unece.org).

Bilgi ve İletişim teknolojilerinin ne olduğuna gelince yine Birleşmiş Milletler Avrupa Ekonomi Komisyonu bunları aşağıdaki gibi sıralamaktadır.

- Her tür bilgisayar, telekomünikasyon ve ilgili malzeme üretimi,

- Her tür bilgisayar, telekomünikasyon ve ilgili araştırma ve geliştirme,
- Her tür bilgisayar, telekomünikasyon ve ilgili teknik destek ve bakım ile her tür yazılım üretimi,
- Ses, veri, video vb. unsurları içeren her tür telekomünikasyon ve tele data hizmetleri,
- Her tür telekomünikasyon ve tele data ağ bakımı, kontrolü ve raporlaması,
- Kitap yayını, magazin ve gazete ile web sayfaları ve web portalları gibi hizmetleri de içeren her tür çevirim içi ve çevirim dışı elektronik ortam hizmetleri,
- Her tür çevirim içi ve çevirim dışı reklamcılık (www.unece.org).

Anlaşılacağı üzere böyle bir ekonomi, Bilgi Toplumu olarak adlandırılan uygun bir çevreyi gerektirmektedir. Bu çevre, kişiyi, Bilgi ve İletişim Teknolojilerine sahip olmaya zorlayacak bir çevredir. Diğer bir ifadeyle, teknolojinin gelişimi, yeni bir çevrenin ortaya çıkmasına neden olmaktadır. İşte bu çevre, Bilgi ve İletişim Teknolojilerine dayanan Bilgi Toplumu olarak ortaya çıkmaktadır.

Bilgi Toplumu

Bilgi Toplumu fenomeni ilk önce 1950'lerde ABD ve Uzak Doğu'da Japonya'da ortaya çıktı. Bununla birlikte, ABD'de Bilgi Toplumu, Sanayi Sonrası Toplum olarak adlandırılırken, Japonya'da Bilgi Toplumu olarak tanımlanmıştır (Dura ve Atik, 2002: 38–39).

Bilgi Toplumu, farklı disiplinlerde çeşitli şekillerde telaffuz edilmesine rağmen kavramın içeriği kendisini aynı kontekst içerisinde ortaya çıkarmaktadır. Yani tanımlar, Bilgi Toplumu'nu işaret etmektedir. Örneğin Bell, toplumları sanayi öncesi toplum, sanayi toplumu ve sanayi sonrası toplum olarak sınıflandırmaktadır. Bell'in temel argümanı, sanayi toplumlarının temel faaliyeti uygun organizasyon modeli içindeki fiziksel ürünlerken, sanayi sonrası toplumun temel etkinliği yine uygun organizasyon modeli içindeki bilgi üretimidir (Bell'den aktaran Dura ve Atik, 2002: 38–39). Bell ayrıca sanayi sonrası toplumun özelliklerini 1) mesleki ve teknik bilim adamlığına dayalı uzmanlıklar, 2) bilgiye dayalı

teknoloji, 3) teorik bilgiye sahip olmaya dayanan sınıf statüsü ve 4) bu bilgiyi kontrol etmeye dayalı olan politik otorite olarak sıralamaktadır.

Bilgi Toplumuyla ilgili diğer bir yaklaşım ise aşağıda gösterilmiştir. Tablo 1 toplumları dört gruba ayırmaktadır.

Tablo I: Farklı Toplumlar ve Genel Özellikleri (Taşçı, 2003:15).

	Avcı-toplayıcı	**Tarım**	**Sanayi**	**Bilgi**
Enerji kaynağı	İnsangücü	İnsan ve hayvan gücü	Kömür, petrol gibi fosil yakıtlar	Elektrik ve nükleer enerji
Zenginliğin kaynağı	Kişisel yetenek	Toprak	Enerji kaynakları ve sanayi	Bilgi ve kişisel yetenek
Sembol	İnsan	Çiftlik	Fabrika	Bilgisayar
Çoğunluğun yaptığı iş	Avcılık, toplayıcılık	Tarım	Fabrika İşçiliği	Sembol işleme
İşlenen nesne	Tabiat	Toprak	Malzeme	Sembol
Zaman Düzenlemesi	Tabiatın yıllık ritmi	Tabiatın yıllık ritmi	Doğrudan saat zamanı	Kişisel biyolojik ritm
Toplumsal örgütlenme	Kabile	İmparatorluk	Ulus-devlet	Uluslararası geçirgenlik

Tabloya göre Bilgi Toplumu'nda elektrik ve nükleer enerji, Sanayi Toplumu'ndaki fosil yakıtların yerini almaktadır. Sanayi Toplumu'nda temel sembol fabrika iken Bilgi Toplumu'nda ana sembol bilgisayardır. Dahası da Sanayi Toplumu'na işlenen temel nesne malzeme iken Bilgi Toplumu'nda işlenen ana nesne semboldür. Diğer bir çarpıcı özellik ise Bilgi Toplumu'nda ulus devlet, uluslararası geçirgenlikle yer değiştirmektedir.[2]

Bilgi birikimi sağlamak, temelde teknolojik yeniliklerle gerçekleştiğinden, sanayi toplumlarının dönüşümü, Bilgi ve İletişim Teknolojileri olmaksızın mümkün gözükmemektedir. Bu nedenle bilginin belirli biçimlerine erişilebilirliği geliştirmede Bilgi ve İletişim Teknolojileri önemli bir potansiyeldir (Spangenberg, vd., 2003: 83-95). Bu nedenle

Ar&Ge yatırımları ile Bilgi ve İletişim Teknolojileri harcamaları ekonomik değer olarak bilgiyi toplamada, üretmede, dağıtmada ve kontrol etmede önem kazanmaktadır.[3]

21. yüzyılda ortaya çıkan diğer bir gelişme ise devletin örgütlenme yapısıyla ilgilidir ki bu aynı zamanda Bilgi Tabanlı Ekonomi ve Bilgi Toplumunu inşa edebilmek için teknolojik gelişmenin de felsefine uygun bir yapılanmadır. Söz konusu yapılanma ise e-Devlet olarak ortaya çıkmaktadır.

e-Devlet

e-Devlet'i tanımlayabilmek için İnternet, Bilgi ve İletişim Teknolojileri (BİT) gibi bazı kavramlara referans yapmak gereklidir. Çeşitli ülkeler tarafından kendi önceliklerine göre yapılan farklı tanımlardan dolayı, kavramın kendisi evrensel olarak aynı manada kullanılmamaktadır. Yine de, farklı tanımlara dikkat edildiğinde, İnternet ve BİT gibi aynı referans kavramlara başvurulduğu görülecektir.

Dar anlamda e-Devlet, internet hizmet teslimi ve danışmanlık gibi internet tabanlı diğer aktiviteler olarak tanımlanmaktadır. Bu tanımdan başka, geniş anlamda e-Devlet, devlet hizmetlerinde BİT' in kullanımıyla eş değer görülmüştür. Yani, BİT ifadesi, internet kavramının yerini alıyor.

Ancak, yukarıda telaffuz edildiği gibi çeşitli hükümetlerin farklı önceliklerinden dolayı, e-Devlet tanımı BİT aracılığıyla kamu yönetimini dönüştürme kapasitesi olarak yorumlanabilir. Yani, BİT çevresinde inşa edilen yönetimin yeni bir biçimi (http://www.oecd-ilibrary.org).

İnce, e-Devlet'i kâğıt tasarrufundan fayda sağlayan bilgi ve teknik devlet olarak tanımlıyor (İnce, 2001: 22-6). Kâğıt tasarrufuna indirgenmiş bu tanımdan başka Yücetürk, e-Devleti, elektronik ortamda vatandaş, iş dünyası ve devlet arasındaki ilişki ve işlemlerin gerçekleştirilmesi olarak tanımlıyor (Yücetürk, 2004).

Daha geniş anlamda Birleşmiş Milletler Genel Asamblesi e-Devleti demokratik hesap verebilirliği, kontrolü ve kolektif karar almayı güçlendirme olarak tanımlarken OECD bu kavramı daha dar anlamda, iyi bir yönetimi başarmanın aracı olarak BİT'in özellikle de internetin kullanımı olarak tanımlamaktadır (http://www.oecd-ilibrary.org).

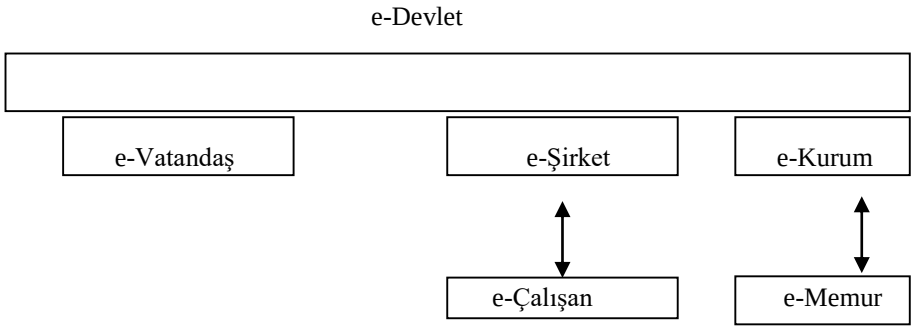
Dahası da bazı organizasyonlar, e-Devletin öncelik ve uygulamalarını özellikle de gelişmekte olan ve az gelişmiş ülkeleri hesaba

katarak standardize etmektedir. Örneğin, Birleşmiş Milletler şemsiyesi altında çalışan Uluslararası Telekomünikasyon Birliği, kendi eylem planında, e-Devlet'in şeffaflık, hesap verebilirlik ve verimliliği artırılabilmesi için yönetimin bütün kademelerin desteklenmesi gerektiğini belirmektedir (http://www.itu.int). Yani, 2003 yılında Cenova'da gerçekleştirilen Bilgi Toplumu Dünya Zirvesi'nde şeffaflık, hesap verebilirlik ve verimlilik kavramları BİT ile ilişkili olarak görülmektedir. Ayrıca, e-Devlet bazı ülkeler için dünyaya entegrasyon olarak algılanmaktadır. Örneğin, Türkiye Cumhuriyeti Başbakanlığı e-Devlet ile ilgili görüşlerini aşağıdaki gibi ifade etmiştir.

> "Küreselleşmenin hızla ilerlediği ve ekonomik anlamda sınırların kalktığı bir dünyada, bilgi ve iletişim teknolojilerindeki hızlı gelişmeler, ülkemiz ile çağdaş ülkeler arasındaki açığı artırmaktadır. Ülkemizin bu açığı kapatarak dünya ile bütünleşmesi ve bilgi toplumu durumuna gelebilmesi için devletin, gelişmiş teknolojiyi ve çağdaş yönetim tekniklerini birlikte kullanılması bireyleri ve vatandaşa hizmeti ön plana çıkaran yeni bir yapılanmaya gitmesi zorunludur. Bu yeniden yapılanma modeli e-Devlet olarak belirtilmektedir. e-Devlet; bilgi, hizmet ve mal alışverişlerinde bilgi teknolojilerini kullanarak, performans ve verimlilik artışını hedefleyen devlet modeli olarak tanımlamaktadır." (Türkiye Bilişim Şurası, 2002: 211-2).

Bütün bu tanımlama ve açıklamalardan, çeşitli kaynaklarca belirlenen farklı önceliklerden dolayı kavramın anlamında bir konsensüs olmadığı açıktır. Bununla birlikte, İnternet ve/veya BİT, e-Devlet örgütlenme modelinde kullanılan aynı temel araçlardır. e-Devlet kavramına hakimiyet kurabilmek için tespit edilmesi gereken hususlardan birisi ise e-Devlet'in bileşenleridir. Bu bileşenler; vatandaşlar, iş dünyası ve kamu kurumları olup sırasıyla e-vatandaş, e-şirket ve e-kurum olarak adlandırılmaktadır.

Her bir bileşen kendi içerisinde "e" yani elektronik ortama dönüşme olgusunu gerçekleştirecek ve e-Devlet zamanla oluşacaktır. e-Devlet'in bileşenleri ve her bir bileşenin kendi alt elementleriyle iletişimi aşağıda gösterilmiştir.



Şekil 1: e-Devlet'in Bileşenleri (Türkiye Bilişim Şurasından Aktaran Demirel, 2006: 85)

Yukarıdaki şekle göre e-Devlet, vatandaşları ve işletme ile kamu kurumları gibi teşekkülleri içeren elementleriyle birlikte bütün toplumu kapsamaktadır. E-Devlet; *devletin vatandaşlara karşı yerine getirmekle yükümlü olduğu görev ve hizmetler ile vatandaşların devlete karşı olan görev ve hizmetlerinin karşılıklı olarak elektronik iletişim ve işlem ortamlarında kesintisiz ve güvenli olarak yürütülmesi* (Türkiye Bilişim Şurası, 2002: 206) olduğundan *yönetimin yeni bir formunu* ifade etmektedir.

Bununla birlikte, yukarıdaki şekil daha makro düzeyde bir gerçeği göz ardı etmektedir ki bu da devletin kendisidir. Çünkü küresel düzlemde bir devlet ile diğer bir devlet yahut bir yönetim ile diğer bir yönetim arasında *e-ilişki* söz konusu olacaktır.

e- Devletle ilgili belirtilebilecek nihai bir husus ise e-Devlet'in ruhuna uygun olarak, iş hayatında ve bireysel yerleşimde meydana gelen değişimdir ki bunlar da FTP ve hibrit mekanlar olarak ortaya çıkmaktadır. Diğer bir ifadeyle, iş yaşamında örgütlenme; FTP olarak günümüz insanının karşısına çıkarken, birey, kendisini şehir merkezinden yahut iş yerine yakınlık kaygılarından uzak tutarak, hibrit mekân içerisinde, kendine bir yer bulabilmektedir.

FTP ve Hibrit Mekân

Bilgi ve İletişim Teknolojilerinin özellikle bilgi ve hizmet sektörlerinde ortaya çıkardığı örgütlenme modeli olan FTP (File Transfer Protokol) kelime anlamıyla, Dosya Transfer Protokolü manasına gelmektedir. FTP, bir bilgisayarda bulunan yazılım, belge ve dosya vb. bilgileri diğer bir bilgisayara aktarmaya yarayan ara yüzdür (Güneş, vd., 2003: 273).

FTP çoğunlukla bir sunucudaki dosyayı interneti kullanarak indirmek amacıyla yahut web sayfası gibi bir dosyayı sunucuya yüklemek için kullanılır. Bununla birlikte FTP'nin görevi sadece veri ve yazılım transferiyle sınırlı değildir. FTP örgütlenme sayesinde, bilgi ve hizmet sektöründe çalışan bir kişi görevini rahatlıkla icra edebilir. Örneğin bir gazeteci yazılarını gazetenin web sayfasında kendisi için tahsis edilen yere iş yerine gitmeden bulunduğu ortamdan internet aracılığıyla gönderebilir. Keza herhangi bir uzaktan eğitim kurumunda görev yapan öğretmen, internet aracılığıyla öğrencilerinden bilgi alabilir, onları bilgilendirebilir ve öğrencilerinin performanslarını değerlendirebilir.

Günümüzde Bilgi ve İletişim Teknolojileri sayesinde hayatın her siperi değişmektedir. İnsanlar fiziksel alandaki iş, alışveriş ve eğlence merkezleri gibi fırsatlara görsel alanda da erişim sağlayabilir (Castells, 1998: 410-428; Muhammad, 2004: 2).

En çok etkilenen siperler ise ulaşım ve iletişim alanlarıdır; çünkü mekan olarak yer ikame edilebilir, değiştirilebilir veya azaltılabilir (Muhammad, 2004: 2). Bir yandan insanlar evlerinden Bilgi ve İletişim Teknolojileri aracılığıyla işlerine erişim sağlayıp, e-alışveriş, e-sağlık, e-öğrenme vb. faaliyetleri gerçekleştirebilirken diğer yandan satın alınan ürün ve hizmetlerin varlığı, ulaşımı daha da önemli hale getirebilir. Örneğin internet aracılığıyla sipariş verilen bir kitaba, kargo aracılığıyla sahip olunabilir.

Muhammad (2004:7), Bilgi ve İletişim Teknolojileri bağlamında işe erişilebilirliği ölçme açısından görsel ve fiziksel mekânın birleşimini işaret etmek için Hibrit Mekân kavramını kullanmaktadır. Bu modelde fırsatlar üç kategoriye bölünmüştür. Birincisi görsel mekânda elektronik ortamda işe gidip gelme (telecommuting), ikincisi hibrit mekanda hem elektronik ortamda işe gidip gelme (telecommuting) hem de fiziksel olarak işe gidip gelme (commuting) ve son olarak da fiziksel mekanda fiziksel olarak işe gidip gelme (commuting) söz konusudur. Kişiler ise iki kategoriye ayrılmıştır. Bu kategorileri ise Bilgi ve İletişim Teknolojisi becerilerine sahip olanlar ile olmayanlar oluşturmaktadır. Eğer kişilerde Bilgi ve İletişim Teknolojisi becerilerine sahiplik söz konusuysa ev temelli ve merkez temelli (tele/call centers) olmak üzere yine ikiye ayrım söz konusudur.

Merkez temelli kavramına bütün vatandaşların Bilgi ve İletişim Teknolojileri aracılığıyla bilgiye kolaylıkla erişim sağlayabilecekleri kamu internet erişim noktaları örnek olarak verilebilir (http://www.etsi.org).

Ev temeli ve merkez temelli fırsatlar kısmi zamanlı, tam zamanlı veya ara sıra olabilir. Görsel mekândaki fırsatlara ise sadece Bilgi ve İletişim Teknolojisi becerilerine sahip olanlar erişebilir. Yani bu modelde Bilgi ve İletişim Teknolojisi becerilerine sahip olanlar çok daha avantajlı konumdadır.

Kısaca bu modelde fırsatlar üç şekilde elde edilebilir.

1. Görsel mekânda telekomikasyon aracılığıyla,
2. Hibrit mekânda ulaşım ve/veya Bilgi ve İletişim Teknolojileri aracılığıyla,
3. Fiziksel mekânda geleneksel olarak ulaşım aracılığıyla.

Doğal olarak Bilgi Toplumu'nda işlerin dağılımıyla ilgili bir kestirimde bulunma güç değildir. Hollanda Merkezi Planlama Bürosu uluslararası politikayı, teknolojik gelişmeyi, sosyoekonomik ve demografik gelişmeleri dikkate alarak 2020 yılı için üç senaryo formüle etmiştir. Birinci senaryoda yavaş gelişmenin olduğu Bölünmüş Avrupa (Divided Europe), ikinci senaryoda orta düzey gelişmenin olduğu Avrupa Koordinasyonu (EC), son senaryoda ise en hızlı gelişmenin gerçekleştiği Küresel Rekabet (GC) söz konusudur (Muhammad, 2004: 24). Tablo 2, Bilgi ve İletişim Teknolojileri çağı Avrupası'nın iş dağılımını göstermektedir.

Tablo 2: Bilgi ve İletişim Teknolojileri Çağı Avrupası'nın İş Dağılımı (Muhammad, 2004:43).

Yıl	**Görsel Mekân %**	**Hibrit Mekân %**	**Fiziksel Mekân %**
1986	1	2	97
1995	1,75	5,25	93
2000	6	9	85
2020 (DE)	5,19	16,91	77,9
2020 (EC)	10,51	34,29	55,2
2020 (GC)	16,15	44,05	39,85

Sonuç olarak yukarıda anlatılanlar, 21. yüzyılın toplumu olan Bilgi Toplumu'nda FTP'nin organizasyonlarda uygun bir örgütlenme modeli olarak ortaya çıkacağına yönelik göz ardı edilemeyecek veriler sunmaktadır.

Para Yerine Geçenler

Para, bir ekonomide, hem mal ve hizmet satıcıları tarafından; bu mal ve hizmetler karşılığı olarak hem de kredi verenler tarafından borç ödemeleri karşılığı genel olarak kabul edilen herhangi bir değişim aracıdır (Özkazanç, vd., 2004: 426).

İnsanlık tarihinin en ilginç mallarından birisi olan paranın Milattan önce en yoğun kullanılan çeşidi inektir. İngilizcede parasal anlamına gelen *pecuinary* sözcüğü Latincede inek anlamına gelmektedir. Elbise, mısır, köleler, bıçaklar ve hatta biranın çeşitli dönemlerde ve çeşitli yerlerde para olarak kullanıldığına ilişkin belgeler mevcuttur (Alkin, vd., 2003: 358). Günümüzde bile Mikronezya'nın federal eyaletlerinden birisi olan Yap Adası'nda 1500 yıldan beri kaya parçaların para olarak kullanılmaktadır. Taş ne kadar büyük ve düzgün olursa ifade ettiği değer de o kadar yüksek olmaktadır (Alkin, vd., 2003: 359) ancak bunlar istisnai örnektir.

Paranın fonksiyonlarına bakıldığında 1) değişim aracı olma, 2) hesap birimi olma, 3) değer muhafaza aracı olma (Şıklar, 2005: 5-9) ve 4) iktisat politikası aracı olma (Dinler, 1995: 350) özellikleri öne çıkmaktadır.

İçinde bulunulan çağda ise paranın değişim aracı olma özelliğinde ise kredi kartı, akıllı kart ve sanal kartların önemini artırdığı görülmektedir. Plastik kart piyasası dünyanın en hızlı gelişen piyasalarından birisidir. Örneğin 2015 yılı itibariyle Amerikalıların yüzde 70'nde en az 1 kredi kartı bulunmaktadır. 2016 yılının ilk çeyreğine doğru buna 10 milyon kişi daha eklenmiştir. Kredi kartı düzenleyicileri, Haziran 2016'da, tüketicilere, 381 milyon kart teklifi götürmüştür (http://www.creditcards.com).

Diğer bir örnek olarak Türkiye'ye bakıldığında ise 1999'da yaklaşık 10 milyon olan kredi kartı sayısı (https://www.capital.com.tr), 2016 yılında 58,7 milyona ulaşmıştır (http://bkm.com.tr).

Teknolojideki en son gelişme hızla yayılan akıllı kartlardır. Kredi kartına benzeyen ve üzerine yerleştirilmiş olan chip'e istenilen düzeyde satın alma gücünün programlanabildiği bu kartlar hızla yaygınlaşmaktadır.

Akıllı kartların nakitsiz topluma geçişte önemli bir adım olduğu ileri sürülmektedir. (Alkin, vd., 2003: 377).

Diğer bir uygulama ise sanal kart uygulamasıdır. Sanal kartlar kişinin internet üzerinden ödeme yapabilmesine imkân sağlamaktadır. (https://www.garanti.com.tr). Keza sanal kart uygulaması da bilgi ve iletişim teknolojileri üzerine inşa edilmiş bir sistemdir.

Sonuç olarak günümüzde bilgisayarların gelişimi ve modern iletişim teknolojisinin kullanımıyla birlikte, kâğıt para kullanımının azaldığı ve yeni elektronik para biçimlerinin yaygınlaşacağı söylenebilir ki bunlarda nakit para gibi, ödeme aracı niteliğine sahip olduğundan, para yerine geçenler olarak nitelendirilebilir.

Uluslararası Sivil Toplum Kuruluşları

Sivil toplum kuruluşu, resmi kurumlar dışında ve bunlardan bağımsız olarak çalışan, politik, sosyal, kültürel, hukuki ve çevresel amaçları doğrultusunda lobi çalışmaları, ikna ve eylemlerle çalışan, üyelerini ve çalışanlarını gönüllülük usulüyle alan, kâr amacı gütmeyen ve gelirlerini bağışlar ve/veya üyelik ödemeleri ile sağlayan kuruluşlardır (Yücetürk, 2016).

Karagül (2007)'e göre sivil toplum kuruluşları (STK'lar) devletlerin geleneksel sınırlarının önemini yitirdiği, devlet merkezli yaklaşımların rafa kalkmaya başladığı ve devlet dışında gelişen alanın olağanüstü büyüdüğü bu ortamda, ulusal ölçeği aşarak küresel ölçekte rol ve etkinlik kazanmaya başlamıştır (Karagül, 2007).

Ulus ötesi faaliyetler yürütebilme yeteneğine sahip olan uluslararası sivil toplum kuruluşlarının, genel STK özelliklerine[4] ek olarak en az üç devlet bireylerinden ya da kolektif varlıklarından oluşması; en az üç devlette faaliyetinin olması; bütçeye önemli finansal desteğin en az üç devletin bireylerinden ya da kolektif varlıklarından gelmesi gerekmektedir (Arıboğan'dan aktaran, Karagül, 2007).

Uluslararası sivil toplum kuruluşlarının tarihi, 19. yüzyılın ortalarına kadar uzanmaktadır. Köleliğe karşı ve kadın haklarının kazanılması konularında çok önemli roller oynayan sivil toplum kuruluşlarının etkinlikleri, Dünya Silahsızlanma Konferansında en üst düzeye ulaşmıştır. Ancak bugünkü manası ile "Sivil Toplum Kuruluşu" kavramı ilk defa 1945 yılında Birleşmiş Milletler Teşkilatının kuruluşu sırasında, kuruluş

beyannamesinin 10. Bölümünün 71. Maddesinde devlet ve üye ülkelere ait olmayan kuruluşların danışmanlık rolü ile ilgili tanımlamada kullanılmıştır. Sivil Toplum Kuruluşlarının sürdürülebilir kalkınma alanındaki hayati rolleri ilk defa Birleşmiş Milletlerin STK'lar ile BM arasında sıkı danışmanlık ilişkilerinin düzenlendiği 21. ajandasının 27. Başlığında dile getirilmiştir (Kurt, 2012).

Küreselleşme, sivil toplum kuruluşlarının dünya ölçeğinde örgütlenme ve etkinlik kurma yeteneğini artırmış; değişen koşullara daha kolay uyum sağlayabilmelerini kolaylaştırmıştır (Karagül, 2007).

Uluslararası sivil toplum kuruluşlarının ana finans sağlayıcısının üyelerin yanında devletler ve uluslararası düzeyde önemli rol oynayan diğer aktörler olduğu kabul edilmektedir. 1990'ların sonu itibariyle, kaynak olarak yıllık 6-8 milyar arası Dolar STK'ların gelişmesi ve dünyanın değişik bölgelerinde yayılması için ayrılmakta, bu fonlar; BM'den 2 milyar Dolar, AB kaynaklarından 1,5 milyar Dolar, iki taraflı yardım ajanslarından 2-3 milyar Dolar, kamu ve özel fon kaynaklarından ise 1-1,5 milyar Dolar olarak sağlanmaktadır (Reimann'dan aktaran Karagül, 2007).

Uluslararası sivil toplum örgütlerinin etkisini aşağıdaki alıntı özetleyebilecek niteliktedir.

> "ABD, Çin Halk Cumhuriyeti gibi büyük ve güçlü ülkeler, Avrupa Birliği (AB) gibi bölgesel örgütlenmeler ve Dünya Bankası gibi nüfuz sahibi teşkilatlar günümüzde politikalarını NGO'ların muhtemel tepkilerini dikkate alarak belirlemekte, hatta sözkonusu belirleme sürecine belli ölçülerde NGO'ların katılımına imkan tanımaktadırlar...
>
> ...1987 yılında imzaya açılan "Ozon Tabakasına Zarar Veren Maddeler Hakkında Montreal Protokolü", 1997'de sonuçlandırılan "Kara Mayınlarının Önlenmesine Dair Sözleşme" ve 1998'de Roma'da imza aşamasına getirilen "Uluslararası Ceza Mahkemesi"nin kurulmasına dair anlaşmanın ortaya çıkarılması çalışmalarına NGO'ların çok büyük katkıda bulundukları bilinmektedir. Bunlar arasında en çarpıcı olanı ise kara mayınları ile ilgili anlaşmanın hazırlık sürecidir. "Kara Mayınlarının Yasaklanması Uluslararası Komitesi" (ICBL) adlı ve 23 ülkeden 350 NGO'yu biraraya getiren hareket, önce konuyu uluslararası gündeme sokmayı başardığını, bilahare, ABD gibi bir ülkenin muhalefetine rağmen ortaya bir anlaşma taslağı çıkardığını, bununla da kalmayıp diğer NGO'larla birlikte yürüttüğü çalışma sonucunda 14 ay gibi kısa bir sürede 122 ülkenin anılan sözleşmeyi imzalamalarına önayak olmuştur. ICBL Başkanı'nın, kampanyaya katılan NGO'lar adına 1997 yılında Nobel Barış Ödülü'nü alması da bu başarının derecesini göstermektedir…" (Bilman, 2001).

Sonuç olarak tarihsel bir süreç içerisinde gelişerek etkisini hissettiren uluslararası sivil toplum örgütleri, 21. yüzyılda bilgi ve iletişim teknolojileriyle köklerini sağlamlaştırma kapasitesine ve küresel toplumun bireylerinde farkındalık yaratma gücüne sahip önemli bir ekonomik ve politik aktördür.[5]

Bilgi ve İletişime Dayalı Oluşumların Uluslararası İlişkilere Yansıması: Güvenlik ve Siber Terörizm

Kitle imha silahları ve terörizm uluslararası düzenin karşılaştığı güçlüklerdir (Kissinger, 2002: 275). Geçmiş yıllardan günümüze milliyetçi, ideolojik ve dini fanatizmden yeterince miras almış olan yeni yüzyılın riskleri anarşi ve teknoloji tarafından yayılmaktadır (Cooper, 2005: 10). Buna ilaveten 21. yüzyılda bilgi ve iletişime dayalı oluşumlar, diyalektik olarak kendini tehdit edebilecek oluşumları da beraberinde getirmektedir. Cooper'ın ifadesiyle küreselleşmenin en endişe verici yanı, yeni ve gerekçeleri zor anlaşılan modern bilimin yahut teknolojinin beraberinde getirdiği tehditlerdir (Cooper, 2005: 10-13).

21. yüzyılda bilgi ve iletişime dayalı oluşumların kendi doğasına uygun olarak ortaya çıkardığı tehdit, siber terörizmdir. Diğer bir ifadeyle Bilgi Tabanlı Ekonomi, Bilgi Toplumu, e-Devlet, FTP tarzı örgütlenme, Para Yerine Geçenler ve Uluslararası Sivil Toplum Kuruluşları düzeni temsil ederken siber terörizm düzene yönelik tehdidi temsil etmektedir.

En dar tanımıyla bilgisayarları, ağları ve onların içerdiği bilgiyi isteyen terörizm olarak tanımlanan siber terörizm (Coffman, 2006), çeşitli zihinsel formülasyonlarca farklı şekilde ifade edilmektedir.

Siber terörizm; ulus altı gruplar veya resmi olarak tanınmayan klikler (clandestine) tarafından savaşçı olmayan hedeflere karşı sonu şiddete varan bilgi, bilgisayar sistemleri, bilgisayar programları ve datalara karşı önceden tasarlanmış, siyasi amaçlı saldırılardır (Pollitt, 2006). Bu tanımda siber terörizmin referans noktaları belirlenmekle birlikte sonuç fiziksel olarak ızdırap veren bir şeye yani şiddete indirgenmiştir.

Sonucun sadece şiddete indirgenmediği başka bir tanımda ise siber terörizm; siber sistemlere karşı şiddet, bozma veya ihlal etmenin kullanım tehdidi veya niyetli kullanımını kasteder. Böyle bir niyet gerçekleştiğinde ise sonuç kişi veya kişilerin yaralanması veya ölmesi, fiziksel mülkiyete muazzam zarar veya önemli ekonomik ziyandır (Sofaer, vd., 2000).

Nitelikten değil ancak olgunun hayata geçirilmesine dayanılarak yapılan bir tanımda ise Özcan (2005) şöyle söylemektedir.

> "Temel amacı bir kısım siyasal sonuçlara ulaşmak olan insanların, ellerine geçirdikleri yeni teknolojik donanımlar ile terör eylemini gerçekleştirmek için yola koyulmuş olmalarıdır. Dolayısıyla terörizmde felsefi olarak köklü bir değişimden bahsetmek güçtür ancak yöntemler ve araçlarda önemli değişimler olmuştur denebilir. Bu bağlamda Siber terörizm araçları bakımından ileri teknoloji ve bilgiyi kullanarak klasik terörizm tanımlamasının yeni şekliyle devamıdır denebilir." (Özcan, 2005).

İnternet teknolojisinin alt yapısının gelişmesi ve yayılması ile birlikte hız kazanmakta olan siber terörizm, zaman içerisinde belirlediği hedeflere göre kapsamını ve içeriğini geliştirmektedir.

1980'lerde Birleşik Devletler hükümetine veya ekonomisine yapılan herhangi bir bilgisayar temelli büyük saldırıyı tanımlamak için "siber terörizm" kavramı kullanılmaya başlanmışken (Coffman, 2006), ilerleyen zamanlarda kavramın içeriğinin daha da genişlediği göze çarpmaktadır. Örneğin, Alkol, Tütün ve Ateşli Silahlar Bürosuna göre, 1985 ve Haziran 1996 yılları arasında en az 30 bombalama olayı ve teşebbüs edilen dört bombalama olayında federal ajanlar, internetten elde edildiğinden şüphe edilen bomba yapım literatürünü ortaya çıkarmışlardır (http://www.adl.org).

Aşağıda siber terörizmle ilgili örnek olaylara yer verilmiştir.

1996 yılında Peru'nun Lima şehrinde Japon Büyükelçiliğine saldırarak diplomatik, askeri ve siyasi personeli rehin alan *Tubac Amaru* adlı terör örgütünün ABD'de ve Kanada da bulunan sempatizanları örgütün faaliyetini destekleyen birçok site kurmuşlardır. Bu sitelerde, propaganda ve eyleme destek ile birlikte örgütün Japon Büyükelçilik binasına saldırı planlarını da yayınlamışlardır (http://www.adl.org).

Latin Amerika gerilla hareketleri elektronik olarak hareket eden marjinal sofistike gruplar arasındadır. Wall Street Dergisine göre, Meksika Zapatista gerillaları 1994 isyanından beri elektronik ortam aracılığıyla toparlanmaya başlamışlardır. Kolombiya Devrimci Silahlı Güçleri e-posta aracılığıyla basın soruşturmalarını ustaca cevaplandırmaktadır. Peru'nun ana terörist organizasyonu Shining Path'a ait web sitesi Marksist-Leninist propaganda yapmaktadır (http://www.adl.org).

İslam dinini meşruiyet kaynağı olarak kullanan terör grupları, interneti ayrıca Batı karşıtlığı ve anti İsrail propagandaları için kullanmakta ve yaymaktadırlar. Hamas taraftarlarınca oluşturulan bazı internet siteleri

örgütün patentini, siyasi ve askeri bildirilerini taşımaktadır ki bu bildirilerin bir kısmı Yahudilerin öldürülmesini istemektedir. İngiltere'de faaliyet gösteren Hizbut Tahrir örgütü ise İngiltere'de düzenli yapılan toplantıları hakkında web sitesi aracılığıyla, halka ayrıntılar sunmaktadır. İran destekli Şii terörist örgütü Hizbullah ise Güney Lübnan'da web siteleri aracılığıyla kitaplar satmaktadır. Bazı İsrail ve ABD resmi kaynakları, Hamas ve İslami Cihad mensubu teröristlerin patlayıcıların nasıl kullanılacağı hakkında, yoldaşlarını harita, fotoğraf, talimat, kod ve teknik detaylar aracılığıyla eğittiklerine inanmaktadır (http://www.adl.org).

Diğer çarpısı bir örnek ise 2010 yılında İran'a yapılan Stuxnet saldırısıdır. Stuxnet olarak adlandırılan bir kurtçuk ile İran-Buşehr nükleer santralindeki sistemlerini etkilemek için özel amaçlar gözetilerek santralin ilgili sistemlerini farklı frekanslarda ve motor hızlarında çalıştıracak şekilde işlevsiz hale getirmek amacıyla, ABD Savunma Bakanlığı desteğiyle, bir grup gönüllü siber savaş yazılımcısı tarafından Alman-Siemens bilgi birikimi ve İsrail'in lojistiğiyle, USB bellekler-diskler ile yayılacak şekilde bu virüsün siber silah olarak hazırlandığı tahmin edilmektedir (Ceylan, 2010).

Yukarıda verilen örnekler siber terörizmin gelişim süreci içerisindeki mevcut örneklerdir. Bununla birlikte, siber terörizmin gelişim süreci içerisinde ortaya çıkabilecek olası senaryolar da söz konusudur. Bunlar;

- Geleneksel bombalama veya biyolojik, kimyasal yahut radyasyon saldırısını takiben suyu, elektriği kesme veya acil durum iletişim imkânlarını bloke etmek.
- Bilgi altyapısı gerçek mekanizmasını yıkmak.
- İnternet, kamu bilgisayar ağları, finansal ağlar veya kitle iletişim araçları gibi önemli sivil sistemlerin altında yatan bilgi teknolojisini bozmak.

Büyük hasar vermek amacıyla trafik ışıklarını, güç tesislerini veya barajları kontrol eden sistemleri kontrol altına almak için bilgisayar ağlarını kullanmak.

- Siber ortamda dosyaları çalmak, web sayfalarının içeriğini değiştirmek, yanlış bilgi yaymak, uygulamaları sabote etmek, verileri silmek vb.

- Güveni yok etmek veya paniğe neden olmak için finans pazarları veya medya yayınlarını bozmak.
- Uzaktan kumanda sistemler aracılığıyla barajlarda gedik açmak, uçakları çarpıştırmak, güç şebekelerini kapatmak vb. (Coffman, 2006).

Siber terörizm ile ilgili tüm bu anlatılardan sonra sonuç niteliğinde bir tanım vermek gerekirse, Terzi (2015:194) *siber terörizmi; siyasal içerikli olup siber ortamda, insanların da bir parçası olduğu siber sistemlere karşı bozma, sızma veya ihlal etmenin gerçekleşmesi veya gerçekleştirme tehdidi gibi bir hareketin neden olduğu engellenme sonucu, milyonların davranışını etkilemek ve günlük yaşamın gidişatını bozmak*, şeklinde tanımlamaktadır.

Siber terörizmin altyapısı, kendi ontolojisine uygun bir yapıyı gerektirmektedir. Bu kavram karşımıza siber alan olan çıkmaktadır. Siber alanı belirleyen ise network (ağ) altyapısıdır. Ağ altyapısını belirleyen unsurlar ise bilgisayar ağı, ağ işletim sistemi, ağ alan sunucusu, dosya sunucusu, yerel alan ağ, geniş alan ağ, yönlendirici, omurga, fiziksel ağ iletim ortamları, modem, göbek, ağ anahtarı, TCP/IP protokolleri, IP numarası, internet sunucuları ile genel anlamda yazılım ve donanım gibi kavramlardır (Güneş, vd., 2003: 217-63).

Siber terörizm 21.yüzyılın terör biçimi olmaya aday bir oluşumdur ki bu da e-Devletin en büyük tehdit algılaması olarak da ifade edilebilir. Diğer bir deyişle, devletin ontolojik olarak yani var olma nedenini ağ ortamına taşıması ve siber terörizmin gelişim sürecinde olabilecek olası terör senaryoları, siber terörizmin e-Devlet karşısında başat bir güç olmak için faaliyette bulunabileceğine işaret etmektedir.

Siber terörizme dair yukarıda senaryolaştırılmış olası örnekler ayrıca uluslararası düzeyde acilen resmi bir tanıma ihtiyaç olduğunu göstermektedir. Aksi durumda örneğin Libya'daki bir teröristin siber ortamda İngiliz borsasına yönelik bir saldırısı Libya'nın saldırısı olarak mı değerlendirilecek, yoksa yasadışı bir örgüt mensubunun saldırısı olarak mı değerlendirilecek netlik kazanmamaktadır. Bu ise siber terörizm ile mücadeleyi daha sofistike hale getirmekte ve zorlaştırmaktadır.

Evrensel ve resmi bir siber terör tanımının olmayışı aynı zamanda devletler tarafından birbirlerine karşı bilgi ve iletişim teknolojileri aracılığıyla sergileyebileceği askeri nitelikteki operasyonları akla getirmektedir ki bu da siber savaş olarak mütalaa edilebilir. Örneğin, Çin

Halk Cumhuriyeti'nin Tayvan'ın altyapısını, hükümetini ve ekonomisini felce uğratmak amacıyla siber saldırılar yaptığına dair raporlar mevcuttur (Brenner, 2007: 402).

Sonuç olarak teknolojinin beraberinde getirdiği siber terör ve hatta siber savaş gibi tehditlere karşı çözümler daha iyi politikalar üretmekle mümkündür. Daha iyi politikalar ise uluslararası düzeyde gerçekleştirilebilecek yoğun diplomasi ve iş birliğiyle mümkündür. 21. yüzyıl diplomasisi ise Cooper'ın belirlediği aşağıdaki beş düstura sahip olmalıdır.[6]

1. Yabancıların farklı olduğu kabul edilmeli ve onlarla empati kurulmalı.
2. Dış politika iç politikayı yansıtmaktadır ve önemli olan iç politikanın ne olduğunu anlamaktır.
3. Yabancıları ikna etmede güçten ziyade onlarda değerler konusunda bilinç yaratmak olgusu ön plana çıkmalıdır.
4. Dış politika sadece çıkar değildir. Dış politika aynı zamanda yerel kimlik olabileceği gibi ülkelerin kendileriyle ilgili çıkarları ifade ediş şeklide olabilir.
5. Sorunların çözümü için bir tarafta yenilgi duygusunu yaratmadan diğer alanlarda onların da söz sahibi olabileceği düşüncesi tesis edilmelidir (Cooper, 2005: 87-148).

Buraya kadar anlatılan bilgiler, 21. yüzyılda bilgi ve iletişim teknolojilerine dayalı olguların uluslararası ilişkilere güvenlik bağlamındaki etkisini tartışmak içindi. Takip eden paragraflarda ise Türkiye özelinde Ulusal Siber Güvenlik Strateji Belgesi 2016-2019 incelenecek olup, Türkiye'nin bu yeni etkilere hazır olup olmadığı tespit edilmeye çalışılacaktır.

2016-2019 Ulusal Siber Güvenlik Strateji Belgesi ve Türkiye[7]

Türkiye'de ulusal siber güvenlikten sorumlu Bakanlık, Ulaştırma, Denizcilik ve Haberleşme Bakanlığı'dır. 20/10/2012 tarih ve 28447 sayılı Resmi Gazetede yayınlanan "Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Bakanlar Kurulu Kararı" ve 5809 sayılı Elektronik Haberleşme Kanunu gereğince ulusal siber güvenliğin sağlanmasına ilişkin politika, strateji ve eylem planlarını

hazırlamak ve koordinasyonunu sağlamak görevi, Ulaştırma, Denizcilik ve Haberleşme Bakanlığına verilmiştir.

Mezkûr Bakanlar Kurulu Kararı'nın 4. maddesine göre Siber Güvenlik Kurulu oluşturulmuştur. Kurula üye kurumlar; Ulaştırma, Denizcilik ve Haberleşme Bakanlığı, Dışişleri Bakanlığı, İçişleri Bakanlığı, Milli Savunma Bakanlığı, Kamu Güvenliği Müsteşarlığı, Milli İstihbarat Teşkilatı, Genelkurmay Başkanlığı, Bilgi Teknolojileri ve İletişim Kurumu, Türkiye Bilimsel ve Teknolojik Araştırma Kurumu (TÜBİTAK), Mali Suçları Araştırma Kurulu ve Telekomünikasyon İletişim Başkanlığı'dır.

2016-2019 Ulusal Siber Güvenlik Strateji Belgesi ve buna bağlı olarak oluşturulan Eylem Planına bakıldığında söz konusu belgelerin ana amacının "…siber güvenliğin ulusal güvenliğin ayrılmaz bir parçası olduğu anlayışının tüm kesimlerde yerleşmesi, ulusal siber uzayda bulunan sistem ve paydaşların tamamının güvenliğini sağlamak üzere idari ve teknolojik önlemlerin alınmasını sağlayacak yetkinliğin eksiksiz bir şekilde kazanılması…"(http://www.udhb.gov.tr) olarak belirlendiği görülmektedir.

Strateji Belgesinin kapsamında ise kamu ve özel sektör tarafından işletilen bilişim sistemlerine ait kritik altyapılar ile küçük ve orta ölçekli sanayi, tüm özel ve tüzel kişiler de dâhil olmak üzere ulusal siber uzayın ülke ölçeğindeki bütün bileşenlerini kapsamaktadır. Diğer bir ifadeyle, kritik altyapılar başta olmak üzere ulusal siber uzaydaki tüm unsurlar, Strateji Belgesinin kapsamı dâhilindedir.

Strateji Belgesinin tanımlar kısmında ise "kritik altyapılar", işlediği bilginin gizliliği, bütünlüğü veya erişilebilirliği bozulduğunda; can kaybına, büyük ölçekli ekonomik zarara ve ulusal güvenlik açıklarına veya kamu düzeninin bozulmasına yol açabilecek bilişim sistemlerini barındıran altyapılar olarak ifade etmektedir. Bu altyapılar, 20/06/2013 tarih ve 2 sayılı Siber Güvenlik Kurulu kararı mucibince "elektronik haberleşme", "enerji", "su yönetimi", "kritik kamu hizmetleri", "ulaştırma" ve "bankacılık ve finans" sektörleri olarak belirlenmiştir.

Siber güvenlik kapsamında riskler ise aşağıdaki gibi belirlenmiştir.

1. Kritik altyapıların kullandığı bilişim sistemlerine yapılacak hizmet dışı bırakma ve benzeri hedef odaklı saldırılar sonucunda enerji, ulaştırma, vb. kritik hizmetlerin kesintiye uğraması.
2. Kamu ve kritik altyapıların kullandığı bilişim sistemlerine yapılacak hedefe yönelik saldırılar sonucunda; vatandaşa ait kişisel bilgilerin veya kamuya ait gizli bilgilerin saldırganların eline geçmesi, ifşa olması, değiştirilmesi veya yok edilmesi.

3. Araştırma, geliştirme ve üretim yapan kurum ve kuruluşların (özel firmalar, araştırma kurumları ve savunma sanayi) ticari sırlarını ve bilgi birikimini elde etmeye yönelik hedef odaklı saldırılar sonucunda hassas veya ticari değere sahip bilgilerin saldırganların eline geçmesi, ifşa olması, değiştirilmesi veya yok edilmesi.
4. Propaganda amaçlı bilgisayar korsanlığı (hacktivizm) saldırıları sonucu çeşitli kurum ve kuruluşların itibarının zarar görmesi veya hassas bilgi/verinin ifşa olması, değiştirilmesi veya yok edilmesi.
5. E-ticaret yapan kuruluşların, E-posta hizmeti veren kuruluşların, sosyal medya hizmeti veren kuruluşların hizmet dışı bırakma ve benzeri saldırılar sonucunda hizmet verememesi nedeniyle maddi kayba uğraması, sahte işlem kaydı oluşturulması, gizli bilgilerin saldırganların eline geçmesi, ifşa olması, değiştirilmesi veya yok edilmesi.
6. E-ticaret yapan kuruluşların, finans sektörü veya çevrimiçi ödeme ya da para transferine imkan veren diğer kuruluşların müşterilerine ait hassas bilgilerin saldırganlar tarafından ele geçirilmesi nedeni ile itibar kaybına uğraması, toplumda çevrimiçi işlemlere yönelik güven kaybı oluşması, bu hizmetlerden faydalanan müşterilerin maddi kayba uğraması.
7. Küçük ve orta ölçekli sanayi, ticaret ve hizmet sektöründeki kuruluşların faaliyetlerinin bilişim sistemlerindeki güvenlik önlemlerinin eksikliğinden veya kullanıcı hatalarından dolayı kesintiye uğraması, hassas veya ticari değere sahip bilgilerin saldırganların eline geçmesi, ifşa olması, değiştirilmesi veya yok edilmesi.
8. Toplumun internete ve sosyal ağlara olan bağımlılığı, siber güvenlik alanında yeterli düzeyde bilgi ve bilinç seviyesine sahip olmaması, mobil ve sabit bilgi sistemlerinde kişisel güvenlik önlemlerini almaması gibi nedenlerle kötücül yazılım ve oltalama saldırılarına, dolandırıcılık ve kimlik hırsızlığına maruz kalması, kişisel bilgilerin ve cihazların saldırganlar tarafından ele geçirilmesi, değiştirilmesi veya yok edilmesi, sahte işlem yapılması.
9. Her türlü kurum ve kuruluşta yığın posta, kötücül yazılım ve benzeri saldırılar sonucunda dolandırıcılıkla karşı karşıya kalınması.
10. Her türlü kurum ve kuruluşta, kullanıcı hataları ya da doğal afetler sonucunda bilişim sistemleri aracılığı ile verilen hizmet ve faaliyetlerin kesintiye uğraması (http://www.udhb.gov.tr).

Son olarak söz konusu belgenin stratejik eylemlerine bakıldığında 5 temel stratejik eylemin belirlendiği görülmektedir. Bunlar;

- Siber savunmanın güçlendirilmesi ve kritik altyapıların korunması,
- Siber suçlarla müdahale,
- Farkındalık ve insan kaynağı geliştirme,

- Siber güvenlik ekosisteminin geliştirilmesi,
- Siber güvenliğin milli güvenliğe entegrasyonu, olarak sıralanmaktadır.

Strateji belgesine bir bütün olarak bakıldığında metnin, siber terörizmle ilgili olarak mevcut ve olası tehditleri dikkate alındığında, iyi hazırlandığını söylemek mümkündür. Bununla birlikte siber terörizmle etkin mücadele için uluslararası iş birliğinin önemi ve gerekliliği dikkate alındığında, metinde uluslararası iş birliğine yapılan referans yeterli değildir. "Uluslararası iş birliği" ifadesi metinde sadece "İlkeler" kısmında 4. maddede geçmektedir ve bunun nasıl olabileceğine ilişkin bir model veya tasarım yahut stratejik amaç ve eylem belirlenmemiştir. Uluslararası iş birliği açısından uluslararası sivil toplum örgütleri ayrıca önemlidir; ancak belgede buna ilişkin bir referans da bulunmamaktadır. Belgede diğer önemli bir eksiklik ise "etik kodlara" ilişkin bir kurgunun veya düşüncenin olmayışıdır. Çünkü yapay zekâ uygulamaları dikkate alındığında; sürecin bir tarafında ameliyat yapan robotlar varken, diğer tarafında Terminatör filmi örneğinde olduğu gibi katil robotlara gidebilecek bir süreç söz konusudur.[8] İnsanoğlu henüz bu tür zararlı yazılımların yapılmaması için ne tür etik kodlara sahip olması gerektiğini bilmemektedir. Bu kodlar; geleneksel manada bilinen ahlaka ilişkin tanımlamalar gibi mi, yoksa kodlar dünyasında özel bir biçime mi sahiptir yahut her ikisinin sentezi eklektik bir şey midir, bu henüz bilinmemektedir. Bu nedenle üniversitelerle iş birliği içerisinde etüt çalışmalarına ihtiyaç vardır.

Son olarak söz konusu belgede, stratejik amaçlar, yukarıda belirtilen risklere ilişkindir ve stratejik amaçlar, bu riskleri azaltmaya yöneliktir. Bu bağlamda stratejik amaçlar, saldırı sonrası ortaya çıkabilecek maddi zararları telafi etmeye ilişkin siber risk sigorta gibi mekanizmalara değinmemektedir. Diğer bir ifadeyle, saldırı sonrası tedbirler de mezkûr belgeye dâhil edilmelidir.

Sonuç

21. yüzyılda bilgi ve iletişime dayalı oluşumlar Bilgi Tabanlı Ekonomi, Bilgi Toplumu, e-Devlet, FTP tarzı örgütlenme, Para Yerine Geçenler ve Uluslararası Sivil Toplum Kuruluşları olarak ortaya çıkmaktadır.

Günümüzde bilgi sadece her şey değil, aynı zamanda ticaretin de bir aracı olmaktadır. Böylece bilgi yoğun ürünler, ülkelerin gayri safi milli

hasılası içinde önemli bir kalem olarak ortaya çıkmaktadır ki bu Bilgi Tabanlı Ekonomi olarak adından söz ettirmektedir.

Böyle bir ekonomi, Bilgi Toplumu olarak adlandırılan uygun bir çevreyi gerektirmektedir. Bu çevre, kişiyi Bilgi ve İletişim Teknolojilerine sahip olmaya zorlayacak bir çevredir. Diğer bir ifadeyle, teknolojinin gelişimi yeni bir çevrenin ortaya çıkmasına neden olmaktadır. İşte bu çevre, Bilgi ve İletişim Teknolojileri üzerine inşa edilen ve Bilgi Tabanlı Ekonominin yeşereceği Bilgi Toplumu'dur.

Bilgi Toplumunu inşa etmek ise hâkim ve otoriter güç olan devletin de bir dönüşüme uğratılmasını gerektirmektedir ki bu da e-Devlet olarak ortaya çıkmaktadır. e- Devletin ruhuna uygun olarak da gerek kamu gerekse özel sektörde ortaya çıkan örgütlenme yapısı ise FTP tarzı örgütlenme olup, bu örgütlenme tarzı aynı zamanda Bilgi Tabanlı Ekonominin bileşenleri olan bilgi ve hizmet sektörlerine uygun bir yapıdır.

Bilgi ve iletişime dayalı diğer bir oluşum ise maddi anlamda paranın ortadan kalkması ve manyetik ortamda sanal bir hal almasıdır. Dünyanın en büyük ekonomilerinden biri olmaya aday olan uluslararası sivil toplum örgütleri ise teknolojinin hız verdiği küreselleşmeyle birlikte göz ardı edilemeyecek önemli bir aktör haline gelmiştir.

Bilgi ve iletişime dayalı oluşumların uluslararası ilişkilere güvenlik bağlamındaki etkisi, söz konusu oluşumların siber tehditler ile aynı ortak altyapıyı kullanmasından kaynaklanmaktadır. Bunların başında ise siber terörizm yer almaktadır. 21. yüzyılda bilgi ve iletişime dayalı oluşumlar, diyalektik olarak kendini tehdit edebilecek oluşumları da beraberinde getirmektedir. Diğer bir ifadeyle, teknolojinin gelişmesi ve beraberinde getirdiği düzen anlayışı, diyalektik olarak yine bilgi ve iletişim teknolojileri üzerine inşa edilen bir tehdidi yani bu anlamda siber terörizmi- ayrıca siber suç ve siber savaş- ortaya çıkarmaktadır. Bu oluşumlardan uluslararası sivil toplum örgütleri hariç, diğer tüm oluşumlar siber terörizmin ortak altyapısı içerisindedir.

Siber terörizm, ihtiyaç duyduğu altyapı gereği, günümüz itibariyle özellikle gelişmiş ve gelişmekte olan ülkeleri tehdit etmektedir ve siber terörizmin tehdit alanı geniştir; çünkü e-devlet ile bilgi ve iletişim teknolojilerine dayalı herhangi bir hizmet yahut yapı, siber terörizmin hedefi olabilir.

Evrensel ve resmi bir siber terör tanımının olmayışı genel olarak terörizm olgusunda olduğu gibi terörle mücadeleyi zorlaştırmaktadır. Ulusal

düzeyde ise kamu ve özel kurumların siber tehditlerle mücadele de bilgisayar okuryazarlığından öte uzman personellere ihtiyacı vardır. Ayrıca kurumların bilgi ve iletişim teknolojilerine ilişkin altyapılarını geliştirmeye yönelik kapasite artırma kaygısını taşımaları gerekmektedir.

Teknolojinin beraberinde getirdiği siber terör gibi tehditlere karşı çözümler, daha iyi politikalar üretmekle mümkündür ki bu politikaların yolu da uluslararası düzeyde gerçekleştirilebilecek yoğun diplomasi ve iş birliğinden geçmektedir. Ancak iş birliğini zorlaştıran unsurlardan biri devletlerin siber terörizm aracılığıyla birbirlerine karşı bir çeşit Proxy savaşları (vekâleten savaşlar)[9] yürütmesinden kaynaklanmaktadır. Bu anlamda siber terörizm ile mücadele, klasik terörizmle mücadelede olduğu gibi aynı olumsuz kaderi paylaşmaktadır.

Diplomasi ise en başta empati yeteneğini içermeli ve güçten ziyade değerler üzerindeki ortak bilince dayanmalıdır. Bu anlamda uluslararası sivil toplum örgütlerinin, "Uluslararası Ceza Mahkemesi"nin kurulması ve "Kara Mayınlarının Yasaklanması Uluslararası Komitesi" hareketi örneklerinde olduğu gibi, terörizmle ve özelde siber terörizmle mücadelede de küresel bir farkındalık yaratma potansiyeline sahip olduğu söylenebilir.

Türkiye örneğinde 2016-2019 Ulusal Siber Güvenlik Strateji Belgesi incelendiğinde söz konusu belgenin siber terörizm ile ilgili tanımlamalar ve tehditler dikkate alındığında, iyi hazırlandığı söylenebilir. Bununla birlikte adı geçen belge, uluslararası iş birliğine yapılan referans açısından zayıftır, buna ilişkin içeriktense yoksundur. Uluslararası sivil toplum örgütlerine herhangi bir referansın olmayışı da bu iş birliğinin tesisi açısından önemli bir eksikliktir.

Belgede önemli diğer iki eksiklik ise “etik kodlara” ilişkin kaygının olmayışı ve saldırı sonrası tedbirlere ilişkin mekanizmalara yer verilmeyişidir. Bu açılardan belgenin revize edilmeye ve tamamlanmaya ihtiyacı olduğunu söylemek mümkündür.

Notlar

1. Gouldner’a göre teknik bilim adamları teorik bilgiye sahip olan bilim adamlarıdır. Yine Gouldner’a göre gelecekte teknik entelektüeller ve politik entelektüeller olmak üzere iki elit sınıf olacaktır (Gouldner’dan aktaran Dura ve Arik, 2002: 39).

2. Bununla birlikte ister bölgesel, ister ulus altı yahut etnik olsun herhangi bir oluşumun küresel dünyaya ulus devlet aracılığıyla eklemlendiğini göz ardı etmemek gerekir. Ulus devlet aynı zamanda küresel dünyaya eklemlenmenin motorudur. Diğer bir ifadeyle, küreselleşme sürecinde gelişme göstermek için ulus niteliğini kazanmak temel koşuldur (Mumcu, 2003: 506)

3. G7 ülkeleri olarak adlandırılan ABD, Birleşik Krallık, Almanya, İtalya, Fransa, Kanada ve Japonya, en fazla Bilgi ve İletişim Teknolojileri harcamaları yapan ülkelerin başını çekmektedir. Ayrıca G7'de yer alan Avrupa ülkeleri dışındaki İsveç, İsviçre ve Hollanda gibi diğer Avrupa ülkeleri, İspanya, Portekiz ve hatta gayri safi milli hasılasının yüzde onlara varan düzeyinde harcama yapan Kore ve Hon Kong listedeki diğer önemli ülkelerdir. Ayrıntı için bakınız http://www.econstats.com/wdi/wdiv_533.htm ve https://data.worldbank.org/indicator/GB.XPD.RSDV .GD.ZS?view=chart. Bilgi toplumunda ayrıca yaşam kalitesini ölçmek için yeni indeksler geliştirilmiştir. Bunlar arasında 1000 kişi başına düşen bilgisayar, eğitimde kullanılan kişisel bilgisayar sayısı, 1000 kişi başına düşen internet sayısı ve güvenli sunucu sayısı örnek olarak verilebilir.

4. Burada sivil toplumun öğelerini sıralamak kavramı daha anlamlı hale getirebilir. Sarıbay (1997)'a göre sivil toplumun öğeleri çoğulluk, kamusallık, özellik ve yasallıktır. Sivil toplumda hiç bir hakim ideolojinin rehberliğine ihtiyaç yoktur. Çoğulluk; sivil toplum içindeki toplulukların birbirlerine karşı özerkliklerini, kamusallık; birbirlerine karşı sorumluluklarını, özellik; birbirine karşı bireyselliği ve yasallık; tabi olunacak ortak çerçeveyi ifade etmektedir (Sarıbay, 1997: 108).

5. Uluslararası sermayeye karşı yerelde mücadele eden sivil toplum hareketleri ve bu sivil toplum örgütlerinin Dünya Sosyal Forumu temsilindeki/örneğindeki örgütlü mücadeleleri için Bové ve Luneau (2006)'nın Sivil İtaatsizliğe Çağrı kitabına ayrıntılı bilgi için başvurulabilir.

6. Benzer sonuçları, Smith, uluslararası ilişkiler disiplini için tasavvur etmektedir. "Bu yeni milenyumda nasıl bir uluslararası ilişkiler teorisi görmek istiyorum? Her şeyin ötesinde disiplin için doğal ve meşru olarak kabul edilen güçlülük olgusundan ziyade çeşitli meselelere, öznelliklere ve kimliklere açık olan bir disiplin görmek istiyorum. Farklı kültürlerdeki bireylerin öznelliklerini ve anlamlarını sorgulayan ve bunu yaparken de baskın dünya güçlerinin yaptığı gibi onları kendi rasyonellikleri, çıkarları ve

kimlikleri olarak algılamayan bir disiplin görmek istiyorum. Sosyal bilimlerde sadece bir model varmış gibi davranmayan, anlamak için pek çok rotayı benimseyen bir disiplin görmek istiyorum. Gerçeğin uyumlu teorileri üzerindeki sınırlamaların farkında olan, gerçeğe keşfedilmesi için bekleyen dünya mülkü olarak bakmayan ve gerçeği münazara ve anlama meselesi olarak kabul eden bir disiplin görmek istiyorum. Nihayet değer tarafsız ve deneyimcilik maskesi ardına gizlenmeyen bir disiplin görmek istiyorum. Bu görüşler belirgin sosyal çıkarlara hizmet eder ve böylece kaçınılmaz olarak politik ve yanlıdır. Sadece insan koşulunun doğasını anlamayla ve sosyal davranışı anlama ve yorumlama probleminin farkında olunmasıyla, uluslararası ilişkiler teorisini inşa edebiliriz…" (Smith, 2003).

7. Bu başlık altında anlatılanlar, kritik amaçlı olarak 2016-2019 Ulusal Siber Güvenlik Strateji Belgesinin özetlenmesinden ve tanıtılmasından ibarettir. Ayrıntı için bakınız http://www.udhb.gov.tr/doc/siberg/2016-2019guvenlik.pdf.

8. Google'ın başmühendisi Ray Kurzweil (2014), "süper-zekâ yazılımlarını kısıtlamaya gücü yetecek ahlak kodları yazmanın çok zor olabileceği" şeklinde bir kaygıyla dile getirmektedir.

9. Vekâlet Savaşları; devletlerin, özellikle küresel ve bölgesel güçlerin kendi çıkarlarını elde etmek ve nüfuz alanlarını genişletmek maksadıyla; kendi askeri unsurlarını kullanmaktan ziyade, müttefiklerini, edilgen ülkeleri, hedef ülkedeki parçalanmış yapıları ve yandaşlarını cepheye sürmek suretiyle gerçekleştirdikleri savaşlardır." (Sandıklı, 2016).

KAYNAKÇA

Alkin, E., Yıldırım, K. ve Özer, M. (2003). *İktisada Giriş*. Anadolu Üniversitesi: Eskişehir

Bilman, L. (2001). Hükümet dışı Kuruluşların (NGO) Dünya Ekonomik ve Sosyal Gelişindeki Rolleri. 04 Ocak 2018 tarihinde http://www.mfa.gov.tr/hukumetdisi-kuruluslarin-_ngo_-dunya-ekonomik-ve-sosyal-gelisimindeki-rolleri.tr.mfa adresinden alınmıştır.

BKM 2016 Yılı Mart Ayı Kart Verilerini Açıkladı. (2016). 05 Aralık 2017 tarihinde http://bkm.com.tr/wp-content/uploads/2016/01/BKM-Mart-2016-b%C3%BClteni.pdf adresinden alınmıştır.

Bové, J., ve Luneau, G. (2006). *Sivil İtaatsizliğe Çağrı*, (Çev. I. Ergüden), İstanbul: İletişim Yayınları.

Brenner, S. W (2007). At Light Speed: Attribution and Response to Cyber Crime/Terrorism/Warfare, *The Journal of Criminal Law&Criminology*, USA: Northwestern University, 97(2), 379-475.

Castells, M. (1998). *The Rise of the Network Society.* Oxford: Blackwell Publishers Inc.

Ceylan, C. (2010). Siber Savaşta Yeni Cephe: İRAN-Buşehr Nükleer Santrali ve SCADA-PLC Sistemler. 09 Ocak 2018 tarihinde http://www.bilgiguvenligi.gov.tr/siber-savunma/siber-savasta-yeni-cephe-iran-busehr-nukleer-santrali-ve-scada-plc-sistemler.html adresinden alınmıştır.

Coffman, J. L.(2006). Terrorism around Us. 02 Aralık 2006 tarihinde http://www.usadojo.com/articles/terrorism-around-us.htm adresinden alınmıştır.

Cooper, R. (2005). *Ulus Devletin Çöküşü*. (Çev. B. Karahan), İstanbul: Güncel Yayıncılık Ltd. Şti.

Credit Card Ownership Statistics. (2017). 09 Eylül 2017 tarihinde http://www.creditcards.com/credit-card-news/ownership-statistics.php adresinden alınmıştır.

Daugèliene, R. (2004). Pecularities of Knowledge-based Economy Assessment:

Theoretical Approach. 06 Aralık 2017 tarihinde https://www.lu.lv/jmconference2006/dokumenti/Papers/Rasa_Daugeliene.pdf adresinden alınmıştır.

Demirel, D. (2006). E-Devlet ve Dünya Örnekleri. *Sayıştay Dergisi***,** 61(2), 83-118.

Dinler, Z. (1995). *İktisada Giriş*. Bursa: Ekin Kitabevi.

Drucker, P. F. (2004). Post Capitalist Society, 20 Ağustos 2004 tarihinde http://www.vedpuriswar.org/book_summary/post_capitalist.html adresinden alınmıştır.

Dura, C. ve Atik, H. (2002). *Bilgi Toplumu, Bilgi Ekonomisi ve Türkiye.* İstanbul: Literatür Yayınları.

eEurope 2005: An Information Society for All. (2002). 08 Aralık 2017 tarihinde http://www.etsi.org/WebSite/document/aboutETSI/EC_Communications/eEurope2005_actionPlan.pdf adresinden alınmıştır.

the e-government Imperative. (2003). 16 Aralık 2017 tarihinde http://www.oecd-ilibrary.org/governance/the-e-government imperative_9789264101197-en adresinden alınmıştır.

Güneş, A., Ataizi, M., Aydın , C.H., Çalışkan, H., Hepkul, A., Şenel, H. ve Taşçı, C. (2003). *Temel Bilgi Teknolojileri*. Eskişehir: Anadolu Üniversitesi Yayınları.

Information and Communication Technology Expenditure % of GDP. (2017). 09 Ocak 2018 tarihinde http://www.econstats.com/wdi/wdiv_533.htm adresinden alınmıştır.

İnce, N. M. (2001). Elektronik Devlet. 19 Aralık 2017 tarihinde http://www.bilgitoplumu.gov.tr/wp-content/uploads/2014/04/ Murat_Ince_E-Devlet.pdf adresinden alınmıştır.

Karagül, S. (2007). Küresel Bir Aktör Olarak Uluslararası Sivil Toplum Kuruluşları. 11 Aralık 2007 tarihinde http://www.turkishweekly.net/turkce/makale.php?id=111 adresinden alınmıştır.

Kredi Kartı İşi Zarar Mı Ediyor? (2004). 23 Aralık 2017 tarihinde https://www.capital.com.tr/finans/bankacilik/kredi-karti-isi-zarar-mi-ediyor adresinden alınmıştır.

Kılıç, G. (2002). *Küreselleşme Karşısında Ulus Devlet*. (Yayımlanmamış Yüksek Lisan Tezi). Ankara Üniversitesi, Ankara.

Kissinger, H. (2002). *Amerika'nın Dış Politikaya İhtiyacı Var mı?* (Çev. T. Evyapan), Ankara: METU Press.

Kurt, S. (2012). Sivil Toplum Kuruluşlarında Çalışma İlişkileri. 20 Kasım 2017 tarihinde http://suleymankurt.com/akademik_detay_sayfasi.php?id=12 adresinden alınmıştır.

Kurzweil, R (2014). Yapay Zeka İnsanlığın Sonu Olacak Korkusu Gerçek mi? 29 Ocak 2017 tarihinde http://www.bbc.com/turkce/haberler/2014/12/141204_yapay_zeka_insanligin_sonu adresinden alınmıştır.

Muhammad, S. (2004). Urbanization Patterns In The Netherlands Under The Influence Of Information And Communication Technologies. 14 Ekim 2004 tarihinde http://www.uic.edu/cuppa/cityfutures/papers/webpapers/cityfuturespapers/session2_5/2_5urbanization.pdf adresinden alınmıştır.

Mumcu, A. (2003). *Atatürk İlkeleri ve Inkılap Tarihi (Cilt 2)*. Eskişehir: Anadolu Üniversitesi.

Özcan, M. (2005). Siber Terörizm ve Ulusal Güvenliğe Tehdit Boyutu. 04 Ocak 2018 tarihinde http://www.uiportal.net/siber-terorizm-ve-ulusal-guvenlige-tehdit-boyutu.html adresinden alınmıştır.

Özkazanç, Ö., Berberoğlu, C. N., Eren, E., Parasız, M. İ. ve Yıldırım, K. (2004). *İktisat Teorisi*. Eskişehir: Anadolu Üniversitesi.

Plan of Action. (2006). 06 Aralık 2007 tarihinde http://www.itu.int/wsis/docs/geneva/official/poa.html adresinden alınmıştır.

Pollitt, M. M. (2006). Cyber Terrorsim- Fact or Fancy. 04 Kasım 2017 tarihinde https://tr.scribd.com/document/21173253/Mark-M-Pollitt-Cyber-Terrorism-Fact-or-Fancy adresinden alınmıştır.

Research and Development Expenditure (% of GDP). (2017). 24 Aralık 2017 tarihindehttps://data.worldbank.org/indicator/GB.XPD.RSDV.GD.ZS?view=chart adresinden alınmıştır.

Sanal Kart. (2017). 10 Aralık 2017 tarihinde https://www.garanti.com.tr/tr/ticari/kredi_kartlari/e_ticaret/sanal_card.adresinden alınmıştır.

Sandıklı, A. (2016). Vekâlet Savaşları: Orta Doğu ve Türkiye. 09 Kasım 2017 tarihinde http://www.bilgesam.org/incele/2293/-vek%C3%A2let-savaslari--ortadogu-ve-turkiye/#.WbRbTKi0PIU adresinden alınmıştır.

Sarıbay, A.Y. (1997). Türkiye'de Demokrasi ve Sivil Toplum. İçinde F. Keyman ve A. Y. Sarıbay (Ed.), *Küreselleşme, Sivil Toplum ve İslam*. İstanbul: Vadi Yayınları.

Smith, K. (2002). What is the Knowledge Economy? Knowledge Intensity and Distributed Knowledge Bases. 23 Aralık 2017 tarihinde http://www.intech.unu.edu/publications/discussion-papers/2002-6.pdf adresinden alınmıştır.

Smith, S. (2003). Singing our world into existence: international relations theory and September 11. 29 Aralık 2017 tarihinde http://faculty.maxwell.syr.edu/.../isa_presidential_address.doc adresinden alınmıştır.

Sofaer, A. ve diğerleri (2000). A Proposal for an International Convention on Cyber Crime and Terrorism. 03 Aralık 2017 tarihinde http://cisac.fsi.stanford.edu/sites/default/files/sofaergoodman.pdf adresinden alınmıştır.

Spangenberg, J., Mesicek, R., Metzner, A. ve Luks, F. (2002). Sustainability Indicators for the-knowledge-based society. 08 Aralık 2007 tarihinde http://www.tukkk.fi/tutu/etieto/Futura_2_2002/02_2_085-095.pdf adresinden alınmıştır.

Şıklar, İ. (2005). *Para Teorisi ve Politikası*. Eskişehir: Anadolu Üniversitesi.

Taşçı, C. (2003). Bilgi Teknolojileri. İçinde C. H. Aydın, Y. Hoşcan ve A. E. Özkul (Ed.), *Temel Bilgi Teknolojileri* (ss.1-20). Eskişehir: Anadolu Üniversitesi Yayınları.

Terzi, M. (2015). Siber Terörizm, E-Devlet ve Aktör-Ağ Kuramı**.** İçinde M. Terzi ve S. Yenal (Ed.), *Uluslararası Güvenlik ve Terörizm (Seçme Konular)* (ss.181-212). Ankara: Sinopsis Yayınları.

Terrorist Activities on the Internet. (1998). 18 Aralık 2007 tarihinde http://www.adl.org/Terror/focus/16_focus_a.asp adresinden alınmıştır.

Türkiye Bilişim Şurası (2002). *e- Devlet Raporu (2002)*. Türkiye Bilişim Vakfı, Ankara.

Toft, G. S. (2002). Human Capital Policies for the Knowledge Economy. 07 Ocak

2018 tarihinde http://slideplayer.com/slide/6335775/ adresinden alınmıştır.

Towards Knowledge-Based Economy. (2002). 07 Aralık 2007 tarihinde www.unece.org/operact/enterp/documents/coverpagregion.pdf adresinden alınmıştır.

Ulusal Siber Güvenlik Stratejisi (2016-2019). 17 Ocak 2018 tarihinde http://www.udhb.gov.tr/doc/siberg/2016-2019guvenlik.pdf adresinden alınmıştır.

Why are ICTs Important for Civil Society Organizations? (2010). 29 ocak 2018 tarihinde http://www.un.org/esa/socdev/ngo/docs/2010/ directory/ictcso.pdf adresinden alınmıştır.

Yücetürk, B. (2016). Sivil Toplum Kuruluşları, Resmi Kurumlar Dışında ve Bunlarda… 06 Aralık 2017 tarihinde https://prezi.com/gq29_8j6zjnq/sivil-toplum-kuruluslar-resmi-kurumlar-dsnda-ve-bunlarda/ adresinden alınmıştır.

Yücetürk, E. E. (2004). Türk Kamu Yönetiminde E-Devlet Uygulamaları ve Tabana Yayılabilme Yeteneği Bakımından Bir Değerlendirme: Bolu Örneği. 08 Nisan 2004 tarihinde http://www.bilgiyonetimi.org/cm/pages/mk1gos.php?nt=225 adresinden alınmıştır.

EXTENDED SUMMARY

The Formations Based on Information and Communication Technologies and the Effects of These Formations on the International Relations in the Context of Security: Cyber Terrorism

(The Case of Turkey in the Scope of 2016-2019 National Strategy Document for Cyber Security)

The formations which are based on information and communication technologies in the 21st century are emerging as Knowledge Based Economy, Information Society, e-Government, FTP style organization, Money Substitutes and International Non-Governmental Organizations.

Today, knowledge is not only everything but also a means of trade. Thus, knowledge-intensive products are emerging as an important item in the gross national product of countries, which makes it known as Knowledge-Based Economy.

Such an economy requires an appropriate environment, called as Information Society. This environment is a medium that will force a person to have the products of Information and Communication Technologies. In other words, the development of technology leads to the emergence of a new environment. This environment is built on Information and Communication Technologies. This environment is the Information Society that Knowledge-Based Economy flees.

Constructing the Information Society requires that the authoritarian state, too, be undergoing a transformation, which emerges as an e-Government. In accordance with the spirit of e-Government, the organizational structure that emerges both in the public and private sectors is the FTP style organization, which is also a structure suitable for the information and service sectors which are the components of the Knowledge Based Economy.

Another formation based on information and communication is the loss of money in a material sense but a virtualization in the magnetic environment. As for NGOs, international non-governmental organizations,

which are candidates to be one of the world's largest economies, have become an important actor that cannot be ignored with the globalization that technology is accelerating.

The impact of information and communication-based formations on international relations in the context of security is due to the use of the same common infrastructure in conjunction with cyber threats. At the head of these is the cyber terrorism. Formations based on information and communication technologies in the 21st century also bring about entities that can threaten themselves as dialectically. In other words, the development of technology and the sense of order that it brings together, dialectically, creates a threat built on information and communication technologies such as cyber terrorism (and also cyber-crime and cyber war). All of these formations, except for international non-governmental organizations, are in the common infrastructure of cyber terrorism.

The infrastructure required by cyber terrorism threatens particularly developed and developing countries today, and the threat of cyber terrorism is widespread; because any service or structure based on e-government and information and communication technologies may be the target of cyber terrorism.

The lack of a universal and formal definition of cyber terrorism generally makes it difficult to fight terrorism as it is in the case of terrorism. At the national level, public and private institutions need more expert staff than computer literacy to combat cyber threats. In addition, institutions need to have capacity building anxieties to improve their infrastructures for information and communication technologies.

Solutions to threats such as cyber terrorism brought by technology are possible by producing better policies, which can be achieved through intense diplomacy and cooperation at the international level. However, one of the elements which make the cooperation difficult is that the states carry out some kind of proxy battles against each other through cyber terrorism. In this sense, the struggle with cyber terrorism shares the same negative fate as it is in the struggle with classical terrorism.

Diplomacy, in the first place, should include empathy and be based on common knowledge of values rather than power. In this sense, it can be said that international non-governmental organizations have the potential to create a global awareness to fight against terrorism and cyber terrorism in

particular, as in the case of the establishment of the "International Criminal Court" and the "International Committee for the Ban on Landmines".

In Turkey, for example, when the National Cyber Security Strategy Document 2016-2019 examined, considering the definitions and threats related to cyber terrorism situated in the said document, it can be said that it is well-prepared. However, the said document is weak in terms of reference to international cooperation, and the content related to international cooperation is lacking. The absence of any reference to international non-governmental organizations is a major drawback for the establishment of this cooperation, as well.

Two other important deficiencies in the document are the lack of "ethical codes" and the lack of mechanisms for post-attack measures. Therefore, it is possible to say that the document needs to be revised and made up for deficiencies.