Volgy, T. J., K. Kanthak, D. Frazier, and R. S. Ingersoll. (2004). Structural Versus Relational Strength: The Cohesion of the G7 and the Development of the Post-Cold War International System. *Fifth Annual Pan European International Relations Conference*.

Walt, S. M. (1997). The Progressive Power of Realism. *The American Political Science Review*. Vol 91. No 4. 1997.

Wilhelmsen, V. C. R. (2014). *Soft War in Cyberspace: How Syrian Non-state Actors Use Hacking to Influence the Conflict's Battle of Narratives*. Master's Thesis - Political Science, Universıty of Oslo.

Winston, H. R. (2011). On the Nature of Military Theory. Charles Lutes (ed.). *Toward a Theory of Spacepower: Selected Essays*. Washington: NDU Press.

Yüksel, M. (2016). 3. Dünya Savaşı Öncesi Siber Güç Testinde Zayiat Büyük. http://www.yenisoz.com.tr/3-dunya-savasi-oncesi-siber-guc-testinde-zayiat-buyuk-makale-16757 (Erişim Tarihi: 01.10.2017).

Yüksel, M. (2017). Siber Savaş Oyunları. http://www.yenisoz.com.tr/siber-savas-oyunlari-makale-22631 (Erişim Tarihi: 09.09.2017).

Zacher, M. W. (1992). The Decaying Pillars of the Westphalian Temple: Implications for International Order and Governance. James N. Rosenau and Ernst-Otto Czempiel (eds). *Governance Without Government*: *Order and Change in World Politics*. Cambridge University Press.

ULUSAL SİBER GÜVENLİK STRATEJİ BELGELERİNDE İNSAN HAKLARI

Gül Nazik ÜNVER[*]

Özet

Bu çalışmada, siber alanda ABD, Türkiye, İngiltere, Almanya ve Hollanda'nın ulusal siber güvenlik strateji belgelerinde insan haklarının nasıl işlendiği, uluslararası insan hakları koruma

[*] Doktora Öğrencisi, Selçuk Üniversitesi, İİBF-Uluslar arası İlişkiler Bölümü, E-mail: gulunver@outlook.com

mekanizmaları da dikkate alınarak bu düzenlemelerin insan hakları üzerindeki etkileri analiz edilmektedir. Bunun için öncelikle, ulusal siber güvenlik perspektifiyle ortaya koyarak ülkelerin güvenlik yaklaşımlarına, hukuki düzenlemelerine odaklanarak yeni bir bakış açısı ve farklı bir boyut getirmesi açısından gereken adımlar ve öneriler üzerinde durulacaktır. Özellikle çalışma, belirli bir ulusun siber güvenliğe ilişkin hukuki yaklaşımı bağlamını netleştirmek için, ulusal bilgi toplumu ile ulusal siber güvenlik stratejisi hedeflerinin bir literatür taramasını sunmaktadır.
Anahtar Kelimeler: Siber Güvenlik, Strateji Belgesi, İnsan Hakları, Koruma mekanizmaları

HUMAN RIGHTS IN NATIONAL CYBERSECURITY STRATEGY DOCUMENTS

Abstract

In this paper, the United States, Turkey, United Kingdom, Germany, the Netherlands and Belgium's national cyber security strategy documents and their impact on human rights and international human rights protection mechanisms are being analyzed in the cyber space. First of all, this work will focus on steps and suggestions with a new outlook for bringing a different dimension by focusing on legal regulations of countries, the security approaches of countries by putting forward the perspective of national cyber security. In particular, the paper describes security and strategic management tasks. To clarify the context of the legal approach to a specific nation's cyber security, it presents a literatute review of the objectives of the national information society and the national cyber security strategy.
Key Words: Cybersecurity, National Strategy Document, Human Rights, protection mechanisms.

Giriş

Yirminci yüzyılda yaşanan teknolojideki hızlı gelişmeler, insan yaşamını etkilemiş, hızlandırmış, değiştirmiş ve dönüştürmüş, aynı zamanda siber alanda büyük ilerlemelere neden olmuştur. Siber uzay, yaşamın her noktasını ve toplumun her tabakasını birçok açıdan etkilemekle beraber, internet kullanımı yaşam tarzını da değiştirmektedir. Siber alanda yaşanan ilerlemeler ile bilgi dijital ortamda yani siber ortamda üretilebilmektedir. Siber ortamda bilginin çoğaltılması, erişilmesi ve paylaşılması oldukça kolay hale gelmiştir. Fakat geçmişte de değerli olan bilginin, elektronik hale gelmesi ve bilişim sistemleri ile yoğun bir şekilde paylaşılması maruz kaldığı tehdidi artırmakta ve bilgi güvenliği kavramına yeni bir boyut kazandırmaktadır. Bu sayede ülke sınırlarının, mesafelerin, mekânın ve zamanın kısıtlamalarından kurtularak, her türlü bilgiye erişebilen yeni bir dünya oluşurken, bunun yanı sıra bilginin güvenliğini sağlamak

zorlaşmakta, bilginin bulunduğu ve iletildiği siber ortam güvenliği de önem kazanmaktadır. Böylece faaliyet alanlarını zorunlu olarak siber uzaya taşıyan ülkeler için ulusal güvenlik, siber uzaydaki güvenlik çerçevesinde yeniden değerlendirme mecburiyetini ortaya çıkarmıştır (Bayraktar, 2015: 18-19).

Bugün insanlar, telekomünikasyon ve bilgi teknolojilerindeki gelişmeler sonucunda sınırları ve mesafeleri göz önünde bulundurmadan kolayca iletişim kurabilirler. Siber uzayın getirdiği sınırsız özgürlük ortamında oluşturulan sanal kavramlar, giderek gerçek dünyayı, kişileri ve devletleri etkileyecek güvenlik sorunlarını da beraberinde getirmiştir. İnternete bağlantılı herhangi bir bilgisayar sisteminin veya ağının başka bilgisayar sistemleri veya ağlarına karşı kötü amaçlı eylemler gerçekleştirmek maksadı ile kullanılması, çağımızın siber suçlara karşı alınacak siber güvenlik önlemlerini sorgulamamızı gerektirmektedir. İnternetin ortaya çıkışı ile beraber siber tehditler de artmaya devam etmiştir. Siber uzayda bulunan bilginin değiştirilmesi, bilginin açığa çıkarılması, erişilebilirliğinin kesintiye uğraması gibi istenmeyen durumlara neden olan siber tehditler, bilgi ve iletişim teknolojilerinin getirdiği imkânların araç olarak kullanıldığı, klasik suçların siber ortama uyarlanmasını sağlamıştır (Ünver, Canbay ve Mirzaoğlu, 2009: 8). Bu durum siber güvenliğin bireysel, ulusal ve küresel alanda önemini artırmış ve alınması gereken önlemler için hukuki boyutunu da vurgulamıştır.

21. yüzyılda insanlar adeta iki ayrı dünyada yaşar hale gelmiştir. Bir yanda ülke sınırlarının, ulusal egemenliklerin, hukuki düzenlemelerin, özgürlüklerin ve hakların bulunduğu, herkesin belirli bir kimlikle tanımlandığı fiziki gerçek dünya yer alırken; diğer yanda ise fiziksel ve özgürlük anlamında sınırların, hukuksal düzenleme ve güvenlik tedbirinin bulunmadığı, kimliklerin gizlenebildiği siber alan yer almıştır (Bayraktar, 2015: 15). Ancak, bu yeni ortamda yaşam, özgürlük ve güvenlik hakkı arasında bir denge kurmak ne kadar mümkündür? Siber alan güvenlik, istikrarsızlık ve insan hakları da dâhil olmak üzere birçok açıdan uluslararası ilişkileri etkiledi. Bu nedenle, kimin kontrol edeceği? ya da kontrol edilmeli mi? anlamında sorunlu bir konu olmuştur (Akyeşilmen, 2016: 39).

Devletlerin siber tehditlere ne kadar açık olduğunun ilk ölçütü, ülkenin kendi yetenekleri, insan hakları boyutu ve siber güvenlik algısıdır. Güncel meseleler daha çok sanal çerçevede gelişme gösterdiği için bireye ve topluma yönelik bilinmeyen bir konumdan, hızlı ve çabuk tehdit türlerini de beraberinde getirmiştir. Bu tehditler özellikle siber uzayda karşımıza çıkarak, küreselleşmeyi, teknolojik ilerleme ve yeniliği de ortaya çıkarmaktadır. İnsan hakları açısından

temel hak ve özgürlüklerin ulusal strateji belgelerinde yoğun bir şekilde göz ardı edilmesi ve hatta siber saldırılarda bireyin ve kamu kurumlarının almış olduğu tehditlere karşı siber güvenliğin strateji belgelerinde yetersiz kalması en önemli sorunların başında gelmektedir. Sorumlular tespit edilse dahi, bu konuda gerekli yaptırımları uygulamaya yardımcı olacak hukuki açıdan herhangi bir uluslararası mekanizma yoktur. İnsan hakları ve siber güvenlik arasındaki ilişki iki yönlüdür: tüm kullanıcılar için güvenli bir siber alan oluşturmak ve siber alanda güvenli bir insan hakları ortamı oluşturmak. Siber güvenlik ve insan hakları gibi nispeten yeni olan bu iki gerçek birbiriyle derin ilişkili ve birbirine bağlıdır. Her ikisini de sağlayabilecek bir uluslararası mekanizma geliştirmeliyiz. Çalışmanın yanıt aradığı temel soruları şu şekilde sıralamak mümkündür:

"Genel kabul görmüş ulusal siber güvenlik tanımı var mı?"
"*Siber güvenliği ele alırken temel insan hakları endişeleri nelerdir?"*
"Ulus-devletlerin hukuki açıdan birey ve kurumların temel hak ve özgürlüklerini kısıtlayıp kısıtlamaması siber güvenlik strateji belgelerinde nasıl değerlendirilmektedir?"
"ABD, Türkiye, İngiltere, Almanya, Hollanda'nın ulusal siber güvenlik anlayışı nasıl şekillenmektedir?"
"Ulus-devletlerin siber güvenlik strateji belgelerine, insan hakları boyutu açısından sağladığı eylemler nelerdir?"

Yukarıdaki sorulardan yola çıkılarak yapılan araştırmalar sonucu, bu çalışmanın temel noktası, ulusal siber güvenlik strateji belgesinin kurgusal temel olarak siber güvenlik yaklaşımı ve insan hakları kavramının açıklanabildiği ve ulusal strateji belgeleri ile bu savı güçlendirdiğidir. Bu çalışmada; siber güvenliği tanımlayarak, strateji belgesinin ne olduğu, siber güvenlikte insan haklarının nasıl olması gerektiği ve ne gibi önlemler alınması gerektiği üzerine tartışılmaktadır. Ardından tarihsel süreç içerisinde ABD, Türkiye, İngiltere, Almanya ve Hollanda'nın ulusal siber güvenlik strateji belgelerinde somut gelişmelerin insan hakları boyutu üzerine etkili olup olmadığı ve her bir ülkenin siber güvenlik kabiliyetlerini incelemektedir. Bu nedenle ulus-devletlerin ulusal güvenliğini de tehdit edecek seviyeye gelen siber alanda ve insan hakları boyutunun etki alanını kapsayan siber alanda, saldırılara karşı alınan ve uygulamaya konulmaya çalışılan önlemler için ulusal siber güvenlik strateji belgelerinin varlığı bu çalışmaya esin kaynağı olmuştur. Ayrıca devletlerin ulusal strateji belgeleri üzerinde almış olduğu önlemlerin insan hakları bağlamında ele alınarak sonuç kısmında kısa bir değerlendirme yapılacaktır.

Siber Güvenlik ve İnsan Hakları

Siber güvenlik, tanımları nispeten değişken, çoğunlukla öznel ve bazen de bilgi sahibi olunmadan geniş yelpazede kullanılan bir terimdir. Siber güvenliğin çok boyutlu olmasını yakından tanımlayan özlü, genel kabul edilebilir bir tanımın bulunmaması, karmaşık siber güvenlik sorunlarını çözmek için uyumlu olarak hareket etmesi gereken disiplinleri birbirinden ayırırken, pratikte de sorunlara neden olabilmektedir. Literatürde çok çeşitli tanımlara rastlamak mümkündür. Örneğin, *Defining Cybersecurity* başlıklı makalede "Siber güvenlik, siber-alan ve siber-alan sistemlerini fiili (de facto) mülkiyet haklarından hukuka (de jure) aykırı olaylardan korumak için kullanılan kaynakların, süreçlerin ve yapıların organizasyonu ve toplanması" olarak tanımlanmıştır (timreview, 2017). Diğer bir tanımda siber güvenlik, "siber alanda kurum, kuruluş ve kullanıcıların varlıklarını korumak amacıyla kullanılan araçlar, politikalar, güvenlik kavramları, güvenlik teminatları, kılavuzlar, risk yönetimi yaklaşımları, faaliyetler, eğitimler, en iyi uygulamalar ve teknolojiler bütünü*"* olarak tanımlanabilmektedir (Ünver, Canbay ve Mirzaoğlu, 2009: 1-2). Siber güvenlik, kurum, kuruluş ve kullanıcıların varlıkları, bilgi işlem donanımlarını, personeli, altyapıları, uygulamaları, hizmetleri, telekomünikasyon sistemlerini ve siber ortamda iletilen veya saklanan bilgilerin tümünü kapsamaktadır. Siber güvenlik, elektronik ortamı oluşturan bilişim sistemlerinin zarar verilmesini, bu sistemlere yetkisiz bir şekilde erişilmesini veya bu sistemlerin suiistimal edilmesini önlemeyi içermektedir. Dolayısıyla siber güvenlik, gizlilik bütünlük, erişilebilirliği sağlamayı amaçlamaktadır (Ünver, Canbay ve Özkan, 2010: 36-37).

Siber güvenlik, teknik bir disiplinden stratejik bir konsepte hızla dönüşmüştür. Küreselleşme ve internet, sürekli gelişmekte olan ağ teknolojisi üzerine kurulu bireylere, örgütlere ve uluslara olağanüstü yeni bir güç vermektedir. Siber güvenlik için devletlerin tek başına çabaları yetmez, işbirlikleri ve hatta devlet dışı aktörlerle birlikte hareket etmeleri önemlidir. En başarılı uluslararası siber güvenlik anlaşması, 2001'de imzalanan Avrupa Siber Suç Sözleşmesi'dir. Bu antlaşma, telif hakkı ihlali, dolandırıcılık, çocuk pornografisi ve ağ güvenliği politikasının ihlal edilmesi konularını kapsıyor. Veri kesme ve bilgisayar ağlarının aranmasına ilişkin kolluk kuvvetleri için kurallar sunmaktadır. Nihai amacı ulusal mevzuat ve uluslararası işbirliği vasıtasıyla dünya çapında siber suç konusunda ortak bir politika oluşturmaktır. Hâlihazırda, kırk yedi taraf imzacıya sahiptir, otuza kadar ulus-devlet onaylamıştır ve ulus devletler için siber güvenlik açısından temel yasal sözleşmedir (Geers, 2011: 29-30).

Siber uzaydaki tehditlerin çoğunluğu birden fazla değişken ile ortaya çıkmaktadır. Tehdidin çok boyutlu olması, savunma ve koruma içinde benzer bir yaklaşımı zorunlu kılmaktadır. Hamleler gizlilik gerektirdiği durumda, gelişmiş ağ güvenlik çözümleri ortaklıkların kurulmasına ihtiyaç duymaktadır (Bıçakçı, 2013: 39). Başlangıçta, internet genellikle insan haklarının geliştirilmesi ve korunması için ütopik bir terim olarak tanımlanmıştı. Demokratikleşmenin ve insan haklarının hayata geçirilmesine yol açarak, tüm bilgiyi özgürleştiren, bireyleri güçlendiren ve devleti daha şeffaf ve hesap verebilir hale getirerek zayıflatacak olan bir alanı temsil ediyordu (Akyeşilmen, 2016: 51).

İnsan hak ve özgürlükleri evrenseldir. Evrensel insan hakları, kozmopolitan bir dünya görüşü ve siyaset modeli öngörmektedir. Kozmopolitan anlayış uluslararası ilişkiler yaklaşımına göre, bireyi ve insan gruplarını başlangıç noktası olarak ele almaktadır. İnsan hakları ülkeden ülkeye farklılık göstermeyen, esasında insan onurunun korunarak bireyin insanca yaşamasını sağlayan temel haklardır. Birleşmiş Milletler kurucu yasası, İnsan Hakları Evrensel Bildirgesi ve Sivil ve Siyasal Haklar ile Sosyal ve Ekonomik Haklar Sözleşmelerinde imza atmış olan bütün ulus-devletler, insan haklarının "ulusal" olmakla beraber "uluslararası bir nitelik ve boyut" taşıdığını kabul etmişlerdir (Dağı, 2010: 219-222).

Strateji Belgesi Nedir ve Nasıl Olmalıdır?

Ulusal bir siber güvenlik stratejisinin hazırlanması görevi karmaşıktır. Siber tehditlere yönelik önlemler bir takım farklı alanlardan gelmektedir: politik, teknolojik, yasal, ekonomik, yönetsel veya askeri nitelikte olabilirler. Dahası belirli risklere uygun diğer disiplinleri içine alabilirler. Bu yetkinliklerin hepsi, güvenliği güçlendirecek ve tehditlere karşı direnebilecek tepkiler sunmak için bir araya gelmesi gerekmektedir. Birçok ülke kendi ulusal strateji belgelerinde siber güvenlikle ne kastettiklerini tanımlamaktadır. Hükümetler, işletmeler ve vatandaşlar, siber dünyanın insan yapımı olduğunu, sezgisel ve giderek genişleyen bir çevre olduğunu bilmektedir. Bu nedenle tanımlar daima değişmektedir. *"National Cyber Security Framework Manual"* kılavuzunun yayınlanmasından bu yana elliden fazla ülke, güvenliğin gelecekteki ulusal ve ekonomik güvenlik girişimleri için ne anlam ifade ettiğini belirten bir çeşit siber strateji belgeleri yayınlamıştır. Strateji Belgesi, belirli hükümet kollarının ve bilgi güvencesi ilkelerinin, kamu, özel ve ilgili uluslararası Bilgi ve İletişim Teknolojileri sistemlerine ve bu

sistemlerin doğrudan ulusal güvenlik ile ilgili olduğu içerikle ilişkili olarak uygulanmasıdır (Klimburg, 2012: 12).

Nispeten yakın zamana kadar, "ulusal güvenlik" terimi yalnızca Amerika Birleşik Devletleri'nde kullanılıyordu. Birçok OECD ülkesinde "ulusal güvenlik stratejileri"nin (NSS) yaygın olarak tanıtılması, birkaç özel "tehdit"e odaklanarak, sayısız riske karşı olan fikri stratejik düşünce değişiminde katı biçimde bağlı olduğu görülen yeni bir olgudur. Örneğin, 2007 sonrası stratejilerin neredeyse tamamında, siber güvenlik kilit bir ulusal güvenlik meselesidir. Nitekim bazı durumlarda, "siber güvenlik" (hatta "ulusal siber güvenlik") konusu, ulusal güvenlik stratejisinin oluşturulmasını öngörmektedir ve bazen daha kapsamlı bir ulusal paradigmaya kayma için bir rehber gibi işlev görmektedir. Stratejilerde devlet sadece çeşitli risklere karşı önlem alınması gerektiğini değil, devlet dışı aktörlerle birlikte çalışarak da risklerin çözümlenebileceğini kabul etmektedir (Klimburg, 2012: 20).

Hükümetler, ulusal düzeyde stratejik eylem planları ve siber güvenlik için kurumlar da dâhil olmak üzere ulusal düzeyde belge ve girişimler geliştirmeye çalışmaktadırlar. Sanal gerçekliği yakalamak için, ulusal stratejik eylem planları ve inisiyatiflerin, ilgili kilit konuları çerçevelemesi ve insan hakları ile ulusal güvenlik hususlarını dengelemesi ve siber tehditlere yönelik uluslararası işbirliğinin geliştirilmesi konularında önemli sorunları tanımlaması gerekmektedir (Akyeşilmen, 2016: 51-52).

Bir stratejinin oluşturulması, politika yapıcılar için bir araçtır. İyi gelişmiş bir strateji, politika yapıcılara temel hedefler, gerekli kaynaklar ve bunları en etkin şekilde nasıl kullanabilecekleri konusunda rehberlik yapmalıdır. Belirli bir alanı kapsayan tek başına bir strateji söz konusu olduğunda, özellikle karar verme ve politika yapıcılar arasında farkındalık düzeylerinin yükseltilmesi için uygulamayı kolaylaştırmak önemli olabilir (Klimburg, 2012: 64). Her bir hükümet sistemi, ele alınması gereken kendi özel durum kümesini sağlayacak ve her belirli strateji bireysel yetkileri vurgulamak isteyecektir. Optimal bir dünyada, ulusal bir siber güvenlik stratejisi (veya NCSS) oluşturmanın tüm süreçlerinin basamak basamak alt süreçlerden oluştuğunu görmek mümkündür. Bu nedenle, strateji belgesinin sunabileceği en önemli katkı bir NCSS'deki en kritik meselelere ilişkin farkındalık yaratmak ve nasıl tanımlanabileceğini belirlemektir (Klimburg, 2012: 191).

ENISA, Nisan 2013'te Ulusal Siber Güvenlik Stratejisini belirleyen ülkeleri kendi web sitesinde sıralamıştır. ENISA'nın 2010 yılından itibaren siber güvenliği sağlamada daha önemli rol oynayabilmesi için yetkileri artırılmıştır. ENISA ile ABD İç Güvenlik Bakanlığı bu alanda işbirliği yapmak adına *'Cyber Atlantic'* adı altında bir faaliyet de düzenlemiştir. Faaliyet çeşitli siber saldırılar için senaryolar üretmek ve bunlara karşı koymak üzere yapılacak çalışmaları içermektedir (sibersavunmalar, 2017). Her strateji, siber faydalar ile siber riskler (veya tehditler) arasındaki dengesiz dengeyi vurgularken, siber dünyanın önemini ve dijital bir toplumun kazanımlarını onaylamayla başlar.

Ulusal bir siber güvenlik stratejisi (NCSS) genellikle teröristler, dış ülkeler, casusluk, organize suç veya siyasi aktivizm dâhil olmak üzere tehditler üzerine bir bölüm içermektedir. Stratejiler genellikle önemli terimleri de tanımlamaktadır. Bununla birlikte, kesin tanımlar, açıklamalarda kullanılan tanımlar ve anlamdaki açıklığa göre daha az önem taşıyabilmektedir. Bütün NCSS'ler aynı tanımları kullanmamaktadır. Örneğin, bazıları *"siber alanı"* sadece internet için, diğerleri ise daha geniş bir tanımlamayı benimsemektedir. Herhangi bir ulusal strateji gibi, bir NCSS'de hükümet birimlerinin vizyonunu tutarlı ve uygulanabilir politikalara çevirmesini sağlamalıdır. Hükümetin uluslararası meselelerde nasıl davrandığını açıklayan ve diğer ilgili stratejilere bağlantı oluşturan bir strateji belgesi oluşturulmalıdır (Klimburg, 2012: 196).

Bazı Ulusal Siber Güvenlik Strateji Belgelerinde İnsan Hakları

Soğuk Savaş'ın sona ermesiyle beraber interneti sağlayan ağlar giderek artmıştır. Soğuk Savaş döneminde öncelik verilen durum bilgi güvenliği üzerine olmuştur. Bilgisayar teknolojisinin kullanımının yaygınlaşması ile kişisel bilgilerin saklanması ve şifrelenmesi noktasındaki ihtiyaçlar ortaya çıkmıştır. Siber güvenlik alanındaki tehditlerin birçoğu farklı çeşitlerde kendini göstermiştir. Tehdidin çok boyutlu olması, sınırlarının belirlenememesi, saldıranın kimlik ve yerinin bilinememesi, insan haklarını siber alanda savunmayı güçleştiren nedenler arasında sayılmaktadır. Siber alan kullanıcısına sınırsız fayda sağlarken, insan hakları ihlaline açık hale getirmiştir.

New York ve Washington'da 11 Eylül 2001 tarihinde yolcu uçaklarını çeşitli hedeflere çarparak yapılan terör saldırıları, uluslararası sistemdeki güvenlik tanımlarını değiştirmiştir. Soğuk Savaş'ın ardından ulusal güvenlik üzerine yapılan görüşler birçok ülkenin listesinde yeniden ilk sıraya çıkmıştır. Terörizme karşı savaş yalnızca saldırıya uğrayan ulus-devletin değil,

neredeyse sistemdeki tüm aktörlerin gündemine girmiştir. Saldırılardan hemen sonra internet üzerinden iletişim kurmuş olduklarının ve kullandıkları uçakları daha önce simülasyon uygulamasında çalışmış olduklarının fark edilmesi üzerine internet ortamının terörist saldırılar için kullanılmakta olduğu düşüncesini giderek artırmıştır (Thomas, 2003: 115-121). Siber güvenliğin ihlali çok farklı şekillerde yapılmış durumdadır. Ulusların siber sistemlerine yönelik saldırılarla ülkenin durumunu derinden zedeleyecek olan ekonomik ve diğer kritik alt yapılara hasar verilerek etkisiz hale getirilebileceğine inanılıyordu. Bu tür kaygıların ulusal güvenlik ile yakın olarak bağlantılı olduğu düşüncesi ile devam etmiş ve izleyen süreçte birçok ülke siber güvenlik stratejilerini ulusal güvenlik belgelerine eklemişlerdir. Bundan dolayı ulusal strateji belgeleri düzenli olarak güncellenmektedir (Bıçakçı, 2013: 32-33).

Peki insan hakları bu belgelerde nasıl işlenmektedir? Birkaç örnek üzerinden bu konuyu irdelemek yararlı olacaktır.

Amerika Birleşik Devletleri ve Siber Strateji Düzenlemeleri

Savunma Bakanlığı Siber Kullanım Stratejisi, Mayıs 2011'den beri siber faaliyetlerini ve operasyonlarını ABD'nin ulusal çıkarlarını desteklemek için rehberlik etmiştir. Amerika Birleşik Devletleri Savunma Bakanlığı (DoD), ABD vatanını ve ABD'nin çıkarlarını siber alanda meydana gelebilecek saldırılar da dâhil olmak üzere saldırıdan korumaktan sorumludur.

> *ABD ve uluslararası hukuka uygun bir şekilde, Savunma Bakanlığı, barış, kriz veya çatışma dönemlerinde ABD ulusal çıkarlarına zarar vermeye çalışan herhangi bir düşmana karşı saldırıları caydırmaya ve ABD'yi savunmaya çalışmaktadır. Bu amaçla Savunma Departmanı, siber operasyonlar için yetenekler geliştirdi ve bu yetenekleri, Birleşik Devletler hükümetinin diplomatik, askeri, ekonomik, finansal ve kanuni uygulama araçları da dahil olmak üzere ABD'nin ulusal çıkarlarını savunmak için kullandığı tüm araçlara entegre etti* (USA, 2015: 3).

DoD, bir etki yaratabilecekleri siber saldırıları engellemek, kolluk kuvvetleri, istihbarat ve diplomatik araçları dahil etmek için çeşitli seçenekler ve yöntemler geliştirmek üzere diğer kamu kurumlarıyla yeteneklerini senkronize etmeyi amaçlamaktadır (USA, 2015: 4). ABD'nin, tehdit ve riskler konusunda daha fazla kamuoyu bilincini geliştirmesi ve ulusun güvenlik

ihtiyacı anayasa ve yasalarla güvence altına alınan gizlilik haklarına ve kişisel özgürlüklere ulusal taahhüdüne yönelik entegre bir yaklaşım sağlamak için siber güvenlik konusunda ulusal bir diyalog yürütmesi gerekmektedir (USA, 2011: 13-15).

Strateji belgesine göre, Birleşik Devletler'de İnternetin açık, güvenli ve erişilebilir olmasının sağlanması ve insan hayatının korunmasının gerekli olduğu gibi, her zaman kısıtlayıcı bir doktrin kapsamında siber operasyonlar yürütülmesi de gereklidir. Siber alanda Savunma Departmanı daima, hukukun üstünlüğünü destekleyerek, ifade özgürlüğüne ve gizliliğine saygı duyarak, ABD'nin değerlerini koruyarak, bilgi, ticaret ve fikirlere önem vererek özgür hareket edecektir. Savunma Bakanlığı kanun uygulaması (law enforcement), istihbarat, karşı istihbarat ve politika kuruluşlarının tamamı DoD'nin ağlarını ve bilgi teknolojisi sistemlerini kuran ve işleten bireyler gibi aktif bir role sahiptir. Uygulanabilir tüm kanunlara ve politikalara uygun olarak, DoD, küresel ağlar ve sistemler, düşman yetenekleri ve kötü amaçlı yazılım aracıları ve pazarları hakkında ayrıntılı, öngörülebilir ve uygulanabilir istihbarat gerektirmektedir (USA, 2015: 24).

Son dönemde yayınladığı ulusal siber güvenlik strateji belgesinde Amerika, sadece ülke içinde değil küresel çapta da insan haklarının korunmasına vurgu yapmaktadır: "Sözlerimiz ve eylemlerimizle birlikte baskıcı rejimler altında yaşayan insanlara, özgürlük, kişisel onur ve hukukun üstünlüğünü arayanlara destek vereceğiz. Özgür ve müreffeh toplumumuzun çıkarlarını baskıcı rejimlere ve insan haklarını kötüye kullanan toplumlara sunma yükümlülüğümüz bulunmamaktadır" (USA, 2017: 42). ABD için sınırları ve göç sistemini kontrol altına almak ulusal güvenlik, ekonomik refah ve hukukun üstünlüğü için merkezi bir noktadır (USA, 2017: 8).

Türkiye'nin Siber Güvenlik Strateji Raporları

Uzun süre Türkiye'de yetkililer siber tehditleri yalnızca siber suç seviyesinde değerlendirmiş ve önemli güvenlik kurumlarına yönelik yapılan saldırılar, terörle mücadele çerçevesinde ele alınmıştır. TÜBİTAK (Türkiye Bilimsel ve Teknolojik Araştırma Kurumu) bünyesinde kurulan birimler ve ulusal bilgi güvenliği kapısıyla devlet kurumlarındaki siber güvenliğe yönelik bilinçlenme çalışmaları giderek hızlanmıştır. Milli Güvenlik Kurulu 27 Ekim 2010 tarihinde siber tehditler üzerine toplantıda bu konuyu tartışmıştır. Toplantıda siber tehditler kavramının Milli Güvenlik Siyaset Belgesi'ne girmesine karar verildiği duyurulmuştur. 25-28 Ocak 2011

tarihlerinde TÜBİTAK ile Bilgi Teknolojileri ve İletişim Kurumu (BTK) işbirliği ile *"Birinci Ulusal Siber Güvenlik Tatbikatı"* icra edilmiştir(TÜBİTAK ve BTK, 2011). Tatbikatın ardından yayınlanan raporda, Türkiye'nin siber saldırılara karşı savunmasız ve açık olduğunu, kamu kuruluşlarının konuyla yeterince ilgilenmediklerivurgulanmıştır.

2012 yılında *"Redhack"* adlı grubun Türkiye'de birçok kamu kuruluşuna yaptığı saldırılar ve bu saldırıların medyada yer alması, Türkiye'de siber tehdit algısının oluşmasını hızlandırmıştır. Bunun üzerine 20 Ekim 2012 tarihinde toplanan Bakanlar Kurulu, *"Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Karar"*ı onaylamıştır (Bıçakçı, 2013: 45-46). Bu kararda siber güvenlik kurulunun strateji belgesi ve eylem planı olarak Ulaştırma, Denizcilik ve Haberleşme Bakanlığı başkanlığınca oluşturulmasına karar verilmiştir. Bu kurulun görevi "kamu kurum ve kuruluşlarınca bilgi teknolojileri üzerinden sağlanan her türlü hizmet, işlem ve veri ile bunların sunumunda yer alan sistemlerin güvenliğinin sağlanmasına ve gizliliğin korunmasına yönelik tedbirlerin alınması ve bilgi ve iletişim teknolojilerine ilişkin kritik altyapıların işletiminde yer alan gerçek ve tüzel kişilerce uyulması gerekli usul ve esasları düzenlemek" olarak açıklanmıştır (Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, 2012).

Türkiye bu düzenlemelerin ardından artan tehdit göz önüne alınarak ikinci Ulusal Siber Güvenlik Tatbikatı yapılmıştır. 25 Aralık'ta başlayan ve sekiz aşamalı olan tatbikata katılan altmış bir kurum ve kuruluşa gerçek siber saldırılar düzenlenmiştir. NATO'nun yeni oluşan tehditler karşısında geliştirdiği politikasıyla eşgüdümlü olarak Türk Silahlı Kuvvetleri 21 Ocak 2013 tarihinde Siber Savunma Merkezi Başkanlığı'nı oluşturduğunu açıklamıştır. Bu başkanlığın Ulaştırma, Denizcilik ve Haberleşme Bakanlığı ile koordineli çalışacağı, NATO tatbikatlarına katılacağı da belirtilmiştir (Bıçakçı, 2013: 46-47).

Türkiye'nin ilk belgesi olan 2013-2014 Ulusal Siber Güvenlik Strateji Belgesi'nde siber güvenlik ve insan hakları için, "…teknik boyutun yanı sıra; hukuki, idari, ekonomik, politik ve sosyal boyutlarda güçlü ve zayıf yönlerin, tehditlerin ve fırsatların belirlenmesini içeren bütüncül bir yaklaşım benimsenir. Hukukun üstünlüğü, temel insan hak ve hürriyetleri ile mahremiyetin korunması ilkeleri temel esas kabul edilir" (Türkiye, 2013, 14-15). Ulusal siber güvenliğin sağlanması konusunda gerek kurum ve kuruluşların görev, yetki ve sorumluluklarını tanımlayan, gerekse ihtiyaç duyulan alanlarda mevcut eksiklikleri gidermeyi amaçlayan mevzuatın oluşturulması çalışmaları yapılacağı belirtilmektedir. Söz konusu bu çalışmalar, ceza

hukuku, medeni hukuk, idari yargı ve bunlara ilişkin tüm usul hükümlerinin düzenlenmesine destek olacak bir nitelik arz etmektedir. Ayrıca, kavram kargaşasının önüne geçmek amacıyla siber güvenlik terminolojisi ve sözlüğünün oluşturulacağı ifade edilmiştir:

> *Uluslararası hukuk kuralları çerçevesinde, siber saldırılara maruz kalan tarafların haklarının korunabilmesi için, saldırı kaynağının tespiti ve saldırılan sistemler ile bu sistemlerden hizmet alan taraflarda hangi boyutta etki oluştuğunun belirlenmesi gerekir. Bu bilgilerin üretilmesi için ulusal siber ortamın günün teknolojisine uygun ve güvenilir kayıt mekanizmaları ile donatılması gerekmektedir*(Türkiye, 2013: 18).

2016-2019 için Türkiye'nin ikinci ulusal siber güvenlik strateji belgesi yayımlanmıştır. Türkiye, diğer ülkelerin strateji dokümanlarında olası siber güvenlik risklerine ve riskleri ortadan kaldıracak eylemler uygulanmasını göz önünde bulundurmuştur. Bu nedenle ikinci strateji belgesinde bu ilkelere yer verilmekte, risklerin ve ilkelerin ülkeden ülkeye çok fazla değişiklik arz etmediği gözlemlemektedir. Bu noktada göz önünde bulundurulan insan hakları ve hukukun üstünlüğünü de dikkate alan ilkeler şunlar olmaktadır:

> *Siber güvenliğin sağlanması için tüm paydaşların siber güvenlik risklerini bilmeleri, bu risklerin yönetilmesine ilişkin yaklaşımlarının kendileri kadar başkalarını da etkileyebileceğinin bilincinde olmaları gerekir. Bu farkındalık ve yetkinliğin sağlanması için tüm paydaşların gerekli eğitim ve deneyimi kazanmaları sağlanır. Teknik boyutun yanı sıra; hukuki, idari, ekonomik, politik ve sosyal boyutları da içeren bütüncül bir yaklaşım benimsenir. Tüm paydaşlar, siber uzay güvenliğinin sağlanması için çalışırken, hukukun üstünlüğü, ifade özgürlüğü, temel insan hak ve hürriyetleri ile mahremiyetin korunması ilkelerini gözetir (Türkiye, 2016: 11).*

Alıntıdan da anlaşıldığı üzere, siber güvenliğin temelinde yer alan kavramlarından birisi hukukun üstünlüğü ve insan haklarıdır. Bu çerçevede, atılacak adımların bu ilkelere uygun olması önem arz etmektedir.

İngiltere Siber Güvenlik Strateji Belgesi

Ulusal güvenlik stratejisi gibi sadece devletin değil, vatandaşların da korunmasını öngören siber güvenlik strateji belgesi, bütün kesimlerin dolandırıcılığın her türünden, kimlik hırsızlığından ve teknoloji kullanılarak işlenen siber suçlardan korunmasının yollarını belirlemektedir

(timeturk, 2009). İngiltere'nin 2010 yılında yayınlamış olduğu strateji belgesinde ulusal çıkarlarının; "hukukun üstünlüğü, demokrasi, özgür ifade, hoşgörü ve insan hakları*"* karşısında ülkenin inancı ile bağdaşarak ilerlemesini sağlamaktır. Bunlar, İngiltere'nin dünyada sahip olduğu nitelikler ve "biz onları ilerletmeye devam etmeliyiz, çünkü değerlerimiz dünyada saygı görürse İngiltere daha güvenli bir konumda olacaktır" (İngiltere, 2010: 4). Stratejisi, olmak istedikleri ülkeyi yansıtarak; değerlerine ve fikirlerine güvenen refah sahibi, güvenli, modern ve dış görünüşlü bir ulus oluşturmaktır. Ülkenin milli menfaati güvenlik, refah ve özgürlüktür. Güvenli ve dayanıklı bir İngiltere inşa etmek ve dengeli bir dünyanın şekillenmesine yardımcı olmak için ulusal gücün tüm araçlarını bir araya getirebilen bir ulus olmaları gerektiğini vurgulamaktadırlar. "Bizim bakış açımız, esneklik ve esneklik ile karakterize edilecek ve insan haklarına, adalete ve hukukun üstünlüğüne olan bağlılığımız tarafından desteklenecektir" (İngiltere, 2010: 10).

Kurallara dayalı uluslararası sistemi uygulamak için BM gibi mevcut uluslararası kurumları ve G20 gibi ortaya çıkan kuruluşları güçlendirmeyi amaçladığını ileri sürmektedir. Güvenliğimizi destekleyen yapılardaki gelişmelere adapte olmak ve bunları etkilemek için de değişime ihtiyaç olacaktır. "ABD'yle olan ilişkimiz merkezli ve kalıcı olacak ancak gelişmeye devam etmesini beklemeliyiz. NATO yeni stratejik konseptini formüle edecek ve uygulayacak; AB'nin uluslararası rolü gelişecek; BM Güvenlik Konseyi de reforma tabi tutulabilir. Uluslararası hukuk ve normları şekillendirmede aktif bir rol oynamaya devam edeceğiz*"* (İngiltere, 2010: 15).

Başlangıç olarak, Birleşik Krallık, tüm hükümetlerin siber alanda ve ulusal ve uluslararası hukuka uygun olarak orantılı olarak hareket etmesi gerektiğine inandığını ifade ediyor. Bu, fikri mülkiyete saygı ve ifade ve dernek kurma özgürlüğüne ilişkin temel insan hakları da içermektedir (İngiltere, 2011: 27). Siber ortamda uluslararası insan hakları hukuku çerçevesinin nasıl uygulanacağını ve bu hakların garanti altına alınmasında yeni zorlukları tartışmak için çok taraflı ve iki taraflı kanallar kullanmayı öncelikli kıldığını ifade etmektedir (İngiltere, 2011: 40).

2016-2021 Ulusal Strateji Belgesine göre; ulusal ve uluslararası kanunlara uygun olarak hareket etmeleri ve başkalarının da aynı şeyi yapmasını beklediklerini ifade etmektedir. Temel değerlerin titizlikle koruması ve desteklenmesi gerektiği vurgulanmaktadır. Bunlara demokrasi dâhildir. Hukuk Kuralı, özgürlük, açık ve hesap verebilir hükümetler ve kurumlar, insan hakları

ve ifade özgürlüğü, İngiltere vatandaşlarının özel hayat ve mahremiyetlerini koruyacaklarını belirtmektedir. Hükümetin öncelikli görevi, ülkeyi diğer devletlerin saldırılarına karşı savunmak, vatandaşlarına ve ekonomilerine zarar vermeden çıkarlarını korumak, temel haklarını korumak ve suçluları adalete teslim etmek için ulusal ve uluslararası çerçeveyi oluşturmaktır (İngiltere, 2016: 25).

Siber güvenlik sadece teknoloji ile ilgili değildir. Başarılı siber saldırılardan hemen hemen tümünün katkıda bulunduğu bir insan faktörü vardır. Bu nedenle, hükümette çalışan herkesin siber bir riskin bilincinde olmasını sağlamak için halkına yatırım yapmayı devam edeceğine değinilmektedir. Risklerin arttığı alanlarda spesifik bir siber uzmanlık geliştirecektir ve bu riskleri etkili bir şekilde yönetmek için doğru süreçleri bulunduklarından emin olunacaktır (İngiltere, 2016: 38).

Siber meselelerde uluslararası işbirliği, daha geniş küresel ekonomik ve güvenlik tartışmalarının önemli bir parçası olmuştur. Tek bir uluslararası vizyon olmadan hızla gelişen bir politika alanıdır. İngiltere ve müttefikleri, kurallara dayanan uluslararası sistemin bazı unsurlarının yerine getirilmesini sağlamada başarılı olmuştur. Online olarak yaptıkları gibi insan haklarının geçerli olduğunu ve çok paydaşlı yaklaşımın, İnternet yönetiminin karmaşıklığını yönetmenin en iyi yolu olduğu konusunda geniş bir fikir birliğine varılmıştır. Ancak, ulusal güvenliği bireysel haklar ve özgürlükler ile uzlaştırmanın ortak meydan okumalarını nasıl ele alınacağına dair giderek artan bir bölünme ile birlikte, küresel uzlaşma hala kırılgan kalmaktadır (İngiltere, 2016: 63).

Almanya ve Siber Alanda İnsan hakları

2011’in başında yayımlanan Almanya Siber Güvenlik Strateji Belgesinde siber alan, tüm bölgesel sınırların ötesinde internet üzerinden erişilebilen tüm bilgi altyapılarını içermektedir. Almanya'da sosyal ve ekonomik yaşamın her noktasında, siber olanaklar kullanılmaktadır. Gittikçe birbirine bağlı bir dünyanın parçası olarak, Almanya’daki devlet, kritik altyapılar, işletmeler ve vatandaşlar, bilgi ve iletişim teknolojisinin ve internetin güvenilir çalışmasına bağlı olmaktadır. Almanya’da bilgi altyapılarının artan karmaşıklığı ve güvenlik açığı göz önüne alındığında, siber güvenlik durumu gelecekte de kritik olarak kalacaktır.

Siber güvenlik, hak ve hürriyetlerin uygulanması ve kritik bilgi altyapılarının korunmasını sağlamaktadır. Ayrıca devletin hem ulusal düzeyde hem de uluslararası düzeyde ortaklarla işbirliği yapmasını gerektirmektedir. Devlet, endüstri ve toplumun paylaştığı sorumluluklar göz önüne alındığında, bir siber güvenlik stratejisi tüm kişilerin ortak hareket edip görevlerini yerine getirmesi ile başarılı olacaktır. Aynı şey, uluslararası durum için de geçerlidir. Bilgi ve İletişim Teknolojileri sistemleri küresel ağlarda birbirine bağlandığından, diğer ülkelerin bilgi altyapılarındaki olaylar dolaylı olarak Almanya'yı etkileyebilmektedir. Bu nedenle siber güvenliği güçlendirmek için uluslararası yönetişim kurallarını, standartlarını ve normlarını uygulanması gerekmektedir (German NCSS, 2011: 2).

Siber güvenlik kapsamlı bir yaklaşıma dayalı olmalıdır. Bu, daha da yoğun bilgi paylaşımı ve koordinasyon gerektirmektedir. Siber Güvenlik Stratejisi ağırlıklı olarak sivil yaklaşımlara ve önlemlere odaklanmalıdır. Bilgi ve iletişim teknolojisinin küresel doğası göz önüne alındığında, uluslararası koordinasyona, yabancılara ve güvenlik politikası yönlerine odaklanan uygun ağlar vazgeçilmez olmaktadır. Buna sadece Birleşmiş Milletler'de değil, aynı zamanda AB, Avrupa Konseyi, NATO, G8, AGİT ve diğer çokuluslu örgütlerde işbirliği de dâhildir. Amaç, uluslararası toplumun siber alanı korumak için tutarlılık ve yeteneklerini sağlamaktır. Alınacak stratejik hedefler ve önlemler olarak;

Kritik bilgi ve altyapıların korunması,
Almanya'da güvenli Bilgi ve İletişim Teknolojileri sistemlerinin oluşturulması,
Kamu yönetiminde Bilgi ve İletişim Teknolojileri sistemlerinin güçlendirilmesi,
Ulusal siber güvenlik konseyi ve yanıt merkezinin kurulması,
Siber alanda da etkili suç kontrolünün yapılması,
Avrupa'da ve dünyada siber güvenliği sağlamak için etkin ve uyumlu bir eylem koordine edilmesi,
Güvenli ve güvenilir bilgi teknolojisinin kullanılması,
Siber saldırılara tepki veren araçların yapılması gerekmektedir (German NCSS, 2011: 3-8).

2016 yılında hazırlanan Almanya Ulusal Siber Güvenlik Strateji Belgesinde insan haklarına vurgu yapılmaktadır:

Almanya'nın ekonomik ve siyasi ağırlığı, insan haklarını, özgürlüğü, demokrasiyi, hukukun üstünlüğünü ve uluslararası hukuku savunmak için Avrupalı ve transatlantik

ortaklarımızla birlikte işbirliği içinde olmasını gerektirmektedir. Dahası Avrupa güvenliğiyle ilgili sorumluluğu üstlenmek bizim görevimiz anlamına gelmektedir. Paylaşılan değerlerimiz için daha da ayağa kalkmalı güvenlik, barış ve bugüne kadar yaptığımızdan daha fazla kurallara dayalı bir düzen üzerine büyük bir bağlılık göstermeliyiz. (German, 2016: 6).

Alman anayasasının başlangıcında Almanya, "birleşik bir Avrupa'da eşit bir ortak olarak dünya barışını destekleme*"* kararlılığını belirtmektedir. Birleşmiş bir Avrupa temelinde, Almanya'nın arzusu aynı zamanda insanların birlikte yaşamasının koşullarını sürdürülebilir bir şekilde iyileştirmek ve uluslararası insan hakları normlarını korumak ve güçlendirmektir (German, 2016: 22). Alman hükümetinin amacı, vatandaşları için özgürlük, güvenlik ve refah sağlamak, barışı geliştirmek ve hukukun üstünlüğünü güçlendirmek olarak ifade edilmiştir. Alman güvenlik politikası değerlerine bağlıdır ve çıkarları tarafından yönlendirilmektedir. Ulusal çıkarları için yol gösterici ilkeler, özellikle insan onuru ve diğer temel haklar (Avrupa Hukuku ve Uluslararası Hukuk, özellikle Evrensel İnsan Haklarının Korunması ve Barışın Sağlanması), demokrasi ve hukukun üstünlüğü gibi anayasanın değerlerini vurgulamaktadır (German, 2016: 34).

Hollanda Siber Güvenlik Stratejisinde İnsan Hakları

Hollanda, güvenli ve güvenilir Bilgi ve İletişim Teknolojisini (BİT-ICT1) ve açık, özgür bir internetin korunmasını desteklediğini ifade etmektedir. Toplumun BİT'e büyümekte olan bağımlılığı, giderek BİT'in kötüye kullanımını ve bozulmasını sağlayarak savunmasız kılmaktadır. Bu nedenle, Hükümet geniş bir yelpazeye yayılmış kamu ve özel kurumlardan, bilgi kurumlarından ve sivil toplum kuruluşlarından gelen girdi ile bir Ulusal Siber Güvenlik Strateji Belgesi hazırladı. 2011'de yayımlanan NCSS1'in amacı, kamu-özel ortaklıklarına dayalı bir entegre siber güvenlik yaklaşımı ile güvenli, güvenilir ve esnek dijital alan yaratmak ve ardından toplum için fırsatları en iyi şekilde değerlendirmek olarak belirtilmiştir.

Haziran 2011'de yayımlanan Strateji, iki kısma ayrılmıştır. Birinci bölümde, sorunun analizi sunulmakta, siber güvenlik için politika ilkeleri anlatılmakta ve hedefler belirlenmektedir. İkinci kısım, her biri hükümet tarafından uygulanacak olan siber güvenliği artırmak için öncelikli hedefler içeren ve diğer taraflarla işbirliği içinde olmak üzere birçok eylem dizisi belirtmektedir. Hollanda Strateji Belgesi ve Eylem Planı'nda BİT, vatandaşları ve ekonomileri

için büyük önem teşkil etmektedir. Siber Güvenlik'te amaç, BİT'nin bozulması, kesilmesi veya yanlış kullanımı yüzünden tehlike veya hasardan kaçınmaktır. Karışıklık, bozulma veya yanlış kullanımdan kaynaklanan tehlike veya zarar, BİT'in varlığı veya güvenilirliği üzerindeki sınırlamalardan, BİT'te saklanan bilgilerin gizliliğinin ihlalinden veya bu bilgilerin bütünlüğünden kaynaklanıyor olabilir (Kaska, 2015: 6-7).

> *Güvenli ve güvenilir BİT, refahımız için vazgeçilmezdir ve daha sürdürülebilir ekonomik büyüme için bir katalizör görevi görmektedir. Avrupa'da verimlilik artışının% 50'si BİT'in kullanımından kaynaklanmaktadır. Hollanda, dijital toplumun" güvenliğini garanti ederken dünyayı BİT kullanımında liderlik etmeyi amaçlıyor. Hollanda, Avrupa Dijital Ağ Geçidi olmak istiyor.* (Netherlands, 2011: 3-4).

Dijital ortamdaki mevcut tarafların ulusal ve uluslararası düzeyde işbirliği yapması gerektiği vurgulanmaktadır. Siber çatışmalar ortaya çıktığında, yalnız, bir örgüt, bir devlet veya üçünün bir kombinasyonu olabilecek faili tanımlamak genellikle zordur. Siber tehdidin doğası da genellikle net değildir. Ancak birçok siber saldırı aynı teknik ve yöntemleri içermektedir. Belirli tehdit türleri üzerinde çalışan kamu kurumları, ağ ve bilgi altyapısını koruyan işletmeler ve bilgi kurumları da dâhil olmak üzere siber güvenlikle ilgili taraflar arasındaki daha fazla işbirliğinin önemini göstermektedir. Siber saldırılar ve aksamalar ulusal sınırları, kültürleri ve hukuk sistemlerini anında aşmaktadır. Genellikle veri iletiminde hangi hukuk yetkisi uygulanacağı belirsizdir ve yasanın her zaman etkin bir şekilde uygulanıp uygulanamayacağı genellikle belirsizdir.

Strateji belgesi sivil ve askeri kurumlar, kamu ve özel kurumlar ile ulusal ve uluslararası taraflar arasındaki tüm güvenlik sistemi boyunca işbirliğine öncelik verilmesini amaçlamaktadır. Ancak o zaman, BİT altyapısının kritik sektörlerdeki dayanıklılığını, siber saldırılara hızlı ve etkili bir tepki ve dijital alanlardaki yasal korumayı sağlayabileceğini belirtmektedir. Siber güvenlik alanında çok şey yaşanmaktadır. Ancak tutarlılık birçok alanda eksiktir. Bu gözlem, Siber Suç ve Dijital Güvenlik Eğilimlerine Dair 2010 Ulusal Raporu ve Ulusal Güvenlik Think Tank'in Bilişim Teknolojileri Güvenlik Açığı ve Ulusal Güvenlik hakkındaki raporunun bulgularıyla ortaya çıkmıştır (Netherlands, 2011: 5).

Hükümet mümkün olan yerlerde mevcut girişimleri inşa edecek ve gerekirse yenilerini geliştirecektir. Tüm kullanıcılar (bireyler, işletmeler, kurumlar ve kamu kurumları), kendi BİT

sistemleri ve ağlarını güvence altına almak ve diğerlerine karşı güvenlik risklerini ortadan kaldırmak için uygun önlemleri almalıdır. Hassas bilgileri depolarken ve paylaşırken dikkat etmeli ve diğer kullanıcıların bilgi ve sistemlerine saygı göstermeleri gerekmektedir. Bakanlıklar arasındaki sorumlulukların bölünmesi Güvenlik ve Adalet Bakanı, ulusal güvenlik stratejisi uyarınca, siber güvenlikle ilgili tutarlılık ve işbirliğinden sorumludur. Aynı zamanda, siber güvenlik sistemindeki her partinin kendi görev ve sorumlulukları vardır. Tehditlerin sınır ötesi doğası, uluslararası işbirliğini teşvik etmeyi gerekli kılmaktadır. Uluslararası düzeyde bir oyun alanı hedeflemeliyiz. Birçok önlem, ancak uluslararası kabul veya koordine edilmesi durumunda etkili olabilir. Hollanda, AB'nin Avrupa için Dijital Gündemi ve İç Güvenlik Stratejisi, NATO'nun yeni stratejik vizyonu olan İnternet Yönetim Forumu ve diğer ortaklıkların bir parçası olarak siber savunma politikasının geliştirilmesi gibi çabaları desteklemekte ve aktif olarak katkıda bulunmaktadır. Hollanda, Avrupa Konseyi Siber Suçlar Konvansiyonunun yaygın olarak onaylanmasını ve uygulanmasını savunmaktadır (Netherlands, 2011: 11).

2011 Strateji Belgesinde önlemlerin orantılı olmasını, insan haklarına saygılı olmasını ve paydaşlar arası işbirliğinin gerekliliğini vurgulanmaktadır:

> *%100 güvenlik diye bir şey yok. Siber güvenlik faaliyetlerinde Hollanda, risk değerlendirmesine dayalı seçimler yapar. Bunu yaparken, gizlilik, başkalarına saygı, ifade özgürlüğü, bilgi toplama ve temel haklar gibi toplumumuzun başlıca değerlerini korumayı amaçlıyoruz. Hâlâ kamu ve ulusal güvenliğe olan arzumuz ile temel hakların korunması arasındaki dengeye ihtiyacımız var. Önlemlerin orantılı olması gerekir. Bu amaçla, mevcut denetleme araçları da dâhil olmak üzere gerekli yerlerde güçlendirilmesi, korunması ve test mekanizmalarının oluşturulması yoluna başvuracağız. Gerektiğinde mevzuat kamu ve özel sektör, öncelikle kendi kendini düzenleme yoluyla aradıkları BİT güvenliğini sağlayacaktır. Özdenetim çalışmazsa, Hükümet mevzuatın kapsamını inceleyecektir. Ancak mevzuat üç şartı karşılamalıdır: rekabeti gereğinden fazla bozmamalı ve mümkün olduğunca düzgün bir oyun alanı sağlamalıdır; idari yük, orantısız bir şekilde arttırılmamalıdır ve maliyetler yararları ile makul orantılı olmalıdır. Hızlı hareket eden bir dünyada yaşıyoruz ve mevzuat kısa sürede eskimiş hale gelebilir. Hükümet, mevzuatın BİT'teki gelişmelere göre ayarlanması gerekip gerekmediğini değerlendirecektir.* (Netherlands, 2011: 12-15).

Güvenlik, özgürlük ve sosyal ekonomik faydalar arasında korelasyon, hem ulusal hem de uluslararası tüm paydaşlar arasında sürekli olarak açık ve pragmatik bir diyalog içinde gerçekleştirilmesi amaçlanan dinamik bir dengedir. Kişisel bilgilerin işlenmesi ve gizliliğin korunması, kısmen Avrupa mevzuatına dayanan katı standartlara ve denetime tabidir (Netherlands NCSS2, 2014: 7-8). Temel hak ve değerleri korumak birçok tarafın çaba sarf etmesini ve tercihen ulusal ve uluslararası bağlamda yer almasını gerektirmektedir. Önerilen yaklaşım uluslararası standartların geliştirilmesini bağlı kılmaktadır. Hükümetlerin yanı sıra, özel sektör kurumları ve sosyal organizasyonlar tarafından önemli bir rol oynanabilir. Hollanda, Birleşmiş Milletler'de, Londra, Budapeşte ve Seul'de düzenlenenler gibi uluslararası siber konferanslar sırasında, İnternet Yönetim Forumu gibi diğer çoklu paydaş ortamlarında, Dünya Ekonomik Forumu tarafından yayınlanan siber güvenlik ilkelerini teşvik etmektedir. Ayrıca güven inşası geliştirmek için Avrupa Güvenlik ve İşbirliği Teşkilatı (AGİT) gibi devletlerarasındaki önlemleri uluslararası düzeyde desteklemektedir (Netherlands NCSS2, 2014: 18).

Ulusal Siber Güvenlik Strateji Belgesi'nde İnsan Hakları Nasıl Düzenlenmelidir?

Ulusal güvenlik stratejilerinin (NSS) formülasyonu oldukça yeni bir olgudur. 1990'ların sonlarına veya 2000'lerin başına kadar ulusal güvenlik stratejisine sahip ülkelerin çoğunluğu ilk güvenlik stratejilerini değerlendirmeye almış ve takip etmişlerdir (Klimburg, 2012: 45). Siber güvenlik, ulus-devletler tarafından farklı anlamlarda kullanılmaktadır. Küresel çapta BM tarafından bu konuda kabul edilen bir anlaşma olmadığı için, dünya üzerinde uzlaşılan ve kabul edilen yegâne bir tanımı da yoktur. Her ülke kendi ulusal siber güvenlik strateji belgesini yayınlamış ve siber güvenlik kavramına farklı tanımlar yapmıştır. Dolayısıyla siber güvenlik alanındaki tanımlar farklı ülkelerce yapılsa da benzer noktaları olmuştur. Ancak tanımların bir kısmı benzer olsa bile çeşitli tanımlar yapıldığı için bu durum ulus-devletleri farklı önlemler almaya itmiştir. Her ülke kendi tanımını yapmakta ve yaptığı tanımı doğru kabul etmektedir. Bu doğrultuda dikkatlerden kaçan en önemli nokta, ulusal strateji belgelerinde sorulması gereken "kimin için, ne için ve nasıl bir siber güvenlik" sorularıdır. Ancak ulusal strateji belgelerinde bu soruların yanıtlarını bulmak oldukça güç olmuştur (Akyeşilmen, 2016).

Genel olarak, ulusal bir strateji farklı hedeflere sahip olabilir: Bunlar, (1) Bütün hükümet kurumlarını aynı bakış açısına sahip kılmak, (2) Kamu ve özel planlamayı tutarlı bir şekilde odaklamak, koordine etmek ve tüm paydaşlar arasında öngörülen rolleri, sorumlulukları ve

ilişkileri ilerletmek, (3) Bir kişinin ulusal niyetini diğer uluslara ve paydaşlara iletmek (Klimburg, 2012:60).

Franklin ve diğerlerine göre, insan hakları ve internet ilkeleri yönetmeliğinde yaşam, özgürlük ve güvenlik hakları çevrimiçi olarak saygı görmeli, korunmalı ve yerine getirilmelidir. Bu haklar çevrimiçi ortamda ihlal edilmemeli veya diğer haklarını ihlal etmemelidir (Franklin, Bolde ve Hawtin, 2014: 7). Erişim hakkında, herkesin yararlanması için internet sağlanmalı ve yasalarca sağlananlar dışında herhangi bir kısıtlamaya tabi olunmamalıdır.

Demokratik bir toplumda ulusal güvenlik, kamu düzeni, halk sağlığını veya ahlakını veya başkalarının haklarını ve özgürlüklerini korumak için bu haktan yararlanma hakkı mevcut sözleşmede tanınan diğer haklarla uyumlu olmalıdır. UDHR'nin 3. maddesinde belirtildiği üzere: *"*Herkesin yaşama hakkı, kişilik özgürlüğü ve güvenliği hakkı vardır". Tüm güvenlik önlemleri uluslararası insan hakları hukuku ve standartlarıyla uyumlu bir biçimde olmalıdır. Bu, güvenlik önlemlerinin istisnai koşullar haricinde başka bir insan haklarını (örneğin gizlilik hakkı veya ifade özgürlüğü hakkı) kısıtladıkları durumlarda yasadışı olacağı anlamına gelmektedir. Tüm kısıtlamaların kesin ve dar bir şekilde tanımlanmış olması gerekmektedir. Tüm kısıtlamalar, Uluslararası Hukuk uyarınca yasal olarak kabul edilen ve bu ihtiyaçla orantılı olarak gerçek bir ihtiyacın karşılanması için gereken asgari düzeyde olması önem teşkil etmektedir. Sınırlamalar, her hakka özgü ek ölçütleri de karşılamalıdır. Bu katı sınırların dışındaki sınırlamalar yasaktır. Herkes, internette güvenli bağlantıların keyfini sürme hakkına sahiptir. Buna virüsler, kötü amaçlı yazılımlar ve kimlik avı gibi İnternet'in teknik işlevini tehdit eden hizmetlerden ve protokollerden korunma da dâhildir (Franklin, Bodle, Hawtin, 2014: 13-15). BM Sivil ve Siyasi Haklar Anlaşmasında ortaya konduğu gibi, ifade özgürlüğü hakkı belirli kısıtlamalara tabi olabilir, ancak bunlar yalnızca kanunlar tarafından sağlanan ve başkalarının haklarına veya itibarlarına saygı duyulması için ulusal güvenliği, kamu düzeni, kamu sağlığı, ahlakın korunması için gereklidir (Franklin, Bodle, Hawtin, 2014: 16).

Ulusal strateji belgelerinde yapılan siber güvenlik tanımlarında bilgi, bilişim ve ağların güvenliğinden bahsedilmektedir. Oysa siber alanın en önemli bileşeni kullanıcı olmaktadır. Ancak stratejilerde yapılan tanımlamalarda kullanıcı genel olarak göz ardı edilmektedir. Bilgi ve İletişim Teknolojisinde sürekli olarak kullanıcı yani insan en önemli bileşen olarak vurgulanmasına karşın, güvenlik tartışmalarında bu unsur göz ardı edilmeye devam etmektedir. Bundan dolayı kimin için güvenlik ya da ne için güvenlik sorusu büyük önem arz etmektedir.

Siber uzayın paydaşları kişiler, şirketler ve devletlerdir. Bütün paydaşların istek ve taleplerinin dikkate alındığı böyle bir strateji ile ancak siber güvenlik sağlanabilir.

Günümüzde Bilgi ve İletişim Teknolojisi'nde yaşanan hızlı gelişmeler yeni fırsatlar sunarken bir yandan da tehditlere karşı savunmasız kılmaktadır. Hukuki açıdan yaşanan bazı boşlukları da ortaya çıkarmaktadır. Yasal boşlukların bulunması, yasalardaki yetersizlikler yani bir ülkede tehdit ve suç unsuru sayılabilen bir fiilin, bir başka ülkede tehdit veya suç unsuru sayılmaması ve söz konusu fiile ilişkin herhangi bir mevzuatın bulunmaması siber saldırganlar için o ülkede güvenli sığınaklar oluşturmaktadır. Dünyada internet kullanımı arttıkça mağdurları ve suçluları tespit etmek zorlaşmakta, delil toplama gibi temel soruşturma aşamaları değişmese de bu aşamalarda kullanılan usule ilişkin mevzuatın yetersizliğini ortaya çıkarmaktadır. Siber saldırıları nasıl önlemek gerektiğine ve delillerin nasıl toplanıp değerlendirileceğine karar verilebilmesi için ülkeler arasında izlenecek bir işbirliği ile usule ilişkin mevzuata ihtiyaç duyulmaktadır (Ünver, Canbay ve Mirzaoğlu, 2009: 27). Sanal dünyanın sınır tanımayan küresel yapısı gereği, siber ortamda yargılama yetkileri, insan hakları, uluslararası hukuk, yaşama ve kişilik özgürlüğü gibi hukuki kavramların belirsizliğini beraberinde getirmiştir. Oysa gerçek dünyada, her ülkenin yargılama yetkisi dâhilinde olan bölge coğrafi sınırlarla belirlenmiş ve uluslararası işbirliği içerisinde uygulanan çoğu hukuki yetkileri de belirlemiştir. Sanal dünyada suçu oluşturan eylemleri hangi adli makamın soruşturacağı ve cezalandıracağı hususunda belirsizlik ve karmaşa halen yaşanmaktadır (Ünver, Canbay ve Mirzaoğlu, 2009: 28).

Ulusal siber güvenlik strateji belgesinin yasal boyutunda yaşanan güçlüklerin azaltılması, soruşturma ve kovuşturmanın etkin rol üstlenebilmesi için yapılması gereken çalışmalarda tedbirlerin alınması gerekir. Bundan dolayı; Yasal boşluklar giderilmelidir. Usule ilişkin yasal eksiklikler ortadan kaldırılmalıdır. Siber ortamda koruma ve gözetme yetkileri belirlenmelidir. Sanal dünyada bireyin haklarını sınırlayan her türlü fiile ilişkin, ulus-devletler arasında insan hakları kavramı üzerine değinilmesi ve ortak bir mevzuatın çıkarılmasını gerekli kılmaktadır. Ülkeler arasında siber suça iştirak eden saldırganların iadesine ilişkin uzlaşma usulleri belirlenmelidir. Siber alanda yargılama yetkileri belirlenmelidir (Ünver, Canbay ve Mirzaoğlu, 2009: 30).

Sonuç

Siber uzayın mevcudiyeti ve siber ortamdaki verilerin bütünlüğü, gizliliği ve erişilebilirliği 21. yüzyılın can alıcı soruları haline gelmiştir. Siber güvenliğin sağlanması hem ulusal hem de uluslararası düzeyde devlet, iş dünyası ve toplum için önemli bir hal almıştır. Siber Güvenlik Stratejisi, bu alandaki çerçeve koşullarını iyileştirmek için hazırlanan bir belge olmuştur. Günümüze kadar oluşan gelişmeler de sınırlarının nerede başlayıp nerede bittiğini bilemediğimiz siber alanın getirdiği faydaların günbegün artması ile beraber, güvenlik açısından sorunların sayısı da artmıştır.

Siber alanın gelişen ortamı henüz uluslararası sistem ve hukukun bütünüyle kapsayabildiği bir alan değildir. Birçok ülkeler "ulusal" siber stratejiler oluşturmaya çalışmaktadırlar. Ülkelerin kendine yönelik bir saldırı olduğunda interneti kapatma çabaları, kapalı internet oluşturma gayretleri sınırların belirlenememesinde olumsuz bir durum yaşatmaktadır. Aktörlerin belirsiz olması ve siber alanın hızı ulus-devletleri internet karşısında güçsüz bırakmaktadır. Siber tehditlerin niteliğini anlamak, alınacak önlemlerin tutarlılığını artıracaktır.

Ulus-devletler siber alanın büyük önem taşıdığının daha yeni farkına varmış ve bunun için siber alanı ulusal güvenlik stratejilerine eklemişlerdir. Sınırları belli olmayan bir alan için ulusal strateji belgesi ve eylem planı belirlemek tek başına yeterli olmamaktadır. Dolayısıyla orantılı güç kullanımı olmalı ve ülkelerin işbirliği içerisinde siber alanda ortak bir yargılama yetkisi belirlenmelidir.

Devlet merkezli uluslararası sistemin siber düzeyde çok az uygulanabilir olduğu söylenebilir. Bu nedenle, ulus-devletlerde, bireylerde ve özel şirketlerde de bağlayıcı nitelikte uluslararası bir düzen ve uluslararası hukuka ihtiyaç duyulmaktadır. Siber aktörler üzerinde bağlayıcı yasal düzenlemeler yapmak da, bu yeni alanda insan haklarının geliştirilmesi ve korunması için yeterli değildir. Ancak küresel düzeyde de uygulanmasını gerekli kılmaktadır. Dolayısıyla, anarşik uluslararası düzenin ötesine geçen küresel bir uygulama organına ihtiyaç duyulmaktadır. Ama nasıl olması gerekir? Daha da önemlisi, yeni toplumsal sözleşme ne olmalıdır? Bu sorunun cevabı muhtemelen insan haklarının ve siber güvenliğin geleceğini belirleyecektir.

Siber dünyada devletlerin, kurumların, bireyin güvenliği ve özgürlüğü sağlanmadan, ulusal güvenlik muhtemel değildir. Siber alanda interneti tamamen kapatmak bir güvenlik önlemi değildir. Siberi güvenlikte erişilebilirlik, bütünlük ve gizlilik amaç olmalıdır. Erişimin

kesilmesi, siber güvenliğin mümkün olmaması, insan hak ve özgürlüklerin kısıtlanması anlamına gelmektedir. İnsan hak ve özgürlüklerinin korunmasını temel dayanak noktası almayan hiçbir siber güvenlik önlemi, gerçek anlamda bir güvenlik sağlayamamaktadır.

Bilgi ve İletişim Teknolojisi'nin getirdiği özgürlük ortamının genişlemesi ulus-devletlerin olayların kontrolden çıkabileceği bir medyanın var olduğu hissiyatını vermektedir. Bu durumda ulus-devletler internet üzerinden bireysel hak ve özgürlükleri ihlal edecek şekilde insanları izlemeye başlamışlardır. Fakat bunu fark eden bireylerin (*hacker*lar gibi) önderliğinde muhalefet grupları da oluşmaya başlamaktadır. Ulus-devletlerin kontrolü arttıkça buna karşı oluşan saldırganların sayısı da artmaktadır. Ortaya çıkan çatışma ise siber güvensizliği arttırmakta ve siber çatışma ihtimalini sık sık gündeme getirmektedir.

Günümüzde siber tehdidin belirsizliği veya imkânsızlığı haline bakılmaksızın genişleyen siber güvensizlik alanı ve onun ekonomisi, varlıklarını anlamlandırmak için çatışmayı teşvik eder hale gelmeye başlayabilir. Böyle bir sürece engel olmak siber güvenlik ve uluslararası hukuk için atılacak en büyük adım çatışmayı önlemek olacaktır. Günümüz güvenlik algılarının ve insan hak ve özgürlüklere uygunluğu açısından bu denli değişimlere ihtiyacı vardır. Ulus-devletlerin siber alanın oluşturduğu sanal gerçekliği detaylı incelemesi ve buna uyumlu strateji belgeleri oluşturmaları zorunlu kılmaktadır. Bu süreç tam anlamıyla gerçekleşinceye kadar siber güvenliğin sağlanması ve insan haklarının korunması kolay olmamaktadır. İnsan haklarının siber alanda açık bir şekilde güvenliğe ilişkin zafiyeti bulunmaktadır. Uluslararası hukuk kurallarının siber güvenliğin sağlanmasında yaptırımı olabilir mi? veya ulus-devletler kendi güvenliklerini uluslararası hukuk sayesinde sağlayabilirler mi? insan hakları kavramında aklımıza gelen başlıca sorulardır. Güvenliğin sağlanabilmesi için bütün aktörlerin karar alma mekanizmalarında olması gerekir. Siber güvenlik ve iyi korunan insan haklarına sahip olmak için yeni bir (sosyal) sözleşmeye ihtiyaç duyulabilir.

KAYNAKÇA

Akyeşilmen, Nezir. (2016). *Siber Güvenlik ve Özgürlük.*http://www.ilksesgazetesi.com/yazar/siber-guvenlik-ve-ozgurluk-3816.html [Erişim Tarihi: 13.12.2017].

Akyeşilmen, Nezir. (2016). *Cybersecurity And Human Rights: Need For A Paradigm Shift.? Cyberpolitik Journal*, Siber Politikalar Dergisi, Volume1, Number 1&2 Winter 2016, ss.38-61.

Alagöz Akçadağ, Emine. (15 Şubat 2015).Amerika'nın Yeni Güvenlik Stratejisi. http://www.bilgesam.org/incele/2032/-amerika-nin-yeni-guvenlik-stratejisi/#.WjP97VVl-00 [Erişim Tarihi: 14.12.2017].

Aytar, Ahmet K. (2015). ABD Ulusal Güvenlik Strateji Belgesi ve Türkiye. http://www.turkishnews.com/tr/content/2015/02/16/abd-ulusal-guvenlik-strateji-belgesi-ve-turkiye/ [Erişim Tarihi: 15.12.2017].

Bayraktar, Gökhan. (2015). *Siber Savaş ve Ulusal Güvenlik Stratejisi*, İstanbul: Yeniyüzyıl Yayınevi.

Bıçakçı, Salih. (2013). *21. Yüzyılda Siber Güvenlik* Editör: Mustafa Aydın, İstanbul: İstanbul Bilgi Üniversitesi Yayınları.

Bıçakçı, Salih. (2012) . *Savaş ve Siber Güvenlik Arasında NATO'nun Yeniden Doğuşu.* Uluslararası İlişkiler Dergisi, Cilt 9 (34).

Bozdemir, Nazlı. (21 Temmuz 2013). Türkiye ve Siber Güvenlik Tehditlerin Farkında mıyız?. http://akademikperspektif.com/2013/07/21/turkiye-ve-siber-guvenlik-tehditlerin-farkinda-miyiz-3/[Erişim Tarihi: 14.12.2017].

Craigen, Dan, Diakun-Thibault, Nadia, Purse, Randy. Defining Cybersecurity, https://timreview.ca/article/835 [Erişim Tarihi: 14.12.2017].

Cyber Security Strategy Documents. https://ccdcoe.org/cyber-security-strategy-documents.html [Erişim Tarihi: 14.12.2017].

Dağı, İhsan D. (2010). Normatif Yaklaşımlar: Adalet, Eşitlik ve İnsan Hakları. *Devlet, Sistem ve Kimlik, Uluslararası İlişkilerde Temel Yaklaşımlar*. (12. Baskı).İstanbul: İletişim Yayınları, s.185-227.

Dünya. (17 Temmuz 2012) .Siber Güvenlik Stratejisi Hazır. https://www.dunya.com/gundem/siber-guvenlik-stratejisi-hazir-haberi-179657 [Erişim Tarihi: 12.12.2017].

Franklin, Marianne, Bodle, Robert, Dixie, Hawtin. (August 2014).*The Charter Of Human Rights And Principles For The Internet*, United Nations, 4th Edition
http://www.ohchr.org/Documents/Issues/Opinion/Communications/InternetPrinciplesAndRightsCoalition.pdf [Erişim Tarihi: 20.12.2017].

Geers, Kenneth. (2011). Strategic Cyber Security.*NATO Cooperative Cyber Defence Centre Of Excellence Talinn, Estonia: CCD COE Publication*.

German. (01.01.2011) .National Cyber Security Strategy. https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/strategies/cyber-security-strategy-for-germany/view [Erişim Tarihi: 28.12.2017].

German. (2016). *National security and defence strategies*. On German Security Policy And The Future Of The Bundeswehr, The Federal Government, White Paper.

National Cyber Security Centre. https://www.ncsc.gov.uk/articles/academic-centres-excellence-cyber-security-research [Erişim Tarihi: 14.12.2017].

İngiltere. (2010) .A Strong Britain In An Age Of Uncertainty: The National Security Strategy. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/61936/national-security-strategy.pdf [Erişim Tarihi: 17.12.2017].

İngiltere. (2011) .*The UK Cyber Security Strategy*.http://www.cabinetoffice.gov.uk/sites/default/files/resources/uk-cyber-security-strategy-final.pdf [Erişim Tarihi: 13.12.2017].

İngiltere. (2016). *UK National Cyber Security Strategy*.https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf [Erişim Tarihi: 13.12.2017].

Kaska, Kadri. (2015)Netherlands, *National Cyber Security Organization*.https://ccdcoe.org/ites/efault/files/multimedia/pdf/CS_organisation_NETHERLANDS_032015_0.pdf [Erişim Tarihi: 14.12.2017].

Klimburg, Alexander (Edited By). (2012) *National Cybersecurity Framework Manual, NATO* https://ccdcoe.org/publications/books/NationalCyberSecurityFrameworkManual.pdf [Erişim Tarihi:17.12.2017].

Netherlands. (2011-2013) *The Netherlands Cyber Security Strategy*. https://english.nctv.nl/inaries/cyber-security-strategy-uk_tcm32-83648.pdf [Erişim Tarihi: 15.12.2017].

Netherlands. (2014-2016) .*The Netherlands Cyber Security Strategy 2*.https://www.enisa.uropa.uopics/national-cyber-security-strategies/ncss-map/NCSS2Engelseversie.pdf [Erişim Tarihi: 14.12.2017].

Sarı, Arif. *Gelişmiş Ülkelerde Ulusal Siber Güvenlik Duvarı Projeleri* http://www.cezerisga.com/makale/Gelişmiş%20Ülkelerde%20Ulusal%20Siber%20Güvenlik%20Duvarı%20Projeleri [Erişim Tarihi: 15.12.2017].

Strat, Acos (Edited By), CHOD (Approved By). (2014).Belgium. *Cybersecurity Strategy For Defence*https://ccdcoe.org/sites/default/files/strategy/Belgian%20Defence%20Cyber%20Security%20Strategy.pdf [Erişim Tarihi: 17.12.2017].

Thomas, T. L. (2003).Al Qaeda and the Internet: The Danger of Cyberplanning. *Parameters*, Cilt 33 (1), ss.114-122.

Türkiye. (2016-2019.).lusal Siber Güvenlik Strateji Belgesi. http://www.udhb.gov.tr/oc/siberg/2016-2019guvenlik.pdf [Erişim Tarihi: 12.12.2017].

TÜBİTAK ve BTK. (2011).*I. Ulusal Siber Güvenlik Tatbikatı Sonuç Raporu* http://www.uekae.tubitak.gov.tr/uekae_content_files/siber_tatbikat_raporları/USGT_2011_tr.pdf [Erişim Tarihi: 15.12.2017].

Türkiye. (Haziran 2012). *Ulusal Siber Güvenlik Stratejisi.* http://www.bilgiguvenligi.org.tr/wp-content/uploads/2016/03/Ulusal_Siber_Guvenlik_Stratejisi.pdf [Erişim Tarihi: 15.12.2017].

Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi. (2012).Yönetilmesi ve Koordinasyonuna İlişkin Karar.http://www.resmigazete.gov.tr/eskiler/2012/10/20121020-18-1.pdf [Erişim Tarihi: 15.12.2017].

USA. (2009). *Cyberspace Police Review*. https://www.dhs.gov/sites/default/iles/publications/Cyberspace_Policy_Review_final_0.pdf [Erişim Tarihi: 17.12.2017].

USA. (April 2015).The DoD Cyber Strategy The Department of Defense https://www.defense.ov/ortals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_YBER_STRATEGY_for_web.pdf [Erişim Tarihi: 17.12.2017].

USA. (December 2017).*ational Security Strategy Of The United States Of America* https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf [Erişim Tarihi: 28.12.2017].

Ünver, M., Canbay, C., Mirzaoğlu, A.G. (2009).*Siber Güvenliğin Sağlanması: Türkiye'deki Mevcut Durum ve Alınması Gereken Tedbirler*. Bilgi Teknolojileri Üst Kurulu http://www.cybersecurity.gov.tr/publications/sg.pdf [Erişim Tarihi: 14.12.2017].

Ünver, M., Canbay, C., Özkan, H.B. (Mayıs 2010).ritik Altyapıların Korunması, Bilgi Teknolojileri Koordinasyon Dairesi Başkanlığı. https://www.btk.gov.tr/File/?path=OOT%2F1%2FDocuments%2FSayfalar%2FSiberGuvenlik%2FCIP_Rapor.pdf [Erişim Tarihi: 14.12.2017].

Yüksel, Mahir.(2017).k Siber Güvenlik Eylem Planı. http://www.yenisoz.com.tr/3-yillik-siber-guvenlik-eylem-plani-makale-15972 [Erişim Tarihi: 15.12.2017].