# DEVLETLERİN SINIR GÜVENLİĞİNİN SİBER AÇIDAN DEĞERLENDİRİLMESİ

**Ayşegül GÜLER***

***Özet***

İnternet, hayatı önemli oranda kolaylaştırması yanında tehdit algılamalarında da dönüşümlere yol açmıştır. İletişimde ortaya çıkan gelişmeler devlet sınırlarını ve ulusal kanunları anlamsız hale getirmiştir. Günümüzde yaygınlaşan terör faaliyetleri arasında ayrı bir alan oluşturan siber saldırılar insanlığın yeri ve zamanı belli olmayan topyekûn bir saldırıyla karşı karşıya kalmasına neden olmuştur. İnternet, klasik zaman ve mekân kavramlarıyla ifade edilemeyen mesafeleri saniyeler içinde ortadan kaldırıp, çok uzak bölgelerdeki insanların birbiriyle konuşup mesajlaşmasına imkân vermektedir. Kurumlarla kişileri mekâna ihtiyaç kalmadan aynı sahada buluşturmaktadır. İnsanların tepkilerini anında duyurmasını sağlayan internette bilgiler denetimsiz olarak yayılmakta, müdahale haber yayıldıktan sonra gündeme gelebilmektedir. Sanal dünya hızla hayatı kuşatırken yöneticisi ve sahibi belirsizdir. Kendisini yönetmek amacıyla oluşturulan kurumlar kapasite açısından gelişmelere ayak uyduramamaktadır. Kuralsız ve kontrolsüz olarak gelişen internete yönelik oluşturulmaya çalışılan kurallar hayata geçirilmeden anlamsızlaşabilmektedir. Küreselleşen dünyada insanlara geniş özgürlük alanları açılırken, evrensel değerlerin korunması yönünde kişinin iradesi dışında bir sorumluluk oluşturulamamaktadır. Gelişen teknoloji insan haklarının evrenselleşmesi beklentilerini karşılayamamıştır. Aksine kurumlardaki yapılanmalar her bireyin sağlıktan ekonomiye, temel insan haklarına kadar geniş bir alanda tehdide açık hale gelmesine zemin hazırlamıştır. Devletlerin bilgilerini koruyamaz hale geldiği bir dönemde kişilerin hakları ciddi bir risk altındadır. Değişimin getirdiği belirsizlik ortamında sorunların boyutları ve nasıl aşılacağı konusunda bir formül bulunmamaktadır. Devletlerin siber saldırılara karşı hazırlıksız olduğu, teknolojinin merkezi gözüken devletlerin bile siber saldırılardan korunamadığı bir ortam vardır. Toplumlar karmaşa ortamından kârlı çıkma hesapları yerine ortak akılla insanları tatmin edecek bilgi güvenliğini sağlamaya dönük küresel işbirliğine yönelmeli ve kurallar oluşturulmalıdır.

**Anahtar Kelimeler:** İnternet, Teknoloji, Güvenlik, Sorumluluk

## EVALUATION OF BORDER SECURITY OF STATES WITH A CYBER APPROACH

* Dr.Öğr.Üyesi, Karamanoğlu Mehmetbey Üniversitesi, Siyaset Bilimi ve Uluslararası İlişkiler

***Abstract***

The internet has led to significant improvements in life as well as changes in threat detection. Developments in communication made state boundaries and national laws meaning less. The cyber attacks, which constitute a separate among the terrorist activities that have become wide spread today, have caused humanity to face a total attack that is not clear of its place and time. The internet allows people in remote are as to talk and communicate with each other by eliminating distances that cannot be expressed by classical concepts of time and space in seconds. It brings institutions and people together in the same field without the need for space. Information on the Internet, which allows people to announce their reactions instantly, is spreading unchecked, and the intervention may occur after the news is spread. As the virtual world rapidly surrounds life, its manager and owner are uncertain. The institutions created to manage themselves cannot keep up with the developments in terms of capacity. The rules that are tried to be created for the internet that develops without rules and without control become meaningless without being implemented. In the globalizing world, wide areas of freedom are opened to people, and no responsibility other than the will of the individual can be established for the protection of universal values. On the contrary, the institutions have prepared the basis for each individual to be vulnerable to a wide range of threats from health to economy, to basic human rights. At a time when states can not protect their information, the rights of persons are at a serious risk. There is no formula on the dimensions of the problems environment of uncertainty brought about by the change. There is an environment in which states are unprepared for cyber attacks, and even states that seem to be the center of technology cannot be protected from cyber attacks. Societies should be directed to global cooperation and rules should be established to ensure information security that will satisfy people with common reason rather than making profitable calculations out of chaos.



**Keywords:** Internet, Technology, Security, Responsibility

## Giriş

II. Dünya Savaşı'ndan sonra savaşları sona erdirmek ve kuvvet kullanılmasına sınırlama getirmek amacıyla Birleşmiş Milletler (BM) Antlaşması'yla devletlerin kuvvet kullanarak sınırları değiştirmesi ve içişlerine karışılmasının açık bir şekilde yasaklandığı görülmektedir. BM Antlaşmasının 2/4. maddesi kuvvet yoluyla sınırların değiştirilmesini ve genel anlamda müdahaleleri de içine alacak şekilde kuvvet kullanmayı yasaklamıştır (Bozkurt, 2003: 19).

Güvenlik Konseyinin aksi yönde izni olmadıkça güç kullanımı sadece silahlı saldırıya uğranması halinde savunma amacıyla sınırlıdır (Chomsky, 2008:143). BM Antlaşmasının 2/7. maddesi ise "anlaşmanın hiçbir hükmü, herhangi bir devleti kendi iç yetki alanına giren konularda BM'ye müdahale yetkisi vermemektedir" (Heywood,2013:409). BM Antlaşmasının önemli bir prensibi olan iç işlerine karışmama uygulaması güçlü devletlerin hedef coğrafyalara yönelik müdahalelerinde insani müdahale veya koruma sorumluluğu uygulamalarıyla ortadan kaldırılmaktadır (Sur,2013:2549). BM Anlaşmasının 2/4. maddesinde saldırı şartının hangi durumlarda gerçekleşmiş sayılacağı tartışılmaktadır. Silahlı saldırının fiilen gerçekleşmiş olması mı gerekmektedir? Saldırı ihtimali meşru müdafaayı gerektirir mi? Uluslararası hukukta saldırı ve savunmaya dayanak oluşturan hükümler tamamen devlet kaynaklı fiziki ihlalleri konu alan bir yaklaşımı temsil etmektedir. Günümüzde toplumlar birçok alanda siber teknolojileri hayata geçirmiştir. Devletlere askeri kuvvetlerce yapılacak müdahalelerden daha fazla ve daha geniş etki alanı oluşturan siber müdahalelere, yürürlükteki normlar ayak uyduramamaktadır. Bazı çevreler siber alanda yapılan saldırıların normlarda belirtilen fiziki ihlalleri karşılamadığından saldırı kabul edilemeyeceği ve meşru müdafaa gerekçesinin oluşmayacağını ileri sürmektedirler. Uluslararası hukuk, kaynağı belirsiz saldırılardan devletlerin sorumlu tutulamayacağını ifade etmektedir. Ancak genel kanaate göre devletler hedeflerine bilgisayar korsanları gibi devlet dışı aktörleri doğrudan veya dolaylı destekleyerek ulaşmayı tercih etmektedir. Devletler siber saldırılara hiçbir şekilde müdahil olmasalar bile altyapı imkânlarını kullandırmaları nedeniyle sorumlu tutulabilmelidir. Ayrıca siber alandaki faaliyetler bazı şirketlerin kontrolü altında cereyan etmekte, çoğu zaman şirket politikası gerekçesiyle kendi ülkelerindeki zararlı faaliyetlerin sorumlularının kimliklerini açıklamaktan çekinmektedirler.



1969'da Amerika Savunma Bakanlığı muhtemel tehlikelere karşı haberleşmesini kesintisiz hale getirmek için üniversite işbirliği ile internet sistemini kurmuştur (Eczacıbaşı, 1998:255-256). Başka bir ifadeyle siber alandaki çalışmalar fiziksel saldırılara karşı veri güvenliğini sağlamak amacıyla başlatılmıştır. Siber alandaki gelişmeler aslında 1950-1990 arasında iki kutuplu sistemin liderleri arasında sürdürülen mücadelenin özellikle de askeri rekabetin ortaya çıkardığı internete dayanmaktadır. Kişilerden devlete çok sayıda alanda kullanılan internet kullanıcı sayısı çoğaldıkça güvenlik sorunları da artmıştır (Akyeşilmen, 2018:58-599). Siber gelişmeler dünyadaki statükoyu zorlamakta jeopolitik ve jeostratejik dengeler yeniden oluşmaktadır. Bu değişim barışçıl yollarla gerçekleşme imkanına sahipken barışçıl olmayan yolların devreye gireceği ve kendini hissettireceği düşünülmektedir (Aksu ve diğ., 2011:179).

Çünkü siber alan konusunda ortak mücadele iradesinin oluşmadığı ve devletlerin bu karışık ortamdan yararlanma arzusuyla hareket ettiği varsayılmaktadır.

Uluslararası sistemde henüz paylaşılmamış olan uzayda yer alan uydular çok güçlü haberleşme imkânlarına sahip olduklarından, karadaki mücadelenin uydular üzerinden uzaya taşınmasına yol açmıştır. ABD ve Rusya kendi ülkelerinin üzerinden geçen uyduları kontrol etmek amacıyla çeşitli yöntem arayışı içerisindedirler. Soğuk Savaş'ın sona ermesiyle uzay tabanlı siber savaş alanında ABD rakipsiz süper güç konumuna gelmişse de Rusya'nın oyuna dâhil olması ve yeni aktörlerin ortaya çıkması ABD'nin interneti kendi sanayi ve teknolojik gelişmeleri doğrultusunda kullanması yönünde engeller ortaya çıkarmıştır (Akman, 2003:299). Haberleşme alanındaki bilimsel gelişmeler karada olduğu gibi atmosferde de ciddi tehlikelerin ortaya çıkmasına yol açmıştır (Vester, 1998:61).Uzayda 1957'den beri yer almaya başlayan haberleşmede yeni ufuklar açan uyduların 1/3'ü askeri amaçlıdır. Uydular ABD ve Rusya'nın savunma sistemi içerisinde önemli bir yere sahiptir ve uzayda uyduları yok edecek sistemler üzerinde yoğunlaştıkları düşünülmektedir. ABD 1980'den itibaren belli bir yörüngeye yerleştirilen balon hedefler üzerinde yaptığı denemelerde başarılı olmuştur. Sovyetler Birliği'nin de katil uydu programı üzerinde çalıştığı bilinmektedir. Dünyaya uzaklıkları nedeniyle güvenlikli gözüken bu uyduları avcı uydular kullanılarak on iki saatten kısa bir süre içerisinde lazer saldırı marifetiyle yok edilebileceği ifade edilmektedir. Ekonomiden kültüre, enerjiden savunmaya, sağlıktan eğitime bağımlı hale geldiğimiz iletişim ağlarının işlevlerini yerine getirebilmesi için uyduların işlevsiz hale gelmesiyle dünya telafisi mümkün olmayan zararlarla karşılaşabilecektir. Devletlerin karada birbirlerine üstünlük sağlamak amacıyla ürettikleri füzeler de işlevsiz hale gelecektir (Akman, 2003:288-294). Sanal dünyanın ne yöneteni ne de sahibi vardır denebilir. Sanal dünya günümüzde sihirbazın çırağı usulü kendini yönetmeye çalışan kurumları aşmış durumdadır. Kuralsız ve kontrolsüz gelişen internete kural koymaya kalktığınızda elinizden kayıp gittiği dahi geç fark edilmektedir (Eczacıbaşı, 1998:255-256). Ağlarındaki oluşumun nasıl yapılması gerektiği konusunda herhangi bir kural bulunmayan bilgisayarlar kendilerine verilen girdiler doğrultusunda çıktılar üretmektedir. Bu açıdan programların hangi amaçla oluşturulduğu oldukça önem taşımaktadır. Çünkü bilgisayar sistemleri çok sayıda bilgiyi kısa sürede işleyebilmekte ve yararlı sonuçlar üretebilmektedir (Öztemel, 2016:30-35). Gelişen bilim ve teknoloji doğru ellerde hayat kurtarmakta, istihdam oluşturmakta, insanlığın refahını artıracak değer katacak faydalar oluştururken, yanlış eller tarafından öldürücü silahlara dönüştürülebilmektedir. Kısacası teknoloji kullanan elin niyeti ile yakından alakalıdır (Taptık ve Keleş, 1998:82).

Diğer yandan teknolojik alanda yaşanan talep patlaması ise fiyatların düşmesine ve siber alana katılanların sayısının her geçen gün artmasına neden olmaktadır (Aksu ve diğ., 2011:46). Dünyanın neresinde olursanız olun insanları birbirleriyle konuşturan, aynı sahada buluşturan (Eczacıbaşı, 1998:255-256) internetin kullanıcı sayısı dört milyar üç yüz milyonu geçmiştir. Yapılan araştırmalara göre bugün internete on-on bir milyar cihazın bağlı olduğu tahmin edilirken 2020 yılına gelindiğinde elli milyar cihaz seviyesine çıkması öngörülmektedir. İnternete bağlanan cihazlar atanan İnternet Protokol Adresi (IP) adresi üzerinden iletişim kurmaktadır. İnternet kullanımının yaygınlaşması bilişim altyapısının gelişmelere uygun olarak "bulut bilişim" sisteminin geliştirilmesini gerektirmiştir (Babaoğlan,2008)."Nesnelerin interneti, benzersiz bir şekilde adreslenebilir nesnelerin kendi aralarında oluşturduğu dünya çapında yaygın bir ağ ve bu ağdaki nesnelerin belirli bir protokol ile birbiriyle iletişim içinde olmaları" (Yetimler,50) olarak tanımlanmaktadır. Her şeyin başına akıllı teriminin getirildiği dünyamızda cihazların birbiriyle bağlantıları sisteme dışarıdan müdahale imkânını artırmaktadır.

Fiber optik kablolar ise sınır sınırlamasını ortadan kaldırarak ülkeler arasında ticaret ve bilgi alışverişini sıradanlaştırmıştır. Geldiğimiz süreçte ulus devletin oynadığı rol uluslararası yapıların denetimi altına girmektedir (Akman, 2003:346-355). Konvansiyonel alanda olduğu gibi siber alanda da güvenlik toplumların en önemli sorunlarından biri olmaya devam etmektedir. Siber alandaki tehditlerin zamanı ve hedefi önceden bilinemediğinden tedbir almak imkânsız gibidir (Akyeşilmen, 2018:13-14). Siber dünya fiziksel sınırların olmadığı bir alana dönüşmüş klasik zaman ve mekân kavramları içinde bulunulan durumu tanımlamakta yetersiz kalmıştır. İletişimde ortaya çıkan gelişmeler devlet sınırlarını ve ulusal kanunları anlamsız hale getirmiştir. İnternet, klasik zaman ve mekân kavramlarıyla ifade edilemeyen mesafeleri saniyeler içinde ortadan kaldırıp, hedefe ulaşılmasına imkân tanımaktadır. Geleceğe dönük planların hayata geçirilmesinde öncelikle tehditlerin asgari seviyeye indirilmesi için gerekli çalışmaların yapılması gerekmektedir.



**Siber Saldırı Yöntemleri**

İnternet ABD'nin güvenli veri oluşturma amacıyla ortaya çıkan bir gelişme olmasına rağmen anarşik yapısı, kullanıcı sayısının kontrol edilememesi nedeniyle ABD'nin sahip olduğu imkânlara rağmen denetiminin dışına çıkmıştır (Akyeşilmen, 2018:270). Siber alandaki gelişmeler insanlığı heyecanlandırırken ciddi "siber endişe" yaşanmasını da beraberinde

getirmektedir (Akın,2016:579). **Bilgisayar sistemleri**, **ağ sistemleri** ya da diğer **siber sistemlerine izinsiz sızma** işlemi yapabilen kişiler genel olarak hacker olarak tanımlanmaktadır ve hackerların birbirlerine üstünlükleri bilgi seviyeleridir. Siber güvenlik alanında hack, açıklık bularak bunu kendi menfaatine kullanmak demektir (Kamış, 2019). Çeşitli endüstrilerdeki elektronik hizmetler ve operasyonlardaki artış, tehditlerin, zararlı faaliyetlerin sayısı ve türünde artışa neden olmuştur. Altyapıları hedef alan güvenlik tehditleri, kötü amaçlı yazılım faaliyetlerinin büyümesi ve saldırıların yaygınlaşmasına neden olmuştur (Abouzakhar ve diğ., 2017). Siber saldırılar daha ziyade küresel boyutta operasyonlar olarak kendisini gösterdiğinden savunma önlemlerinde zorluklar yaşanmaktadır (Akyeşilmen, 2018:223). Hem kablolu hem de kablosuz olabilen ağ katmanı, çeşitli saldırılara maruz kalmaktadır. Kablosuz kanalların açık olmasından dolayı, haberleşmeler bazı bilgisayar korsanları tarafından kolayca izlenebilmektedir. Servis Hizmet Reddi(DoS) saldırısı, sahte bilgilerin Radyo Frekansı ile Tanımlama (RFID) sistemlerine yayınlaması, hedef odaklı oltalama saldırısı, malware yazılımı sıkça karşılaşılan saldırı yöntemleridir (Farooq ve diğ., 2015). Fidye yazılımlarının en yaygın olarak kullanıldığı yerlere bakıldığında, en fazla etkilenen ilk üç ülkenin Kazakistan, Rusya ve Ukrayna olduğu görülmektedir. Ancak ABD'deki kullanıcılar en çok, kötü şöhretli Cryptowall fidye yazılımı Cryptodef ile hedef olmaktadır. Örneğin, ABD'de Rusya'nın üç katı virüs saldırısı gerçekleşmiştir. Cryptowall, kullanıcının sıkıştırılmış bir JavaScript aldığı istenmeyen e-postalar yoluyla yayılmaktadır. JavaScript yürütüldüğünde Cryptowall'u indirip dosyaları şifrelemeye başlamaktadır (Medikal Akademi, 2016). Nesnelerin İnterneti (IoT) yaygınlaştıkça güvenlik önlemlerine yönelik tehdidin boyutu da artmaktadır (Fu ve diğ., 2017). İnternetin devreye girmesiyle veri güvenliğinin önemi artmıştır. Önceki dönemlerde verilerin bozulması söz konusuyken internetin yaygınlaşmasıyla birlikte verilerin başkalarınca kullanılması, kopyalanması gibi konular ön plana çıkmıştır. Veri güvenliğinin kapsamı bilgilerin izinsiz kullanımı, açıklanması, yok edilmesi, değiştirilmesi, bilgilere hasar verilmesi, izinsiz erişimlere kadar geniş bir alandır (Veri Güvenliği,56).



**Kişi ve Kurumlara Yönelik Saldırılar**

Günümüzde yüksek teknoloji kullanımı modern toplumların vazgeçilmezi olurken yeni fırsatlarla eşzamanlı ciddi riskler gündeme gelmektedir. Siber saldırılar genellikle para, veri veya teknolojik fikirleri çalma amacı taşımakla birlikte giderek, uluslararası ve devlet destekli hale gelerek gittikçe artan bir şekilde ülkelerin iç politikalarını etkilemeye yönelik faaliyetlere dönüşmüştür (Martin ve diğ., 2017). Gerek kişiler gerekse devletler faaliyetlerinin büyük bir

bölümünü siber alana taşımıştır. Siber faaliyetler sadece yazılım dünyasının ilgi alanı olmayıp devletlerin kendi aralarında yürüttükleri mücadelenin önemli bir aracı haline gelmiştir (Akyeşilmen, 2018:13-15). Haberleşmenin güvenlik içinde yararlı olma niteliğindeki sınırlandırmalar toplumun büyük bir bölümünce dikkate alınmamaktadır. Siber alandaki bilgiler kolaylıkla korunamayan bir görünüm arz etmektedir (Wiener, 1975:163-167). Karşılaşılan problemlerin nedenini anlamadan yapılan mücadele çoğu kez başarıya ulaşmamaktadır (Vester, 1998:108). Hackerlar bu sistemleri elde edince toplumda karışıklığa neden olabilmekte ve zararlı yazılımlar yoluyla oluşan tehlikeler uzun süre fark edilmeden tahribat yapmaya devam etmektedir.

Dijital dünya mahremiyet kavramlarını hızla değiştirmeye başlamış, mahrem değerler kamuya açık hale gelmek zorunda bırakılmıştır (BTSGD, 2019). ABD'nin Mississippi eyaletinde bir hacker, çocukların odasına güvenlik için yerleştirilen kamerayı ele geçirerek sekiz yaşındaki kız çocuğuyla konuşmaya çalışmıştır (TRTAvaz). Aynı eyalette üç genç kızın yatak odasına yerleştirilen dünya devi bir şirkete ait ev içi güvenlik kamerasının kurulumundan dört gün sonra bir hacker tarafından ele geçirildiği anlaşılmıştır (Memleket, 2019). ABD'de güvenlik araştırmacısı Bob Diachenko iki yüz altmış yedi milyondan fazla Facebook kullanıcısına ait kişisel bilgilerin istismara açık bir şekilde göründüğü, veri tabanının Kısa Mesaj Servisi (SMS) yoluyla oltalama ve spam için kullanılmasının muhtemel olduğunu açıklamıştır. Hatta bu bilgilerin indirilmek üzere hacker formuna gönderildiği düşünülmektedir (Baylançiçek, 2019). Siber alan insanları bireyselleştirirken, bireyler kendi istek ve tercihlerini toplum menfaatlerinin üzerinde görmeye başlamaktadır. İnternet hizmeti sağlayıcıları insanların verilerini şirketlerle paylaşmakta ve ayrı bir ticari alanın oluşmasına neden olmaktadır (Aksu ve diğ., 2011:46-61).



Güvenlik ve gizliliği sağlayacak yeni teknolojilerin geliştirilmesi gerekmektedir (Suoa ve diğ., 2012). IoT, insanların hayatını iyileştirme vaadi beraberinde siber güvensizliği ve potansiyel olarak her yerde güvenlik ve gizliliğe yönelik felaketle sonuçlanan tehlikeleri de beraberinde getirmektedir (Davis, 2017). Siber alan birey seviyesinden başlayıp küresel bir sorun haline gelmiştir. Devletler siber alanı strateji ve askeri politikalarının temel girdilerinden bir alan olarak görmeye başlamıştır. Dünyada her gün elli bin internet sitesi saldırıya maruz kalırken, bilgisayarların % 30'u bu saldırılardan etkilenmektedir. Belirsizlik siber alanda güvensizliği beraberinde getirmekte, saldırılar güvenlik önlemlerinden daha önde

gitmektedir (Akyeşilmen, 2018:118-119). Düşmanlar şekil ve anlam değiştirdiği için bu durum sağlığımızı, hayatımızı, ekonomik yapımızı doğrudan ve dolaylı olarak etkilemektedir. Devletlerin siber alanda sürekli bir rekabet ve çatışma içerisinde oldukları iddiası her geçen gün güçlenmektedir. Siber alan ekonomik ve kültürel boyutu dışında devletlerarasında daha çok askeri ve stratejik boyutuyla tartışılmaktadır (Akyeşilmen, 2018:211-212). Ordular geleceğimiz açısından önemli olan hizmet sahalarıyla ilgili belirli stratejiler ve güvenlik politikaları oluşturmuştur. Artık düşman elimizdeki toprakları denetim altına almak isteyen başka ülkelerin insanları olarak karşımıza çıkmamakta aynı zamanda maddesel ve yapısal fenomenlere bağlı tehlikeleri de bünyesinde barındıran oluşumlar olarak karşımıza çıkmaktadır. Bu yeni tehlike dünyadaki toplumları potansiyel olmaktan öte gerçek bir şekilde tehdit etmektedir (Vester, 1998:63-64). İleri teknolojiye dayalı üretim gerçekleştiren devletler, uluslararası sistemi kendi çıkarları doğrultusunda düzenleyen hegemon güç olma gayreti içerisine girmektedir (Ayhan,2006:72). Gelişmiş ülkelerin askerleri, bürokratları, bilim adamları güçsüz ülkelerce yapılan uyarıları kibirli bir tavırla dikkate almamaktadır (Forbes, 2009:75). İnternet bireylerin haberleşip toplu hareket edebilmesine olanak sağlamaktadır. İran'da yetkililerin yabancı ajanların etkin olduğunu ifade ettiği benzin zammını protesto etmek amacıyla yüzden fazla şehirde önü alınamayan gösteriler başlamış, İran göstericilerin sosyal medya üzerinden haberleşmesini engellemek amacıyla internete erişimi kesmiştir (BBC, 2019). Erişim yasağı katılımları azaltmazken, bankacılık ve ulaşım sektörü başta olmak üzere büyük ekonomik kayıplar yaşanmıştır (Anadolu Ajansı, 2019). Bir ülkede yatırımı bulunan veya yatırım kararı alan küresel şirketler faaliyette bulundukları ülkelerin siyasi yapısını siber imkanları da kullanarak ekonomik çıkarları doğrultusunda etkilemeyi amaçlamaktadır (Ayhan, 2006:40). Dünyadaki ülkelerin büyük bir bölümü siber saldırıların hedefi konumunda iken Almanya, Çin, ABD ve Rusya siber istihbarat konusunda hem kaynak hem hedef ülke konumundadır (Akyeşilmen, 2018:231-236). ABD ve Rusya'nın dünyayı elinde tutma yarışı iletişim alanında hırsız polis oyununu girift hale getirmiştir (Wiener, 1975:158).



Yeni kavramlardan olan siber savaş kavramı, ülkelerin artık siber güvenlik alanına yönelmesi ve siber ordularını oluşturmasıyla güvenli hale gelinmesidir. Siber savaş ile ülke ekonomisine büyük zarar verip ülkenin elektriklerini kesebilme gibi zarar verici yıkıcı saldırılar mümkündür (Kamış 2019). Siber saldırıların henüz fiziksel yıkım boyutunun sınırlı olması ortaya koyabileceği etkilerin ve etki alanının anlaşılamamış olması siber suç kavramının tanımlanmasını zorlaştırmaktadır. Siber suç genel anlamda bilgisayarlar aracılığıyla

oluşturulan verilerin yasadışı amaçlarla kullanılması ve bilgisayarların hedef alınması eylemi olarak tanımlanmaktadır (Akyeşilmen, 2018:94-97). Daha önce Türkiye'de resmi kurumlara ait siteleri hackleyen Anonymous, bu kez daha ciddi ve sonuçları ağır bir saldırıya imza atmıştır. Siber korsanlar, şifreleme sistemini çözüp hastanenin elektronik haberleşme imkânlarını ele geçirmiştir. Bu yüzden hastane yönetimi iletişimde kağıt-kalem, telefon-faks gibi geleneksel yöntemlere dönüş yapmak zorunda kalmıştır (Medikal Akademi, 2016).

Sanal alemde herkesin güvenlik öncelikli bir yaklaşımı beraberinde bireysel özgürlüklerin sınırlandırılmasını getirmektedir. Ekim 2010 tarihinde Wikileaks'in dört yüz bin gizli belgeyi kamuoyunun bilgisine açması devletlerin gizli bilgilerinin de saldırıya ne kadar açık olduğunu ortaya koymuştur. Bu gelişme diplomasinin 11 Eylül'ü olarak algılanmıştır (Aksu ve diğ., 2011:65-71). Güvenlik seviyesi düşük olan çevre alanlardaki bir hedefe saldırı düzenlemek sureti ile istenilen etki ve tahribat devletler üzerinde oluşturulabilir. Örneğin Türkiye'de yapımı devam etmekte olan nükleer santrale yönelik algı operasyonlarını güçlendirmek için Çernobil sürekli gündeme taşınmaktadır. Komşumuz Ermenistan'da teknolojisi Çernobil'den daha geri olan ekonomik nedenlerle bakımının da tam yapılamadığı düşünülen nükleer santrale karşı gerçekleşecek bir siber saldırı Türkiye'nin yarısını etkileyebilecek bir tehdit potansiyeline sahiptir.



Her geçen gün artan internet destekli araçların işlevlerini doğru olarak yerine getirebilmesi için güvenliklerinin sağlanması oldukça güçleşmektedir. Yazılımın reklamdan para kazandırdığı model, cihaz düzeyinde uygulanmaktadır. Toplanan verilerin güvenliğinin ne kadar sağlandığının kullanıcılar tarafından bilinmesi gerekmektedir. Telefon uygulamalarıyla toplanan bilgilerin kişilerin bilgisi dışında şirketlerce satıldığı bilinmektedir (Fu ve diğ., 2017). Saldırganlar çok uzaklardan saldırabilmekte, üstelik bunu anonim olarak ve ışık hızıyla yapabilmektedir, mobil aygıtlar hızla yaygınlaşmakta ve hatta geleneksel kişisel bilgisayarların önüne geçmektedir. Dünya çapındaki internet kullanıcılarının sayısındaki artış nedeniyle bu kullanıcılar yeni güvenlik açıklarına yol açabilmektedir (Siber Güvenlik Nedir ?). Özetle internet, hayatı önemli oranda kolaylaştırması yanında tehdit algılamalarında da dönüşümlere yol açmıştır. Bilgisayar ve internet işlemleri hayatımızın her alanına nüfuz etmiş, yeni nesiller interneti hayatın temel şartlarından biri olarak görmeye başlamıştır. İnternet insanların günlük hayatlarında da en temel faaliyet alanlarından biri haline gelmiştir. Ancak ciddi kolaylıklar ve ekonomik avantajlar sağlamakla birlikte beraberinde taşıdığı dezavantajlarıyla da düşündüren bir alan haline gelmiştir (Karakaş, 2016:7-9). Siber alanda

saklanan bilgilerin dışarıdan müdahale yoluyla kötü niyetli kişilerin eline geçme potansiyeli dikkat edilmesi gereken bir konudur (Abouzakhar ve diğ., 2017).

**Siber Güvenlik**

İnsanlar bilinen ilk dönemden beri bilgi ve belgelerin korunmasına dönük çalışmalar yapmış, sosyal bilimciler, filozoflar bu konuda açılımlar yapmaya çalışmıştır. Günümüzde klasik yöntemler yerine bilgiler bulut uygulamasının devreye girmesiyle sanal ortamda depolanmaya başlamıştır. Bilgi teknolojileri insanların oturduğu yerden başka ülkeler hakkında daha fazla bilgi sahibi olmasına imkân sağlarken müdahale etmesine de zemin hazırlamaktadır.

Günümüzde bilgisayar sistemleri hayatımızın vazgeçilmez bir bölümü haline gelmiştir. Askeri sistemler de ağırlıklı olarak bilgisayardan yararlanmaya başlamıştır. Ortaya çıkan gelişmeler bilgisayarları büyük miktardaki bilgileri özetleyebilen mevcut bilgilerden hareketle strateji oluşturabilen bir niteliğe taşımıştır (Öztemel, 2016:13). Tarihin hiçbir döneminde günümüzde olduğu gibi dünyayla ilgili bu kadar bilgi bir araya getirilememiştir. Geniş bilgi potansiyeline rağmen beklenmeyen şaşırtıcı problemler giderek daha fazla ortaya çıkmaktadır. İnsanların ortaya koyduğu medeniyet içinde her gün alışılmamış yeni durumlar görülmeye başlanmıştır (Vester, 1998:103). Bilgisayar ağları üzerinden aktarılan bilgiler devasa boyutlarda olup uluslararası bilgisayar ağlarını kullanmaktadır. Bu yoğunluk, suç işlemeyi belirsizlikleri nedeniyle teşvik etmekte her gün milyonlarca suç işlenmekte, insanlar zarar görmekte, saldırganlar tespit edilememektedir (Akyeşilmen, 2018:88). Siber güvenlik, siber alandaki hayatın güvenlik ve gizliliğinin korunmasıdır. “Yakın gelecekte çıkabilecek büyük bir savaşta ilk mermi internette atılacaktır” (RexHughes). Siber güvenlik yalnızca verileri korumakla ilgili değildir. İyi güvenlik, verileri korumaktan daha fazlasını ifade etmektedir. Tüm ilgili yamaların, güncellemelerin düzenli olarak yapılmasına rağmen siber güvenlik hiçbir zaman% 100 etkili olamaz (Martin ve diğ., 2017). Siber alanda hiçbir kullanıcı tam olarak güvende değildir çünkü kullanıcıların sayısı arttıkça hedef haline gelme ihtimali de artmaktadır (Akyeşilmen, 2018:107).

Üzerinde çalışılan siber güvenlik stratejileri öncelikli olarak devlet güvenliğini amaçlamaktadır. Siber saldırılarda devlet sınırları yoktur. Siber alanda verilere uzaktan ulaşım ve değiştirme imkânı bulunduğundan beklenmedik sonuçların ortaya çıkması her zaman mümkündür (Akyeşilmen, 2018:108-113). Sanal ortamda saklanan kişilere ve kurumlara ait bilgilerin korunması saldırılardan zarar görmemesi sanal ortamdaki güvenliğin amacını oluşturmaktadır (Sır,2017). Gerçekleştirilen her siber saldırının bir şekilde devletlerle

bağlantısı vardır. En azından saldırganlar devletlerin oluşturduğu alt yapıyı kullanmaktadır. Bazı devletler doğrudan siber saldırıyı kurumsal olarak planlarken bazıları devlet dışı aktörler üzerinden vekâlet savaşı sürdürmeyi tercih etmektedir. Her nedense saldırıları kurumsal veya kişisel olarak hiç kimse sahiplenmemekte kendileri de saldırıya uğradıklarında büyük yıkımlar ortaya çıkmamışsa gizli tutmayı tercih etmektedirler.

Mobil cihazlar ve bulut sistemleri çeşitlidir, genellikle birden çok kuruluş tarafından yönetilir. Sonucunda ise teknoloji ve teknolojinin faaliyet gösterdiği sosyal, ekonomik ve düzenleyici ortam için her ikisinin de sonuçları ile olan güven ilişkilerinin karmaşık bir karışımıdır (Kotz ve diğ., 2015). Haberleşme sisteminde ortaya çıkan bütün gelişmelere rağmen dışarıdan gelecek tehditler önlenemezse gerek iletim aşamasında, gerekse depolama aşamasında dış etkenlerden kaynaklanan kayıpların ortaya çıkması kaçınılmazdır (Wiener, 1975:131). Saldırılar sistem güvenlik seviyesinin artırılması için vesile olmaktadır. Ancak alınan tüm tedbirlere rağmen siber güvenlik konusunda kesin olan daha fazla saldırı olacağı ve bu saldırıların bazılarının başarılı olacağıdır. Zararlı bir saldırganın zarar verebileceği zararı sınırlamak için, tek tek cihazları güvenli konumda tutmak gerekmektedir (Fu ve diğ., 2017). Güvenlik ve emniyet karmaşık fiziksel tesislere sahip bilgisayar donanımı ve yazılımı ile bağlantı kurularak bağlanabilir (Wolf ve Serpanos, 2017). Son on yılda kablosuz kanallar aracılığıyla siber uzaya bağlı tüm endüstrileri kapsayan büyüyen tehdidi vurgulayan önemli sayıda veri güvenliği olayı yaşanmıştır (Abouzakhar ve diğ., 2017). Diğer yandan güvenlik endişeleri birçok geleneksel güvenlik saldırısının sonuçlarını büyütmektedir. Güvenlik ve emniyet arasındaki etkileşimi gösteren bir örnek Mayıs 2015'te, uçağın uçtuğu sırada United Airlines tarafından işletilen bir Boeing 737'nin uçuş kontrol sistemlerine girdiği iddia ettiği zaman meydana gelmiştir. Kişi uçuş kontrollerine bir komut vermek için yeterli yetkiye sahip yerleşik eğlence sistemi aracılığıyla uçuş kontrol sistemlerine girebildiğini iddia etmiştir (Wolf ve Serpanos, 2017). Almanya'da da başta Cumhurbaşkanı olmak üzere yüzlerce siyasetçiye ait kişisel bilgilerin aşırı sağcı gruplarla Rus Hackerlerin ortak operasyonuyla elde edilip Twitter üzerinden yayımlandığı görülmüştür (Dalaman 2019). Son dönemde siber saldırılar yoğunluk ve sayı bakımından artış göstermektedir. 2017 verilerine göre gerçekleştirilen siber saldırıların % 87'si hükümetler tarafından yapılmaktadır. (Akyeşilmen, 2018:223-231). Tek bir cihazı emniyetli ve güvenli hale getirmek zaten zor bir sorunken, ne yazık ki bu tür cihazların sayısı ve bağlantısı arttıkça, bu cihaz koleksiyonlarını yönetme zorluğu katlanarak artmaktadır (Fu ve diğ., 2017). Siber güvenlik devletler açısından hayati önemde bir öncelik olarak değerlendirilmektedir. Alınacak bütün tedbirlere rağmen siber

alanda güvenliğin her geçen gün biraz daha zorlaşacağı bilinmektedir. Siber alanın tabiatı gereği tam güvenlik sağlamak mümkün değildir. Alınacak tedbirlerle tehditleri minimuma indirmek mümkündür. Ancak bu konuda paydaşların samimi olarak güvenliği benimsemeleri ve işbirliğine yönelmeleri gerekmektedir (Akyeşilmen, 2018:121-251). Devletler tehlikelere karşı ortak mücadele zemini oluşturmanın gerekli olduğunu, aksi takdirde anarşik ortamın küresel huzursuzluğu körükleyeceğini düşünmelidir.

**Hukuki Altyapı Oluşturma Çalışmaları**

Kamu düzen ve güvenliği devletin en önemli sorumluluk alanlarından biridir. İletişimdeki gelişmeler devletlere kamu düzeninin sağlanmasında kolaylıklar sağlarken ciddi tehlikeleri de beraberinde getirmektedir. Gelinen noktada bilgisayarlar sadece bilginin otomasyon sistemlerine ulaştırılması ve iletişim aracı olmaktan çıkmıştır (Öztemel, 2016:14). Teknolojik gelişmeler saldırı imkânlarını artırıp çeşitlendirmiştir. Saldırılarla mücadele devletlerin sorumluluğu olmaktan ileri boyutlara geçmiş ve küresel bir işbirliğini zorunlu hale getirmiştir. Devlet sınırları rahatlıkla geçilebilen (Aksu ve diğ., 2011:66) devletlerin klasik sınır kavramı yerine gümrüğün, pasaportun, vizenin olmadığı sorulamadığı bir yapıya dönüşmüştür. Siber alanda sınırların kaybolması devletlerarasında yetki ve sorumluluklar karmaşası yaşanması, kullanıcıların hukuki ve ahlaki kuralları bilerek göz ardı etmesine neden olmaktadır (Akyeşilmen, 2018:321). Ulusal ve uluslararası alanda düzenlenen yaptırımlar "denetim yeterli derecede kuvvetli olan ve varlığı yargıları bir cezayla destekleyebilen bir gücün elindeyse etkin bir araç olabilir" (Wiener, 1975:148). Ancak uluslararası hukuki düzenlemeler siber suçlara çözüm oluşturacak yapı ve yaklaşımdan uzaktır. Küresel ve bölgesel düzeyde Avrupa Konseyi tarafından 2001 yılında kabul edilen siber suçlarla mücadele sözleşmesinden başka uluslararası bir anlaşma bulunmamaktadır. Devlet dışı aktörler de sürece dâhil edilip, güçlü devletlerin lehine olmayacak şekilde düzenlemeler yapılmalıdır (Akyeşilmen, 2018:60-104). Çünkü denebilir ki mevcut uluslararası hukuk kuralları da ancak güçlü devletlerin istediği oranda uygulanabilmektedir.



**Sonuç**

İnsanlığın ilk dönemlerinden itibaren toplumlarda barış isteği sürekli gündemde olmuş ancak küresel anlamda bir barış sağlanamamıştır (Marangoz, 2009). Günümüzde yaygınlaşan terör faaliyetleri insanlığın yeri ve zamanı belli olmayan ciddi bir savaş tehdidiyle karşı karşıya kalmasına neden olmuştur (Kırılmaz,2013:67). Küreselleşen dünyada insanlara geniş özgürlük alanları açılırken ciddi sorumluluklar da yüklenmektedir. Günümüz insanı kendisine

çizilen rolleri icra etmek yerine evrensel değerlerin korunması amacıyla kendi iradesini ortaya koyma sorumluluğu yüklenmektedir. Çünkü insan haklarının yerine getirilmesinin en önemli yollarından biri diğer vatandaşların kendi sorumluluklarını yerine getirmesiyle hayat bulabilmektedir (Tekeli,2002:14). Küreselleşme, insanlığın ve insan haklarının evrenselleşmesi beklentilerini karşılayamamıştır (Taptık ve Keleş, 1998:33). Haberleşme alanında ortaya çıkan gelişmeler dünyadaki bilimsel araştırmaları kısa sürede geniş kitlelere ulaştırmaktadır. Bu gelişmeler eskiden olduğu gibi farklı "kültür alanı" olgusunu hızla ortadan kaldırmaktadır. Değişik kültürlerin kaybolması hızlanırken bütün dünyayı kapsayan yeni bir kültürün etki alanı giderek hız kazanmaktadır (Vester, 1998:22-24).

İletişimde ortaya çıkan gelişmeler dünyayı haberleşme açısından küçültmüşse de toplumlar ve coğrafyalar arasındaki gelişmişlik seviyesi küçülmemiş aksine bazı bölgelerde tabanla tavan arasındaki uçurum daha da derinleşmiştir (Eczacıbaşı,1998:255-256). Soğuk Savaş sonrasında gelişen küreselleşme hareketi dünyayı tek pazar haline getirmiş, üretim ve pazarlama yöntemleri tamamen değişmiştir (Özsoylu,2017:43). Siber alandaki faaliyetler insanların fiziksel iletiminden çok, bilgi iletimi üzerinde yoğunlaşmaktadır. Gerek devletlerin kendi içinde gerekse uluslararası alanda tarihte benzeri görülmemiş boyutta haberleşme sistemi oluşturulmuştur. Siber alandaki gelişmeler bilginin alınıp satılabilen bir nesne görünümüne dönüşmesine neden olmuştur (Wiener, 1975:147-159). İletişimde ortaya çıkan gelişmeler kişilere, kurumlara ve devletlere sağladığı yararlar yanında çok sayıda tehdit ve tehlikeyi de beraberinde getirmiştir. İnsanlar siber risklerin menfaatleri geride bırakmasıyla karşı karşıyadır. İnsanlar aktif olarak interneti kullanmasalar bile günlük hayatta yer alan cihazlar interneti sahipleri adına kullanıyor olacaktır. İnternetin herkes tarafından kullanıldığı ve herkesin etkili olduğu bir alan olarak değerlendirildiğinde sağlanan faydaların mı yoksa muhtemel risklerin mi daha ağır bastığı tartışılmaya devam edecektir (Aksu ve diğ., 2011:35-36). Bilgisayarlar verilen bilgilere göre hareket ettiğinden bilgilerin doğruluğu oranında geçerli sonuçlara ulaşılacaktır (Öztemel, 2016:14). Bilim adamları günümüzde ortaya çıkan şeylerden birçoğunun sonuçlarını görememektedir (Wiener, 1975:177). Geliştirilen robot teknolojisi öğrenme ve birbiriyle iletişime geçme noktasına geldiğinde insanlar üzerinde hâkimiyet kurup kuramayacağı tartışılmaktadır. Günümüzdeki uygulamalar doğrultusunda insanlar tarafından geliştirilen ve programlanan makinelerin insanlara hâkim olamayacağı savunulmaktaysa da bu soru zihinleri sürekli meşgul edecektir. Makineler çok sayıda veriyi değerlendirerek objektif neticelere ulaşabilir. Ancak verilerin sübjektif değerlendirilmesi insanlar tarafından yapılmaktadır (Songar, 1991:139-148)."İnsan beyninin bir benzerini

yapma konusundaki çalışmalar, çocukluk döneminde olmakla birlikte, gelişme yolu tamamen açıktır. Heyecanla dolu olan bu yolun bazı yönleri, ürkütücü düşünceleri akla getirmektedir". "İnsan beyni" ile "elektronik makine" nin ortak hayatından yeni türlerin ortaya çıkarılması hedeflenmektedir (Akman, 2003:15-16). Diğer bir ifade ile bilgisayar teknolojilerinde ortaya çıkan gelişmeler insan beyninin temel fonksiyonlarını yerine getirebilen sistemlere dönüşmüştür (Öztemel, 2016:41).

Bilgi depolama işleminden çok, o günün ihtiyaçlarını karşılayabilecek durumda olan ve dış dünyayla kendi bilgilerini karşılaştırıp davranışlarını düzenleyebilen ülkeler güvenlik içindedir. Diğer bir ifadeyle üzerine gizlilik damgası vurularak arşivlerde saklanan bilgiler sürekli değişen dünya şartlarında insanları kısa bir süre için dahi korumaya yeterli değildir. Bilimsel gizli bilgilerin alınacak tüm güvenlik önlemlerine rağmen yayılması bir zaman sorunudur. Bu nedenle ortaya konulan her buluş insanları yenisini yapmaya zorlamaktadır (Wiener, 1975:182). İnternet bağlantılı ürünlerin yaygınlaşması güvenlik açıklarını artırmaktadır. Siber alandaki gelişmeler baş döndüren yeni fırsatlar yanında tehditler oluşturmaktadır (Fu ve diğ., 2017). Belirli hayat imkanlarından mahrum, küresel değerlere sahip olmayı amaçlayan insanlar için Hugo "sefil" sıfatını kullanmaktadır (Hugo,2013:10). "Art niyetli ve ilkel bir adaletsizliğin, kitlelerin istatistiksel bir mutluluğunun biricik koşulu olabilecek bir dünya devleti tehlikesiyle karşı karşıyayız", bu durum aklıselim her insan açısından karşılaşılabilecek büyük bir tehlikedir. Siber alanda çalışma yapan bilim adamlarının değişik disiplinlerdeki bilim adamlarıyla fikir alışverişi içerisinde olması çıkabilecek tehlikeleri bir nebze de olsa sınırlandırabilecektir (Wiener, 1975:249). Özellikle güvenlik, fiziksel güvenlik, gizlilik ve kullanılabilirlik ile ilgili konular sıkı bir şekilde birbiriyle bağlantılıdır ve aynı anda dördüne hitap eden çözümler gereklidir (Fu ve diğ., 2017). Siber saldırılar, güvenliğin ötesinde küresel manada insan haklarının tehdit altında olmasına yol açabilmektedir. Devletler siber alan söz konusu olduğunda sınır güvenliğini yeni bir konseptle değerlendirmelidir. Ancak artan güvensizlik ortamına rağmen yapay zekânın devreye girmesi güvenlik önlemlerini artırabilecektir.



**Kaynakça**

Anadolu Ajansı, (2019), İran'da benzin zammına tepkiler siyaseti de sarstı,https://www.aa.com.tr/tr/analiz/iranda-benzin-zammina-tepkiler-siyaseti-de-sarsti/1648846, Erişim Tarihi: 08.12.2019.

Abouzakhar, N.S.,Jones, A., Angelopoulou, O.,(2017), Internet of Things Security: A Review of RisksandThreatsto Healthcare Sector, IEEE International Conference on Internet of Things, Exeter, UK.

Akın,A.,(2016), Siber Güvenlik Endişesi ve İnternet, http://www.Stratejik analiz.com/analizler/harp-ve42.

Akman, T. (2003), Sibernetik Dünü, Bugünü, Yarını, İstanbul: Kaknüs Yayınları.

Akman, Toygar,(2003), Öbürgünkü Sibernetik, İstanbul: Kaknüs Yayınları.

Aksu, H., Candan, U., Çankaya, M.N., (2011), Her Şey Çıplak Bildiğiniz İnternetin Sonu: Web3 3.0, İstanbul: Kapital Medya Hizmetleri.

Akyeşilmen, N., (2018),Disiplinlerarası Bir Yaklaşımla Siber Politika ve Siber Güvenlik, Ankara: Orion Yayınları.

Ayhan, Veysel., (2006), İmparatorluk Yolu: Petrol Savaşlarının Odağında Orta Doğu, Ankara: Nobel Yayın Dağıtım.

BBC, (2019), İran'daki protestolar: Benzin fiyatlarının yükselmesine gösterilen tepki nasıl büyüdü?,https://www.bbc.com/turkce/haberler-dunya-50488584, 21 Kasım 2019 Erişim Tarihi: 08.12.2019

BTSGD (Bilişim Teknolojileri ve Siber Güvenlik Derneği), Nesnelerin İnterneti ve Değerler (Konferans),http://www.bs.org.tr/blog/nesnelerin-interneti-internet-of-things-ve-degerler/41, Erişim Tarihi:30.11.2019.

BM Antlaşması, TBMM.https://www.tbmm.gov.tr/komisyon/insanhaklari/pdf01/3-30.pdf, Erişim Tarihi: 15.09.2015.

Bozkurt, Enver (2003), Birleşmiş Milletler Sisteminde Kuvvet Kullanımı Körfez Krizi Örneği ve Irak'ın Durumu ABD'ye 11 Eylül 2001 Terörist Saldırı, Ankara: Nobel Yayınları.

Baylançiçek, Berk, 267 Milyon Facebook Kullanıcısının Telefon Numarası Açığa Çıktı,

https://www.webtekno.com/milyonlarca-facebook-kullanicisinin-telefon-numarasi-internete-dustu-h82117.html, Erişim Tarihi:20.12.2019.

Chomsky, Noam (2008), Müdahaleler, (Çevirenler: Taylan Doğan, Nuri Ersoy). İstanbul: Bgst Yayınları.

Dalaman, Cem (2019) Almanya'da siber saldırı https://www.amerikaninsesi.com/a/almanya-da-siber-sald%C4%B1r%C4%B1/4728627.html 4 Ocak 2019 Erişim Tarihi:06.01.2019

Davis, J.,(2017), TheLighter Side of Things: TheInevitableConvergence of the Internet of Thingsandybersecurity, Information Technology ve CIO NASA AmesResearch Center GITEC.

Eczacıbaşı, F., (1998), Dördüncü Oturum: Sivil Toplum Kuruluşları Arası İletişim ve İlişkide Deneyimler, Girişimler ve Öneriler, Üç Sempozyum Sivil Toplum Kuruluşları, Sivil Toplum Kuruluşları Arasındaki İletişim Sorunları ve Çözümleri Sempozyumu 7-8-9 Aralık 1995, İstanbul: Türkiye Ekonomik ve Toplumsal Tarih Vakfı Yayınları.

Farooq, M.U.,Waseem, M., Khairi, A., Mazhar, S., (2015), International Journal of Computer Applications, Volume 111 - No. 7.

Forbes, Jack. D., (2009),Kolomb ve Diğer Yamyamlar, Beyaz Yağmacılığın Gölgesinde Sömürü ve Emperyalizm. (Çeviren: Işıl Özbek). İstanbul: Kalkedon Yayınları.

Fu K.,Kohno T., Lopresti D., Mynatt E., Nahrstedt K., Patel S., Richardson D., &Zorn B., (2017). Safety, Security, andPrivacyThreatsPosedbyAcceleratingTrends in the Internet of Things. http://cra.org/ccc/resources/ccc-led-whitepapers/

Heywood, Andrew (2013),Küresel Siyaset, (Çevirenler: Nasuh Uslu, Haluk Özdemir). Ankara: Adres Yayınları.

Hugo,Victor, (2013), Bir İdam Mahkûmunun Son Günü,Çeviren: Erhan Büyükakıncı, İstanbul:Can Sanat Yayınları.

Karakaş, Muammer, Hakkı. (2016), Büyük Veri, Endüstriyel İnternet ve Sağlık Alanındaki Uygulamaları. Betim Konferansları. (Editör: Hakan Ertin). Hayat Sağlık ve Sosyal Hizmetler Vakfı, Beşikcizade Tıp ve İnsani Bilimler Merkezi.

Kamış,Enes (2019), **Siber Güvenlik Nedir?,**https://www.eneskamis.com/siber-guvenlik-nedir/ (Erişim Tarihi: 10.11.2019)

Kırılmaz, M., (2013), Güven ve Güvenliğin Sağlanmasında Sivil Toplum Kuruluşları, Ankara: Adalet Yayınevi.

Kotz, D., Fu, K., Gunter, C., Rubin, A., (2015),Privacyand Security, Security for Mobile and Cloud Frontiers in Healthcare, Communications of the ACM, August 2015, Vol. 58 No. 8, Pages 21-23.

Marangoz, M., (2009, Toplumsal Barışın Sağlanmasında STK'ların Rolü, Her Yönüyle Dernekler Dergisi, s.42-56.

Martin, G., Martin, P., Hankin, C., Darzi, A., Kinross, J., (2017),Cybersecurityandhealthcare: how safearewe?. BMJ;358:j3179 doi: 10.1136/bmj.j3179.

Medikal Akademi, (2016), Siber korsanların gözü sağlık sektöründe ve hastanelerde, https://www.medikalakademi.com.tr/siber-korsanlarin-gozue-saglik-sektoruende-ve-hastanelerde/, Erişim Tarihi: 10.06.2019.

Memleket (2019),https://www.memleket.com.tr/ev-ici-guvenlik-kamerasi-kullanicilarina-hacklenme-uyarisi-1955754h.htm, Erişim Tarihi:14.12.2019.

Özsoylu, A.F., (2017), Endüstri 4.0 Çukurova Üniversitesi İİBF Dergisi,Cilt:21, Sayı:1 s.41-64

Öztemel, E., (2016), Yapay Sinir Ağları, 4.Basım. İstanbul: Papatya Yayıncılık Eğitim.

RexHughes–NATO Güvenlik Danışmanı, Siber Güvenlik Nedir?http://donencebilisim.com/siber-guvenlik-nedir.html, (Erişim tarihi:01.09.2019).

Sır,Ali Sabri, (2017),https://medium.com/@alisabrikim/siber-g%C3%BCvenlik-nedir-i%CC%87nternette-ne-kadar-g%C3%BCvendeyiz-c55691b98679 Siber Güvenlik Nedir? İnternette Ne Kadar Güvendeyiz?, Erişim Tarihi:15.11.2019.

Siber Güvenlik Nedir ?,http://sibertehdit.com/siber-guvenlik-nedir/,Erişim Tarihi:15.11.2019.

Songar, Ayhan., (1991), Sibernetik. İstanbul: Yeni Asya Yayınları.

Sur, Melda (2013). Birleşmiş Milletler Örgütünün Gelişimi ve Geleceği, Prof. Dr. Aydın Zevkliler'e Armağan, C.III, Yaşar Üniversitesi Elektronik Dergisi, C.8, Özel Sayı, http://journal.yasar.edu.tr/wp-content/uploads/2014/01/10-Melda-SUR.pdf, s.2535-2550, Erişim Tarihi: 08.12.2016.

Suoa, H.,Wana, J., Zoua, C., Liua, J., (2012),Security in the Internet of Things: A Review International Conference on ComputerScienceandElectronicsEngineering, China.

Taptık, Y., Keleş, Ö.(1998). Kalite Savaşı, İstanbul: KalDer Yayınları.

Tekeli, İlhan (2002). Sivil Toplum Kuruluşları, Yerel Yönetimler ve Yerelleşmenin İç İçeliği. STK'lar, Yerelleşme ve Yerel Yönetimler, Türkiye'de Sivil Toplum Kuruluşları Sempozyumu-XI. Yayıma hazırlayan: Ali Çakmak, İstanbul: Türkiye Ekonomik ve Toplumsal Tarih Vakfı Yayını, 21-22 Haziran 2002, İTÜ Maçka Sosyal Tesisleri.

TRTAvaz, https://www.trtavaz.com.tr/haber/tur/dunya/bilgisayar-korsani-cocuklarin-odasindaki-kamerayi-hackledi/446398, Erişim Tarihi:13.12.2019.

Vester, Frederic., (1998), Sibernetik Toplum. Yeni Bir Hayatta Kalabilme Modeli, (Çeviren: Aydın Arıtan). İstanbul: Arıtan Yayınevi.

Veri Güvenliği; htpp://www.entegreyazilim.com.tr/indekx.php? Erişim Tarihi: 10.04.2019.

Wiener, Norbert., (1975), Emek Sibernetik ve Toplum, (Çeviren: İbrahim Keskin). İstanbul: Özgün Yayınları.

Wolf, M.,Serpanos, D., (2017), Safetyand Security of Cyber–Physicaland Internet of ThingsSystems, IEEE, Vol. 105, No. 6.

Yetimler, E., Internet of Things (Nesnelerin İnterneti) Nedir? Cihazların Etkileşim Trendleri, https://www.karel.com.tr/blog/internet-things-nesnelerin-interneti-nedir-cihazlarin-etkilesim-trendleri, Erişim Tarihi: 10.04.2018.