ÜLKE GÜVENLİĞİMİZDE ALINABİLECEK MAKRO SİBER GÜVENLİK ÖNLEMLERİ

Tayfun ACARER

Bilgi Üniversitesi, Bilgisayar Teknolojileri Bölümü, Meslek Yüsek Okulu, Bilgi Üniversitesi, İstanbul

tacarer@hotmail.com

ÖZET

Günümüzde siber güvenlik olgusu bütün ülkelerin en öncelikli ve kritik güvenlik konularından birisi haline gelmiştir. Özellikle Covid19 salgını sürecinde ve sonrasında toplumlar iş ve işlemlerini her zamankinden daha fazla sanal ortamda gerçekleştireceklerdir. Bunun sonucu ortaya çıkan yeni ihtiyaçlar şebekelerin geleneksel yapılarını ve kapasitelerini önemli ölçüde değiştirecektir. İnternet kullanımının artması, siber güvenlik konusunu bundan sonraki süreçte geçmişe göre çok daha önemli hale getirecektir. Çünkü önümüzdeki süreçte bu tür saldırıların hem sayısı hem de verdiği zararların boyutu giderek artacak ve yaşantımızın ayrılmaz bir parçası haline gelecektir. Bu nedenle ülkelerin siber güvenlik konusundaki politika ve stratejileri yeniden gözden geçirmeleri ve bu konuda alabilecekleri önlemleri acilen uygulamaya koymaları zorunlu olmuştur. Bugün Siber uzayda savaş tüm hızıyla devam etmekte ve dünya ülkeleri halen uluslararası alanda hukuki bir çerçeve içinde anlaşmaya varamamaktadırlar. Bu çalışmada Anayurt Güvenliği konusunda ülkelerin politika ve stratejilerini belirlerken göz önünde bulundurması gereken makro düzeydeki siber güvenlik önlemleri ele alınmış ve bu konuda çözüm önerileri ve uygulama örnekleri ortaya konulmuştur.

***Anahtar Kelimeler*—**Siber Güvenlik, Siber Saldırı, Siber Savunma, Siber Uzay, Siber Caydırıcılık

Macro Cyber Security Measures in Homeland Security

ABSTRACT

Today, the concept of cyber security has become one of the top priority and critical security issues of all countries. Especially during and after the Covid19 epidemic, societies will carry out their work and transactions in more virtual environments than ever before. The resulting new needs will significantly change the traditional structures and capacities of networks. The increasing use of the Internet will make the issue of cyber security much more important than in the past. Because both the number of such attacks and the size of the damages it will cause in the coming period will gradually increase and become an integral part of our lives. For this reason, it was compulsory for countries to revise their policies and strategies on cyber security and immediately implement the measures they can take in this regard. Today, war in Cyber space continues at full speed and the countries of the world are still unable to reach an agreement in a legal framework internationally. In this study, macro cyber security measures that countries should take into consideration while creating policies and strategies on Homeland Security are discussed and solution suggestions and application examples are presented.

***Keywords*—** Cyber Security, Cyber Attack, Cyber defence, Cyber Space, Cyber Deterrence

I. GİRİŞ (INTRODUCTION)

Bilgisayar ve haberleşme teknolojilerinde yaşanan baş döndürücü gelişmeler ve özellikle internetin katalizör etkisi ile insanların çalışma, iletişim kurma ve her türlü günlük ihtiyaçlarını karşılama biçimi sürekli dönüşüm halindedir [1]. Günümüzde İnternet artık her alanda karşımıza çıkmakta olup ve günlük yaşamda çok önemli bir yere sahiptir [2]. Gelişen teknolojiler sayesinde neredeyse her zaman ve her yerden İnternete erişim sağlanmaktadır [3].

Çünkü özellikle son 5 yıllık süreç dikkate alındığında Mobil ses ve data ile İnternet ve Sabit datanın pazardaki payı giderek artmaktadır [4]. Bu nedenle günümüzde İnternet tabanlı cihazlar hayatımızda olduğu sürece zararlı yazılım tehdidi ile karşılaşması kaçınılmaz bir gerçek olarak karşımıza çıkmaktadır [5].

Cihazların kendi arasındaki haberleşmesi olarak bilinen Nesnelerin İnterneti'nin (Internet of Things-IoT) giderek yaygınlaşması ve bu sistemlerin kablosuz algılayıcı ağlara dayanan bir teknoloji olması [6], Bilgi Güvenliği konusuna ayrı bir boyut getirmektedir. Çünkü Nesnelerin internetinin temel amacı, insan yardımı olmaksızın nesnelerin kendi aralarında bilgi alma/vermesini temin etmektir [7].

Yazılım ve elektronik alanlarındaki gelişmelerin giderek artmasıyla adreslenebilir cihaz/nesne sayısında çok ciddi artışlar meydana gelmiştir ve artan bir ivmeyle bu artış hızla devam etmektedir [8]. Nesnelerin İnterneti çeşitli iletişim ve haberleşme protokolleri sayesinde birbiri ile iletişim kuran nesnelere ait verileri toplayıp analizini yaparak nesneleri kontrol eden bir ağdır [9]. Bu ağda bulunan cihazlar ve algılayıcılar insan-makine, makine-makine (M2M) iletişimi kurabilen organizmalardır [10].

Nesnelerin İnternetinde üreticiler farklı teknolojiler kullanmaktadır [8]. Bu teknolojilerden bazılarında bulunan güvenlik açıkları [11] nedeniyle Nesnelerin İnternetinde uçtan uca güvenli haberleşme sağlanamamaktadır [12]. Uçtan uca güvenli haberleşmenin sağlanması için söz konusu güvenlik açıklarının tespit edilip önlemler alınması gerekmektedir [13]. Bu durum, siber saldırıların bu tür sistemlere daha kolay ve kontrolsüzce yapılmasına olanak sağlamaktadır. Bu arada yaygınlaşan akıllı nesneler, bunların İnternete bağlı olarak birbiriyle iletişim kurabilmesi, bunların kolaylıkla çeşitli siber saldırılara maruz kalabilmelerini de beraberinde getirmektedir [14].

Bu değerlendirmeler doğrultusunda yapılan çalışmada öncelikle değişik kademelerde yapılan Siber Saldırılar ve bunlara karşı alınan Siber Güvenlik Önlemleri ile ilgili bilgi verilmiş ve özellikle III. Bölümde yakın süreçte yaşanan bazı önemli Siber saldırılar ile konunun önemine dikkat çekilmiştir. Çünkü tarihsel süreç, bu saldırıların sayısının ve boyutunun giderek artacağı yönünde bir eğilim göstermektedir. Bu süreçte özellikle uluslararası düzeyde yapılan saldırıların etkisi ve verdiği zararların boyutunun giderek arttığı ve konvansiyonel saldırı araçlarının verdiği zararlardan çok daha olumsuz sonuçlar doğurduğu gözlemlenmektedir.

IV Bölümde de bu saldırılara karşı Ülke bazında alınabilecek önlemler ele alınmış ve dünya uygulamalarından örnekler verilerek, siber saldırılara karşı makro baz'da yapılabilecek çalışmalar detaylı olarak değerlendirilmiştir.

Ortaya konulan tüm veriler Sonuç bölümünde değerlendirilerek ülke güvenliğimizde alınmasında fayda mütalaa edilen siber güvenlik önlemleri uygulayıcıların dikkatine sunulmuştur.

II. SİBER SALDIRILAR VE SİBER GÜVENLİK ÖNLEMLERİ (CYBER ATTACKS AND CYBER SECURITY PROCESS)

"Siber saldırı" tanımı, günümüzde gerek uluslararası, gerekse ulusal platformda kesin olarak yapılamamakla [15] birlikte, genel anlamda hedef seçilen şahıs, şirket, kurum, örgüt, gibi yapıların bilgi sistemlerine veya iletişim altyapılarına yapılan planlı ve koordineli saldırılara olarak tanımlanmaktadır.

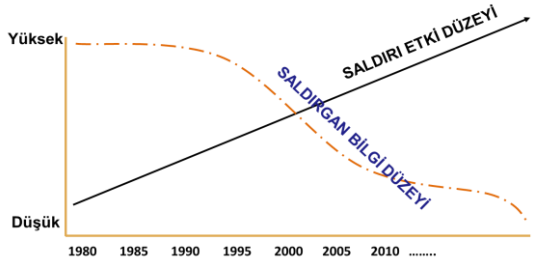
Siber savunmayı ise; siber uzayda faaliyet gösteren yazılım, donananım, iletişim ağı altyapısından meydana gelen bilgi sistemlerini ve bu sistemleri içeren her türlü teçhizat, sistem ve altyapıyı siber tehditlere karşı korumak için alınan önlemlerin uygulanması olarak tanımlamak mümkündür

Buna bağlı olarak ortak kabul edilmiş bir tanımı bulunmayan "siber terör" ifadesi, ucu açık bir kavram olarak kabul edilmektedir.

Siber Güvenlik (SG), siber uzayı oluşturan bilgi teknolojileri sistemlerinin tehditlerden korunmasını, buradaki bilginin gizlilik, bütünlük ve erişilebilirliğinin güvenli bir

şekilde sağlanmasını, saldırı ve siber durumların belirlenmesini, bu belirlemelere yönelik önlemlerin alınmasını ve sonrasında ise sistemlerde karşılaşılan sorunların saldırı öncesine geri getirilmesi olarak ifade edilmektedir [16]. Siber güvenlik ilk olarak 1990'lı yıllarda bilgisayar mühendisleri tarafından ağa bağlı bilgisayarlarla ilgili güvenlik sorunlarını ifade etmek için kullanılmıştır [17].

Önceleri ciddi bir bilgi birikimi gerektiren Siber Saldırıların, günümüzde kullanılan programların gelişimi ve bilişim sistemlerinin yaygınlaşması ile hem "Sayısı" artmış hem de "Etki Düzeyleri" yükselmiştir.



Şekil 1. Sibel Saldırıları sayısı ve etki düzeyi

Günümüz bilgisayar dünyasında ilk hizmet engelleme saldırısı olarak bilinen morris virüsü, 1988 yılında Rober Tappan Morris tarafından eğlence amaçlı yazılmıştır. Morris solucanı olarak tanımlanan ve Morris'in kodlama sırasında yaptığı bir yanlış sonucu ortaya çıkan bu program, sadece birkaç gün içinde günümüz İnternetinin öncüsü olan Arpanet'i gezmiş ve internete bağlı olan bilgisayarların %10'unun ağlarını çalışamaz hale getirmiştir [18].

Modern toplumlardaki altyapının yüksek teknolojiye ihtiyaç duyması nedeniyle, sanal dünya üzerinden gerçekleştirilen saldırıların etkileri konvansiyonel silahlar kadar büyük olabilmektedir. Ayrıca siber saldırıların maliyeti geleneksel saldırılarla mukayese edilemeyecek kadar düşüktür ve siber saldırının hedefinde yer alan objenin kasten mi, yoksa kazayla mı saldırıya maruz kaldığının anlaşılması kolay değildir [19]. Bu nedenle Siber Güvenlik önlemlerini "Yapılması kolay ve ucuz, savunulması zor ve pahalı bir süreç" olarak tanımlamak mümkündür.

Siber saldırılarının gerçekleştirilme sebepleri kronolojik olarak incelendiğinde, saldırı motivasyonun beş temel evrede geliştiği gözlemlenmektedir. Bu saldırıların başlangıcı olarak bilinen 1988 yılında saldırının gerçekleştirilme nedeni merak ve eğlenceyken, günümüze gelindiğinde ise saldırıların motivasyonunda ciddi değişimler olduğu görülmektedir [20]. Bu nedenle Siber saldırılar önceleri kendini ispat etme, heyecan meydana getirme, karşı tarafı cezalandırma, zarar verme, vb daha masum gerekçeler ile yapılırken, bu saldırılar daha sonra veri hırsızlığı, ticari kazanç sağlama, menfaat temin etme, ülkeleri cezalandırma gibi daha profesyonel ve kötücül amaçlarla yapılmaya başlanmıştır.

Genellikle saldırganın amacına bağlı olarak zararlı yazılımın türü ve yöntemi de değişkenlik göstermektedir [21]. Bu saldırılarda saldırgan, genelde saldırı yapacağı ağa botnetler yardımı ile çok fazla sayıda paket göndererek ağın bant genişliğinin taşmasına sebep olmaktadır. Bu saldırılardan en çok karşılaşılabilecek olan ve en yaygın kullanılan ise servis engelleme saldırılarıdır [22]. Böyle bir saldırıda, Internet Kontrol İletisi Protokolü (ICMP), Kullanıcı Veri Bloğu Protokolü (UDP) ve İletim Denetimi Protokolü (TCP) gibi farklı ağ katmanı protokolleri kullanılabilir. Saldırıların büyüklüğü genellikle saniyede bit veya paket olarak ölçülmektedir.

Arbor Network'ün 2017 yılında yayınladığı internet güvenliği raporuna göre, DDoS saldırılarının %65'i volümetrik (hacimsel) niteliktedir [18].

III. YAKIN SÜREÇTE ÜLKELERARASINDA YAŞANAN BAZI ÖNEMLİ SİBER SALDIRILAR (SOME IMPORTANT CYBER ATTACKS BETWEEN COUNTRIES IN THE NEAR PROCESS)

Ülkelerarasında yapılan saldırıların tamamı kamuoyu ile paylaşılmadığı hatta gizli tutulduğu için, bu saldırıların tümüyle bilinmesi olanaksızdır. Ayrıca başarıyla atlatılan veya zararı hissedilmeyecek kadar az olan pek çok saldırının da olduğu unutulmamalıdır. Ancak bundan sonraki süreçte bu saldırıların hem sayısının hem de verdiği zararların boyutunun giderek artması ve yaşantımızın ayrılmaz bir parçası haline gelmesi kaçınılmazdır.

Son yıllarda Siber saldırılar nedeni ile ortaya çıkan zararlar kurumları ciddi olarak tehdit etmektedir. Siber Güvenlikle bilişim sistemlerinin Siber saldırılardan korunması, işlenen bilgilerin gizlilik, bütünlük ve erişilebilirliğinin güvence altına alınması, Siber saldırıların önceden tespit edilmesi ve bu tespitlere karşı önlemlerin alınması kurumlar için artık bir zorunluluktur [23]. Siber Saldırılar devletler tarafından yapıldıkça boyutları ve etkileri artmakta ve savaşa dönüşmektedirler [24].

Bu konuda ortaya çıkan bir başka problem de siber saldırıların devlet eliyle mi, yoksa suç unsurları tarafından mı gerçekleştirildiğinin anlaşılmasında ve tespitinde yaşanan sorunlardır. Bu sorun ise devletlere siber saldırıların kaynağı konusunda şüphe ile yaklaşılmasına sebep olmaktadır [25].

Siber alandaki faaliyetlerin kolay ve arkada iz bırakmadan yapılabilir oluşu, terör örgütlerinin yanı sıra devletlerin de ilgisini çekmeye başlamıştır. Hatta kimi ülkeler siber saldırı ve siber savaşı önemli stratejik savunma ve rakibe zarar verme yöntemi olarak görmektedir. Bu nedenle yakın süreçte kamuoyuna yansıyan bazı makro düzeydeki saldırılar aşağıda başlıklar halinde toplanmıştır.

Bunlardan ilki, Suriye Elektronik Ordusunun yaptığı Siber saldırılar olup, bu grup siber uzay yeteneklerini kullanarak saldırılar gerçekleştirdiğini zaten gizlememektedir. Bilinen saldırılarının başında Mayıs 2015'de Washington Post gazetesine ait web sayfasının kendi kontrollerindeki bir adrese yönlendirilmesi olmuştur. Bu grup The Guardian, New York Times ve Forbes'e yapılan saldırıları takiben Haziran 2015'de ABD ordusuna ait web sayfasına da saldırı düzenlemiştir [26]. Benzeri saldırılar 2015 yılı içinde Türkiye'ye de yapılmıştır.

Yine yakın süreçte Çin ordusu tarafından da siber uzayda birçok saldırı yapılmıştır. 2014 yılı Mayıs ayında Amerika Birleşik Devletleri Adalet Bakanlığı, Çin ordusunda görevli beş kişinin 2006 yılından 2014 Nisan ayına kadar ABD'ye yönelik siber saldırılar düzenledikleri, bu saldırılar sonucu birçok e-postanın kopyalandığı (yaklaşık 700.000 sayfa) ve pek çok bilgisayara zararlı yazılım yüklendiğini açıklamıştır. Yine adı geçen Bakanlık bu kişilerin iade edilmeyeceklerini bildikleri halde suçlu bulunduklarını ilan etmiş ve bunların resimlerini yayınlamıştır. ABD istihbarat örgütlerinin ve FBI'ın yaptığı ortak çalışmada, bu kişilerin Şanghay havaalanı yakınında bulunan orduya ait 12 katlı "Datong Road" karargâhında görevli personel olduğu belirtilmiştir [27].

Son 10 yıl içinde yakın çevremizdeki ülkelerden Estonya, Ukrayna, İran'a da Ülkelerarası saldırılar yapılmış ve bu ülkelerdeki farklı sistemlere ve ekonomilerine ciddi zararlar verilmiştir.

2008 yılında Rusya ile Gürcistan arasında yaşanan savaşta Rusya'ya ait siber alandan Gürcistan'a yapılan siber saldırı da bu duruma örnek gösterilebilir. Rusya Gürcistan'a yönelik siber saldırılarda herhangi bir katkısı olmadığını iddia etse de, bu saldırıların Rusya'nın bilgisi dahilinde devlet destekli olarak mı, yoksa bu ülkede bulunan terör örgütleri tarafından mı gerçekleştirildiği kesinlik kazanmamıştır [28].

Siber saldırıların güncel örnekleri biri de 2007 yılında Estonya'ya düzenlenen yüksek yoğunluklu saldırılardır. Estonya'ya düzenlenen bu yoğun siber saldırıların başlangıç noktasını ülkede yaşayan Rus kökenli azınlıklarla Estonyalılar arasındaki sorun meydana getirmiştir. Geçmişten gelen anlaşmazlığa 2007 yılının Nisan ayında ortaya çıkan sorunlar da eklenince, ülke yoğun bir siber saldırı tehdidi altına girmiştir. Bu süreçte Estonya hükümetine ve ulusal medyaya ait sitelere yoğun DDoS saldırıları yapılmış ve bazı siteler kullanılamaz hale getirilmiştir [29].

Yakın dönemde yaşanan siber saldırı hedeflerinden bir başkası olan Gürcistan ise, 2008 yılında yaşanan Rusya-Gürcistan savaşıyla birlikte yoğun olarak siber saldırıyla karşı karşıya kalmıştır. 8 Ağustos 2008'de Rusya'nın Gürcistan'a saldırısını takiben Gürcistan hükümetine ait internet sitelerine DoS saldırıları düzenlenmiştir. Fiziki saldırıyla eş zamanlı düzenlenen siber saldırılar gerçek dünyada oluşan sorunların anında sanal dünyaya da yansıyabileceğini göstermiştir. Gürcistan ve Rusya arasındaki siber savaş

kamuoyunu şekillendirmek amacı da taşımaktadır. Her iki tarafın destekçileri tarafından gerçekleştirilen DoS saldırılarına ek olarak sahte siteler hazırlanmış ve bu sitelerde iki grup da kendi doğruları konusunda propaganda yapmışlardır [30]. Yine bu saldırılar ile Bankacılık, medya ve hükümete ait sitelere bilgi akışı durdurularak Gürcistan içinde ve uluslararası alanda haberlere ulaşım engellenmiştir [30].

Bir diğer siber saldırı Kırgızistan'da 2009 yılında meydana gelmiş ve yapılan DoS saldırısı ile ülkenin iki ana internet sağlayıcısı hedef alınarak, web sitelerinin çökmesine, ülkedeki elektronik posta servisinin de kullanılamaz hale gelmesine neden olunmuştur. Bu saldırıların Rusya kaynaklı olduğu tespit edilmiş, ancak saldırıların arkasında Rus hükümetinin olduğuna dair herhangi bir kanıt bulunamamıştır [31].

Siber saldırıların diğer bir türü olan kötü amaçlı yazılım programlarının en gelişmiş versiyonu olarak tarihe geçen Stuxnet adındaki solucan 2010 yılında İran'da ortaya çıkmıştır. Stuxnet'in en belirgin özelliği kendisini otomatik olarak kopyalayabilmesidir. Bu virüs böylece içine yerleştiği ağı kullanılamaz hale getirene kadar yayılabilen bir tür yazılım bombası işlevi görmüş ve dahil olduğu Nükleer sistemin kısa sürede büyük hasara uğramasına yol açmıştır [32].

IV. SİBER GÜVENLİK İLE İLGİLİ ÜLKE BAZINDA ALINABİLECEK MAKRO ÖNLEMLER (MACRO MEASURES THAT CAN BE TAKEN BY COUNTRY RELATED TO CYBER SECURITY)

Siber güvenlik konusunu bireysel, kurumsal ve ulusal güvenlik olmak üzere temel olarak üç ana başlıkta ele almak mümkündür. Güvenlik yaklaşımları günümüzde ağırlıklı olarak bireysel ve kurumsal güvenlik önlemleri olarak ele alınmış ve çözümleri de büyük oranda bu yaklaşımla geliştirilmiştir. Ayrıca Güvenlik çözümleri ve ürünleri bireysel ve kurumsal olarak tasarlanmış, bu konudaki politika ve stratejiler de bu bakış açısıyla tesis edilmeye çalışılmıştır.

Yine siber suçların dünya genelinde verdiği zararın 2021 yılı sonuna kadar 6 trilyon doları bulacağı tahmin edilmektedir [33]. Gelinen nokta itibariyle ulusal ve toplumsal güvenlik her geçen gün daha fazla önem arz etmeye başlamıştır. Çünkü kritik sistemlerdeki bir ihlalin etkileri daha da fazla olacaktır. Tüm bu olumsuz etkiler düşünüldüğünde günümüzde teknolojide bilgi güvenliği konusunun her geçen daha fazla önem kazandığını söylemek mümkündür [34].

Neticede Ülke güvenliği, e-devlet güvenliği, kritik altyapıların güvenliği gibi kavramlar bu ihtiyaçların sonucu ortaya çıkmıştır. Tüm bu güvenlik problemlerine çözüm oluşturabilmek için Makro Güvenlik Önlemleri konusu günümüzde önemli bir başlık olarak ele alınması gereken bir husus olmuştur. Bu nedenle ülkelerin ulusal güvenliklerini sağlayabilmek için aşağıda ele alınan makro güvenlik önlemlerine yönelik politika ve stratejilerin geliştirmesi ve uygulamaya geçirilmeleri zorunlu hale gelmiştir.

4.1. Sistem Mimarilerinin Rehabilite Edilmesi

Ülkelerin sistem mimarilerinde halen büyük ölçüde "Best practice" anlayışı geçerlidir. Bu nedenle Ülkemizde ".TR alan" adlarına yapılan saldırılar her gün birçok DNS sunucusuna da yapılmaktadır. Özellikle mimari yapı ve kapasite planlamasındaki eksiklikler nedeniyle ".TRalan" adlarına yapılan bu saldırılar çok büyük sorunlara yer açmakta ve birçok kuruluşumuzu olumsuz etkileyebilmektedir. Bunun için Sistem Mimarisinde çalışan Yönetici ve Mühendislerin bu konuda dünya standartlarını öğrenmeleri ve onları sürekli takip ederek sistem dizaynlarını bunlara göre yapmaları gerekmektedir.

Bu şekilde ".TR alan" adlarında şimdiye kadar yaşanan sorunların, bundan sonraki süreçlerde de tekrar yaşanmasının önünde geçilebileceği düşünülmektedir.

4.2. Siber Güvenlik Eğitimindeki Boşlukların Giderilmesi

Siber tehditleri önlemenin veya en azından etkisini azaltmanın en etkin yollarından biri de eğitimdir. Gerek bireysel olarak gerekse kurumsal olarak personeli siber güvenlik konusunda eğitmek ve son bilgilerle donatmak artık kaçınılmaz hale gelmiştir. Buna paralel olarak kurumlardaki ve bireysel kullanımdaki

bilgisayarlar en son teknoloji ve güvenlik yazılımları ile donatılmalıdır [35]. Günümüzde siber güvenlik kavramı daha çok akademik bir eğitim ve alınan bir sertifika olarak görülmektedir. Bu nedenle bazı yöneticiler Siber güvenliğin sertifika programlarında veya üniversitede öğrenildiğini düşünmektedirler. Bu da çok büyük bir eksiklik, hatta yanlıştır.

Siber Güvenliğin en önemli unsurlarından birisi, sürekli olarak değişen bir ekosistem olmasıdır. Sertifika ve diğer akademik programlar birçok yararlı bilgi içerse de, verdikleri bilgiler genelde güncel olmamaktadır. Bu güncel olmayan bilgiler ve sertifikalar yüzünden kişiler ve firmalar kendilerini güvende hissetmekte, ancak bu da çok büyük bir yanılgıya yol açmaktadır. Bu nedenle güncel olmayan bilgileri güncel tutmanın çeşitli yöntemleri bulunmakta olup, bunun sürekli yapılması gerekmektedir.

Bu açıdan tıpkı bilgisayar veya telefonundaki bir işletim sisteminin sürekli kendini güncellemesi gibi, siber güvenlik ve siber savunma alanlarında çalışan kişilerin bilgilerini pratikleştirebilmeleri ve sürekli güncel tutabilmeleri çok önemlidir. Bu konuda verilecek eğitimlerde Ülkemizde BTK, Tübitak, Havelsan gibi kurumlardan faydalanılmasında ve bu kuruluşlarda ulusal ve süreklilik içeren bir vizyon çerçevesinde eğitim çalışmalarının verilmesi halinde, bu sorunun aşılması büyük ölçüde temin edilebilecektir.

4.3. ".TR Alan Adları" İle İlgili Düzenleme Yapılması

Türkiye'de ".TR alan adları" sistemi Ulaştırma ve AltyapıBakanlığı (UAB) kontrolünde bir yönetime bir an önce devredilmelidir. Bu husus öncelikli bir konu olarak ele alındığı takdirde, çok kısa zamanda giderilerek çözümlenmesi mümkündür. Bu nedenle halen bu konuda devam eden hukuksal sürecin bir an önce tamamlanmasında büyük fayda bulunmaktadır.

4.4. Milli Yazılım ve Donanımların Geliştirilmesi

Diğer mühendislik alanlarında olduğu gibi yazılım mühendisliği alanında da teknik olmayan becerilerin önemi her geçen gün gittikçe artmaktadır. Yazılım mühendisliği süreçleri gerek mühendislerin gerekse farklı alanlardan paydaşların birlikte çalışmasını gerektirmektedir [36].

Ülkemizde milli yazılıma karşı çok büyük bir talep bulunmaktadır. Milli yazılımın faydası tartışmasız olmakla birlikte, %100 yerli yapmak istediğimiz programlar aslında "açık kod/open source" kaynaklardan üretilmektedir. Bu kodların yeniden yazılması yıllar suren bir emek ve uğraşı gerekmektedir. Bu nedenle sorun sadece kodun yazılması değil, o kodun güncel halde tutulması olmalıdır. Bu amaçla İnternete bağlantılı yazılımların güvenlik açıklarının sürekli olarak kapatılması çok önemlidir. Ayrıca, ülkemizde milli yazılımların geliştirilmesi konusunda çalışılırken, aynı zamanda milli donanımların da kullanılması gereklidir. Çünkü 2016 yılından itibaren siber saldırıların daha çok donanım ekipmanlarına yönelik olacağı dünyadaki güvenlik uzmanlarının ortak düşüncesidir.

4.5. Şebekelerimizde Kullanılan Yabancı Ürünlerin Yol Açabileceği Tehditlerin Giderilmesi

Halen Sabit ve Mobil Alt Yapımızda kullanılan sistemlerde çok büyük oranda yabancı menşeli ürünler kullanılmaktadır. Özellikle bu ürünlerin farklı firmalarda eşite yakın oranda dağıtılmış olmaması daha da büyük risk teşkil etmektedir.

Bugün pek çok ülke bu konuyu büyük bir tehdit olarak gördüğü için, network sistemlerinin kurulumunda bu sakıncayı bertaraf edecek bazı şartlar koymaktadırlar. Bu durum sadece Devletler olarak değil, büyük firmalar ve Yer sağlayıcılar tarafından da önemle dikkate alınmaktadır. Örneğin Google'da hizmet verecek hiç bir altyapı sağlayıcısının gerek donanım, gerekse fiber optik bağlantı için kullanacağı ürünlerde firma mülkiyet oranının %40'ı aşmaması gerekmektedir.

Bu nedenle bu tip yatırımlara sadece finansal açıdan bakılmamalı, Ülkenin stratejik hedefleri ve milli güvenliği de göz önünde bulundurmalıdır. Bu tür arka kapı sorunlarının ancak milli yazılım ve milli donanımlar ile ortadan kalkacağı açıktır. Ancak bu konuda çok kısa sürede fazla bir şey yapılması oldukça zordur. Bu nedenle söz konusu sorunun sistem mimarisinin ve planlaması aşamasında milli

unsurlar ve milli imkan / kabiliyetler göz önünde bulundurularak, belirlenecek milli bir politika çerçevesinde orta dönemde çözülmesi hedeflenmelidir.

4.6. Milli Savunma Kalkanının Tesis Edilmesi

Ülkelerin Siber Güvenliklerinde dış tehditler kadar iç tehditler de büyük problemlere yol açabilmektedir. Bilindiği üzere Türkiye'nin yurt dışı bağlantı kapasitesi yaklaşık 7 Tbps'dır. Bu değer her yıl artmasına karşılık yurt içi sistemlerin birbirlerine olan bağlantısı yüzlerce TBps'dır ve bu durumda iyi bir gelişmedir. Yurt içi internet bağlantısının güvenilir olmasının avantajı tartışılmaz. Ancak bu iletişim kontrol edilmez bir yapıda ise bunun riskinin de son derece tehlikeli olacağı açıktır. Çünkü yurt dışından gelen bir saldırıyı bir şekilde önleyebilmek mümkün iken, birkaç milyon kullanıcının bilgisayarının hacklenmesi ve bunların hepsinin bir anda içeriden saldırıda kullanılması halinde, bir anda alt yapıda ciddi sıkıntılarla karşılaşılması kaçınılmazdır.

Bu nedenle gerek yurt içi, gerekse yurt dışından gelebilecek saldırılara karışı Milli Siber Savunma Kalkanı kurulmalı ve Türk Telekom, Superonline, Ulakbim gibi İnternet'i taşıyan birimlerle koordineli olarak bir çalışmaya gidilmelidir. Bu şekilde halen ülkemizde kullanılan ve çoğunluğu yabancı firmalara ait olan güvenlik yazılımlarına olan bağımlılığın azaltılması da mümkün hale gelebilecektir.

4.7. Gizlilik Artırıcı Teknolojilerin Etkin Kullanımı

Gizlilik artırıcı teknolojiler (Privacy Enhancing Technologies) kavramı; bilgi sistemlerinin işlevselliğini kaybetmemesi koşuluyla kişisel verileri ortadan kaldırarak veya azaltarak ya da kişisel verilerin gereksiz ve/veya istenmeyen şekilde işlenmesini önleyerek gizliliği koruyan, tutarlı bir Bilgi İletişim Teknolojisi (BİT) önlem sistemi olarak tanımlanmaktadır. Bu kavram aynı zamanda veri koruma mevzuatı açısından da bir veri güvenliği tedbiri olarak kabul edilebilmektedir [37]. Gizlilik artırıcı teknolojiler, kişi veya kişi gruplarının gizliliğini korumayı amaçlayan teknik bir önlem sınıflandırmasıdır.

Gizlilik koruma modelleri Bilgi Teknolojisi dünyasında önleyici ve tespit edici teknolojiler kullanılarak gizliliğin korunmasına yönelik yapılan yeni bir kavram değildir. Bu konuda yeni teknolojiler kullanarak gizliliği korumak için çeşitli modeller araştırılmış ve önerilmiştir**.**

Etkin bir savunma uygulanabilmesi için en önemli başlıklardan biri de, bilginin gizliliği dikkate alınarak erişim yetkilerinin buna göre planlanması ve kullanıcıların bu konuda eğitilmesidir. Siber uzaydan gelen tehditlerin çoğunlukla insan odaklı olduğu, saldırı sistemlerinin insanların yapacakları hatalar üzerine inşa edildiği unutulmamalıdır.

Günümüzde en yoğun olarak kullanılan saldırı yöntemi olan sosyal mühendislik saldırılarına karşı en iyi savunma yöntemi, kullanıcıların bu konuda eğitilerek sürekli bilgilendirilmesidir. Binlerce kullanıcının olduğu bir sistemde bir kullanıcının yapacağı hata, diğer birçok kullanıcının da verisini tehlikeye atacaktır. Kullanıcı eğer sistem üzerinde kritik yetkilere sahip bir yetkili ise, saldırının etkisi de o derece fazla ve önlenmesi yine aynı oranda zor olacaktır.

4.8. Casus Yazılım Tespiti ve Sistemlerden Silme

Casus yazılım tespit sistemleri, mevcut işletim sistemleri için birçok farklı tipte tasarlanmış casus yazılımların tespiti, işlevlerinin durdurulması ve tamamen sistemlerden silinmesi için kullanılırlar. Antivirüs yazılımlarından farklı olarak casus yazılım tespit sistemleri zararlı ve zararlı olmayan yazılımlardan oluşan casus yazılımlar için kullanılırlar.

Casus yazılımların sistemlere girişlerinin engellenmesi sadece kullanıcının gizliliğinin korunmasını değil, aynı zamanda sistemlerin düzenli çalışmasını da sağlamaktadır. Casus yazılımların sistem üzerindeki etkisini engellemek için mutlaka casus yazılım tespit sistemleri kullanılmalı ya da üzerlerine casus yazılım tespit sistemleri eklenmiş anti virüs yazılımlar tercih edilmelidir.

Siber saldırganların daha tecrübeli hale gelmesi nedeniyle Kamu ve özel sektördeki güvenlik analistlerinin de saldırıları tespit ve önleme

yöntemlerinde daha tecrübeli ve zamanla yarışır hale gelecekleri düşünülmektedir [38].

4.9. Açıklık Tarayıcılar

Açıklık tarayıcıları ile bilgisayarlar, ağ bağlantıları, işletim sistemleri veya uygulama yazılımları kontrol edilerek buralardan kaynaklanabilecek açıklıklar nedeniyle sistemlerde oluşabilecek hasarların önceden tespit edilerek engellenmesi amaçlanır. Açıklık tarama programları ile yapılan tarama sonucunda oluşabilecek riskleri ortadan kaldırmak için bir raporlama yapılır. Bu raporlama ile tespit edilen aksaklıkların en kısa süre içinde giderilmesi hedeflenir.

Açıklık tarayıcıların sürekli işlevsel olarak tutulması ve buradan gelecek raporların hızla değerlendirilerek aksiyon alınması makro bazda alınacak önlemlerin başında gelmektedir.

4.10. Bal Küpü Sistemlerinin Tesis Edilmesi

Son yıllarda veri mahremiyeti kapsamında pek çok yeni çözümler geliştirilse de teknolojik gelişmeler, yapay zekâdaki ilerlemeler, derin öğrenme yaklaşımlarının uygulama başarısı, bu yaklaşımların pek çok alanda kullanılmaya başlanması ve yapısı itibariyle kara-kutu çözüm sağlaması, veri mahremiyeti açısından yeni endişeleri de beraberinde getirmiştir [39].

Kötü amaçlı yazılım sunucu vasıtasıyla yayılabilir, uygulamalara bulaşabilir ve diğer kullanıcılara geçebilir. Sanal ortamlar, sanal makineler arasında bir makineden daha fazla koruma sağlar, ancak yine de tamamen izolasyon sağlamazlar [40].

Bal küpü ya da bal çanağı sistemleri dahil oldukları ağlara yapılacak saldırıların tespit edilmesi için kurulmuş tuzak sistemlerdir. Bu görevi üstlenmiş sistemler geçerli bir servis sunmadıklarından, kendilerine yönlenen her türlü erişim şüpheli olarak kabul edilmekte ve inceleme altına alınmaktadır. Bal küpleri hali hazırda bilinen açıklıklar karşısında zayıf görünerek, bunları değerlendirmeye çalışan saldırganların tespitinde kullanılmaktadır. Güvenlik sistemlerini aşarak sistemlere girmeye çalışan saldırganlar, kasti olarak açıklıklar bırakılmış sistemlere yönlendirilerek tespit edilirler.

Bal küpü sistemlerinden yararlanılması, Ülke bazında alınacak en önemli makro önlemlerden biri olarak kabul edilmektedir. Bu sistemlerin özellikle kademeli olarak tesis edilmesi çok etkin bir güvenlik yapısı teşkil edecektir.

4.11. Saldırı veya Misilleme Tedbirlerinin Alınması

Siber güç: Siber uzayın, avantajlar elde etmek ve tüm harekât ortamlarında söz sahibi olmak amacıyla kullanılmasıdır. Bu tanımlama sadece ABD'de değil aynı zamanda birçok Avrupa ülkesinde de kara, hava, deniz ve uzaydan sonra siber uzay ordular için yeni harekât alanı olarak tanımlanmış ve bu konuda birçok ülkede resmi politikalar geliştirilmesinin önü açılmıştır**.** ABD Silahlı Kuvvetleri tarafından 5 Şubat 2013 tarihinde yayınlanan "Siber Uzay Harekâtları" dokümanında [41] siber uzayda yapılacak operasyonlar konusunda detaylı bilgilere ulaşmak mümkündür.

Saldırı amaçlı siber uzay harekâtlarında amaç, siber uzayda veya siber uzay imkânları kullanılarak güç tesis edilmesidir. Savunma amaçlı siber uzay harekâtlarında amaç, Savunma Bakanlığı ya da diğer dost olarak tanımlanan kurumlara ait siber uzay imkânlarının savunulmasıdır. Saldırı ve Savunma amaçlı harekatlar günümüzde Siber güvenlik konusunda en yoğun ve etkin kullanılan yöntemlerin başında gelmektedir.

V. SONUÇLAR VE TARTIŞMALAR (RESULTS AND DISCUSSIONS)

Bilişim suçları günümüzde istisnai bir suç işleme aracı olmaktan çıkmış, bilişim sistemlerine yönelik işlenen suçların yanında; sahtecilik, hakaret, dolandırıcılık, özel hayatın gizliliği ve kişisel verilere karşı suçlar gibi pek çok suç türü sıklıkla bilişim sistemleri aracılığıyla işlenen suçlar haline gelmiştir [42]. Büyük verinin elde edilmesinden yayınlanmasına kadar geçen süreç, bir büyük veri mahremiyeti koruma sürecini temsil eder. Bu süreç gerek tarafları gerekse de bu tarafların rollerini ve sorumluluğu altında gerçekleşen işlemleri kapsar [43].

Dijitalleşen dünyanın ürettiği önemli bir konsept olan Büyük veri, sosyal medyadan

güvenlik sistemlerine, sağlıktan finansa kadar pek çok alanda hayatın bir parçası haline gelmiştir. Veri büyük olunca üretilecek çıktıların değerinin de büyük olması beklenmektedir [44].

Önümüzdeki süreçte Siber Saldırıların hem sayısı hem de verdiği zararların boyutu giderek artacak ve yaşantımızın ayrılmaz bir parçası haline gelecektir. Çünkü yeni teknoloji ve mimari yapılar şebekeleri ile alt yapıların kontrolünde ve yönetimlerinde önemli ölçüde geleneksel yapıyı değiştirecektir. Bunun sonucu yakın gelecekte ülkeleri bekleyen ve onları en çok meşgul edecek önemli sorunların başında Siber saldırılar gelecektir. Çünkü günümüzde kritik altyapılara düzenlenen saldırılar sadece yazılımlara değil, donanımsal hasarlara da sebep olarak sistemlerin çalışmasını etkilemektedir. Bu nedenle makro düzeyde bu tür saldırılar karşısında meydana gelebilecek hasarlar da dikkate alınmalı ve ülke bazında yapılacak sistem yedeklemeleri bu çerçevede planlanmalıdır.

Doksanlı yıllardan günümüze kadar gelen ve artarak devam eden siber saldırıların gelecekte olası çatışmalarda büyük rol oynayacağı kesindir. Siber saldırıları nükleer saldırılar ile kıyaslamak doğru olmasa da, bu saldırılar özellikle kritik altyapılara yapıldığında artan düzeyde ulusların güvenliklerini tehlikeye atar boyutlara erişmektedir. Bu saldırıların ülkeler bazında yol açacağı hasarlar dikkate alındığında, Siber caydırıcılığın tesis edilebilmesi için siber uzayda bulunan aktörlerin iyi tanımlanması gerekir. Bu aktörler bir ülke olabileceği gibi bir terör grubu veya kendi başına hareket eden bir hacker ya da hacker grubu da olabilir. Bu nedenle Siber alanda saldırganın tespitinde ciddi zorluklar yaşanmakta, bu güçlükler caydırıcılığın tesisi konusunda ciddi soru işaretlerine yol açmaktadır.

Siber caydırıcılığın tesis edilebilmesinin şartlarından biri, siber caydırıcılığın nükleer caydırıcılıktan farklı olduğunun kabul edilmesidir. Çünkü sınırların belli olmadığı bir siber alanda tesis edilmeye çalışılacak siber caydırıcılığın, nükleer caydırıcılıkta olduğu gibi salt askeri yöntemler kullanılarak sağlanması olanaksızdır. Bu nedenle aktörlerinin çok farklı alanlardan olduğu siber uzayda gerek taktik, gerekse stratejik seviyede atılacak adımlar da buna göre planlanmalıdır. Teknik alanda yapılacak düzenlemeler ve alınacak tedbirler ile hem taktik seviyede caydırıcılığın sağlanabilmesi mümkün olabilir, hem de hukuki ve askeri yöntemlerinin geliştirilmesi halinde stratejik olarak caydırıcılığın tesis edilmesi temin edilebilir.

Halen siber uzayda cezalandırma korkusu sonucu oluşacak caydırıcılığın tesis edilmesi önündeki en büyük engel saldırı kaynağının bilinmemesi ve saldırgana ulaşılamamasıdır. Ancak 2014 yılında Amerika Birleşik Devletlerinin, Çin ordusu tarafından yapılan saldırılarda kişi ve yer belirterek saldırı kaynağını göstermesi, günümüzde bu konudaki bilinmezliğin de ortadan kalkmaya başladığını göstermektedir.

Bu nedenle günümüzde kaynağa ait doğru bilgilere ulaşılması saldırı ve misillemeyi gündeme getirmektedir. Bunun en güzel örneği 2015 yılında Çin, İngiltere ve ABD'nin birbirlerinin ticari sırlarına karşı siber saldırılarda bulunmayacakları konusunda anlaşmaya varmalarıdır. Bu konunun ülkeler arasında bir iyi niyet göstergesi mi olduğu, yoksa birbirleri üzerinde caydırıcı mekanizma oluşturma gayretimi içerdiği hususu, incelenmesi gereken ayrı bir konudur. Bu nedenle Ülkelerin Siber savunma veya saldırı yöntemlerinin geliştirilmesine sadece Silahlı Kuvvetlerin konusu olarak bakmayıp, sivil/asker işbirliği içinde ele alınması ve stratejiler geliştirilmesi gereken bir husus olarak değerlendirmek gerekir.

Alınacak tedbirlerle belirli saldırılar engellense bile, birçok ülkenin bu alanı stratejik savaş ortamı olarak görmesi nedeniyle bu konudaki güçlerini kaybetmek istemeyecekleri de açıktır. Bunun sonucu ülke kaynaklı saldırılarda uluslararası anlaşmalar olmadığı takdirde, önümüzdeki süreçte azalma olmayacağını söylemek mümkündür. Bu konuda kuvvetli ülkelerin sahip oldukları bu gücü kullanma isteği de çok açıktır.

Nükleer savaşla birlikte ortaya çıkmış caydırıcılık kavramı Hiroşima ve Nagazaki'ye atılan atom bombalardan sonra daha çok önem kazanmış ve o bombalar atılan ilk ve son bombalar olmuştur. Bugün Siber uzayda savaş

tüm hızıyla devam etmekte ve dünya ülkeleri halen uluslararası alanda hukuki bir çerçeve içinde anlaşmaya varamamaktadırlar. Bu nedenle dünya ülkelerinin bu konuda tüm çabaları, söz konusu anlaşmazlığın siber uzayda bir Hiroşima veya Nagazaki felaketi yaşanmadan son bulması olmalıdır.

Bu açıdan konuya bakıldığında sayılan önlemlerin alınması ve geliştirilmesi Ülkemizin siber güvenliği ile ilgili alınacak en rasyonel makro tedbirler olacaktır.

KAYNAKLAR (REFERENCES)

[1]. A. Nagurney, J. Dong, and P.L. Mokhtarian, "Multicriteria Network Equilibrium Modeling with Variable Weights for Decision-Making in the Information Age with Applications to Telecommuting and Teleshopping", Journal of Economic Dynamics & Control, 1629-1650, 2002.

[2]. E. Deniz, R. Samet, Nesnelerin İnternetinde Zigbee 3.0 Ağlarına Güvenli Katılım İçin Yeni Bir Model Önerisi, Uluslararası Bilgi Güvenliği Mühendisliği Dergis, Cilt:5, No:1, S:35-44 35, https://doi.org/10.18640/ubgmd.548157, Yıl 2019, Cilt 5 , Sayı 1, Sayfalar 35 – 45.

[3]. J. Zhou, Z. Cao, X. Dong and A. V. Vasilakos, "Security and Privacy for CloudBased IoT: Challenges," in IEEE Communications Magazine, vol. 55, no. 1, pp. 26-33, January 2017.

[4]. T. Acarer, Bilgi ve İletişim Sistemlerinde Eğilim Kitabı, Boyut Yayıncılık ve Tic. A.Ş, Sertika No:10855, ISBN:978-975-23-1200-5, İstanbul, 2017, S. 143.

[5]. İ. Kara, Web Tabanlı Zararlı Yazılımların Saldırı Yöntemleri ve Analiz Teknikleri, Uluslararası Bilgi Güvenliği Mühendisliği Dergisi, 2019, Vol:5, No:1, S:46-53.

[6]. S. Li, L. Da Xu, and S. Zhao, "The internet of things: a survey," Information Systems Frontiers, Vol. 17, No. 2, pp. 243-259, 2015.

[7]. Y. Canbay, Ş. Sağıroğlu, Nesnelerin İnternetinin Kişisel, Kurumsal ve Ulusal Bilgi Güvenliği Açısından İncelenmesi, Türkiye Bilişim Vakfı Bilgisayar Bilimleri ve Mühendisliği Dergisi, 2017, Cilt:10, Sayı:2, S. 28.

[8]. T. Çavdar, E. Öztürk "Nesnelerin İnterneti için Yeni bir Mimari Tasarımı" in Sakarya Üniversitesi Fen Bilimleri Enstitüsü Dergisi, 2017

[9]. A. Arış, S. Oktuğ, S. Yalçın "Nesnelerin İnterneti Güvenliği: Servis Engelleme Saldırıları" in Signal Processing and Communications Applications Conference, May 2015

[10]. L. Gökrem, M. Bozoklu "Nesnelerin İnterneti: Yapılan Çalışmalar ve Ülkemizdeki Mevcut Durum" in Gaziosmanpaşa Bilimsel Araştırma Dergisi Sayı:13, Aralık 2016.

[11]. M. Sain, Y. J. Kang, H. J. Lee "Survey on Security in Internet of things: state of the art and challenges" 2017.

[12]. Y. Yang, H. Peng, L. Li and X. Niu, "General Theory of Security and a Study Case in Internet of Things," in IEEE Internet of Things Journal, vol. 4, no. 2, pp. 592-600, April 2017.

[13]. A. Mosenia and N. K. Jha, "A Comprehensive Study of Security of Internet-of-Things," in IEEE Transactions on Emerging Topics in Computing, vol. 5, no. 4, pp. 586-602, 1 Oct.-Dec. 2017.

[14]. K. Gupta and S. Shukla, "Internet of Things: Security challenges for next generation networks," International Conference on Innovation and Challenges in Cyber Security, (ICICCS-INBUSH), Noida, 2016, pp. 315-318.

[15]. M. Önok, 2013. Marmara Üniversitesi Hukuk Araştırmaları Dergisi. Süleyman Demirel Üniversitesi Fen Bilimleri Enstitüsü Dergisi, Cilt 23, Sayı 1, 2019, S. 238-244.

[16]. Ulusal Siber Guvenlik Stratejisi 2016 - 2019, http://www.udhb.gov.tr/doc/siberg/2016-2019guvenlik. pdf, 2018.

[17]. L. Hansen and H. Nissenbaum, "Digital Disaster, Cyber Security, and the Copenhagen School", International Studies Quarterly, 2009, Cilt 53, 2011, P. 1155.

[18]. Findingdulcinea, On This Day: Robert Spreading Virus. http://www.findingdulcinea.com/news/on-this, 2018.

[19]. Findingdulcinea, On This Day: Robert Spreading Virus. http://www.findingdulcinea.com/news/on-this, 2018.

[20]. M.G. Todd, "Armed Attack In Cyberspace:Deterring Asymmetric Warfare With Anasymmetrıc Definition", Air Force Law Review, (2009), P.68.

[21]. T. Kimberly, et al. "The evolution of android Malware and android analysis techniques." ACM Computing Surveys (CSUR) 49.4, 2017, P. 76.

[22]. E. Masum, R. Samet "Mobil BOTNET İle DDOS Saldırısı", Bilişim Teknolojileri dergisi, Cilt 11, Sayı 2, Sayfalar 111-121, 2018.

[23]. M. A. Akyıldız, Uygulamalarla Siber Güvenliğe Giriş, Gazi Yayınevi, ISBN:9786053442745, 2015, S.585.

[24]. M. Alkan, Mayıs) Siber Güvenlik ve Siber Savaşlar, www.tbmm.gov.tr. Retrieved from https://www.tbmm.gov.tr/develop/owa/tbmm_internet.arama?q=sunumlar, 2012.

[25]. M. Gürkaynak, A. A. İren, "Reel Dünyada Sanal Açmaz: Siber Alanda Uluslararası İlişkiler", Süleyman Demirel Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi, 2011, Cilt 16, S.264.

[26]. Syrian Electronic Army Claims Responsibility For Hacking U.S. Army Website, Forbes, http://www.forbes.com/sites/katevinton/2015/06/08/syrian-electronic-army-claims-responsibilityfor-hacking-army-website/, 2015.

[27]. M. S. Schmidt & D. E. Sanger, China Army Face U.S. Charges of Cyberattacks, http://www.nytimes.com/2014/05/20/us/us-to-charge-chinese-workers-withcyberspying.html?_r=0, 2015.

[28]. J. Markoff, (2008), " Before the Gunfire, Cyberattacks", http://www.nytimes.com/2008/08/13/technology/13 cyber.html, 2011.

[29]. J. Davis (2007), "Hackers Take Down the Most Wired Country in Europe" http://www.wired.com/politics/security/magazine/15-09/ff_ estonia?currentPage=all, 27.05.2011, P.10.

[30]. T. L Thomas, "The Bear Went Through the Mountain: Russia Appraises its Five-Day War in South Ossetia", Journal of Slavic Military Studies, (2009), P.39.

[31]. C. Rhoads, "Kyrgyzstan Knocked Offline", http://online. wsj.com/article/SB123310906904622741.html , (2009).

[32]. H. K. Williams,& R. J. Mahncke, (2010), "International Relations and Cyber Attacks: Official and Unofficial Discourse", Australian Information Warfare and Security Conference Edith Cowan University, S.9.

[33]. S. Cantürk, "Bireysel Siber Farkındalık Araştırması" https://home.kpmg.com/tr/tr/home/gorusler/2018/05/bireysel-siber-farkindalik_arastirmasi.html, 2018.

[34]. E. Deniz, R. Samet, https://doi.org/10.18640/ubgmd.548157, Uluslararası Bilgi Güvenliği Mühendisliği Dergisi, Cilt:5, No:1, 2019, S. 35.

[35]. M. N. Öğün ve A. Kaya, Siber Güvenliğin Milli Güvenlik Açısından Önemi ve Alınabilecek Tedbirler, Güvenlik Stratejileri, Yıl: 9, 2013, Sayı: 18, S.178.

[36]. G. Giray, M.P. Uysal, Üniversitelerdeki yazılım mühendisliği öğretim programlarında teknik olmayan Becerilerin yeri: İlk sonuçlar. 11. Ulusal Yazılım Mühendisliği Sempozyumu: Alanya, Türkiye; 18/10/2017 - 20/10/2017.

[37]. O. Tahaoğlu, Personal Data Protection In Turkey: An Information Technology Framework Intended For Privacy Risk Management, Master's Thesis, Dokuz Eylül Univercity Graduate School of Naturel and Applied Sciences, 2009.

[38]. I. K. Aksakallı, Uluslararası Bilgi Güvenliği Mühendisliği Dergisi, 2019, Cilt:5, No:1, S:8-34.

[39]. Yavuz CANBAY, Derin Öğrenmede Diferansiyel Mahremiyet,Uluslararası Bilgi Güvenliği Mühendisliği Dergisi, https:/dergipark.gov.tr/ubgmd, Yıl 2020, Cilt:6, No:1, S:1.

[40]. Z. Tari, Yi X., U.S. Premarathe, P. Bertok, and I. Khalil, Security and Privacy in Cloud Computing: Vision, Trends, and Challenges, IEEE Cloud Computing published by The IEEE Computer Society, 2015.

[41]. Cyberspace Operations, Joint Publication 3-12 (R), http://www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf, Erişim 14.11.2015.

[42]. H. Bayrak, "Dünya'da İnternet Kullanımı ve Sosyal Medya İstatistikleri-2. Çeyrek Raporu", https://dijilopedi.com/dunyada-internetkullanımı-ve-sosyal-medya-istatistikleri-2-ceyrek-raporu/ Yıl.2018).

[43]. Y. Canbay, Y. Vural, Ş. Sağıroğlu, Politeknik Dergisi, *Politeknik Dergisi* , Mahremiyet Korumalı Büyük Veri Yayınlama İçin Kavramsal Model Önerileri, https://dergipark.org.tr/tr/pub/politeknik/issue/54737/535184, 2020, S. 792.

[44]. H. Chen, Chiang R.H., and Storey V.C., "Business intelligence and analytics: From big data to big impact", MIS, 36(4), 2012.