http://dergipark.ulakbim.gov.tr/tujes
Trakya University Journal of Engineering Sciences, 17(1): 13-21, 2016
ISSN 2147–0308
Araştırma Makalesi / Research Article

SİBER GÜVENLİKTE LİSANSÜSTÜ EĞİTİM: DENİZ HARP OKULU ÖRNEĞİ

Mehmet Bilge Kağan ÖNAÇAN[1], Hasan ATAN[2]

[1] Deniz Harp Okulu, Bilgisayar Mühendisliği, İstanbul
konacan@dho.edu.tr
[2] İstanbul Şehir Üniversitesi, Fen Bilimleri Enstitüsü, İstanbul
hasan.atan@outlook.com

Özet: İnternet kullanımının hayatın her alanında yaygınlaşmasına paralel olarak siber uzaydaki tehditlerin sayısında da artış gözlenmektedir. Kişi, kurum ve devletlerin siber uzaydaki saldırılardan maddi ve manevi etkilendiği ve zarara uğradığı görülmektedir. Bu tür zararlardan korunabilmek için siber güvenlik farkındalığının artırılması, bilgi ve bilinç seviyesinin yükseltilmesi gerekmektedir. Bunu başarmak için de hem son kullanıcıların bilgilendirilmesi ve bilinçlendirilmesini hem de siber güvenlik alanında nitelikli, uzman personel ihtiyacının karşılanmasını sağlayacak eğitim ihtiyacı ortaya çıkmaktadır. Bu çalışmada dünyadaki, ABD'deki ve Türkiye'deki Siber Güvenlik eğitimleri incelenmekte ve Deniz Harp Okulu (DHO)'ndaki Siber Güvenlik Yüksek Lisans Programı hakkında bilgi verilmektedir. Anılan programın siber güvenlik alanında özellikle uzman personel yetiştirilmesine önemli katkı sağlayacağı değerlendirilmektedir.

Anahtar Kelimeler: Siber Güvenlik Eğitimi, Siber Güvenlik Uzmanı, Siber Tehdit, DHO DEBİM, Müfredat.

Graduate Education in Cyber Security: The Case of Naval High School

Abstract: It is observed that an increase in the number of threats in cyber space in parallel with widespread usage of internet in all areas of life. It is seen that people, corporations and governments are being affected and suffered from the attacks on cyber space financially and morally. To be protected from cyber attacks, it is required to increase the level of knowledge, consciousness and awareness about cyber security. In order to manage this, the need of education for both the last users and the qualified specialists is arised. In this study, the cyber security educations in the World, USA and Turkey are analysed and information about cyber security master program in Turkish Naval Academy is given. It is evaluated that the mentioned program would provide the important contribution to educate especially the qualified specialists in the area of cyber security.

Keywords: Cyber Security Education, Cyber Security Specialist, Cyber Threats, DHO DEBIM, Curriculum.

GİRİŞ

Tüm dünyada internet kullanım oranı son yıllarda hızlı bir şekilde artmaktadır. Türkiye de internetin bu hızlı büyümesinden payını almıştır. Kişi başına düşen bilgisayar ve internet kullanım oranı dünyanın birçok ülkesi gibi Türkiye'de de hızla artmaktadır. Uzmanlar, sonraki dönemde de bu artışın devam edeceğini değerlendirmektedir.

İnternet kullanımının bu denli artması ve özellikle sosyal medya başta olmak üzere birçok internet platformlarında her türlü bilginin paylaşılıyor olması gizlilik, mahremiyet ve içeriği suç teşkil eden problemleri de beraberinde getirmektedir. Kaspersky Lab tarafından yürütülen "2013 Finansal Siber Tehditler" çalışmasına göre Türkiye özellikle finansal siber suçların oranının en fazla olduğu ülkeler arasında yer almaktadır (Kaspersky Lab, 10 Nisan 2014).

İnternet kullanımının ve internet platformlarında işlenen suçların gün geçtikçe artması, bilgi güvenliğine daha fazla önem verilmesini zorunlu kılmaktadır. Kişi, kurum ve devletlerin bu platformlarda işlenen her türlü illegal fiillerden maddi ve manevi etkilenmemesi için gereken önlemlerin alınması gerekmektedir. Bu önlemlerin başında hem son kullanıcıların siber güvenliğe ilişkin olarak bilgilendirilmesi ve bilinçlendirilmesi hem de siber güvenlik alanında nitelikli personel ihtiyacının karşılanması gelmektedir. Bunun için eğitime ve eğiticilere ihtiyaç duyulmaktadır. Türkiye'de bilgi teknolojilerine ilişkin eğitimler veren birçok eğitim programı bulunmakla birlikte siber suçlar konusunda derinleşmiş uzman sayısı sınırlıdır oysa siber suçlarla mücadele özel eğitim (Varol, 8-10 Aralık 2015:1) ve uzmanlaşmış eğiticiler gerektirmektedir.

Türkiye'de birçok kamu ve özel kurumun siber suçlarla mücadele için siber güvenlik alanında nitelikli personele ihtiyacı bulunmaktadır. Bu ihtiyacı karşılamaya yönelik son yıllarda hem üniversitelerde hem de özel eğitim kurumlarında eğitim programları hazırlanmakta ve verilmektedir. Bu kapsamda gerek Türk Silahlı Kuvvetlerinin gerekse ülkemizin diğer kurumlarının/firmalarının ihtiyaç duyabileceği nitelikli personel ihtiyacını karşılamak amacıyla 2015 yılında Deniz Harp Okulu (DHO)'nda Siber Güvenlik Yüksek Lisans programı açılmıştır. Söz konusu

programın yanı sıra, siber güvenliğe ilişkin farkındalığın artırılmasına yönelik faaliyetlere de devam edilmektedir.

Bu makalenin ikinci bölümünde siber uzay, siber tehdit, siber savaş ve siber güvenlik kavramları açıklanmış, üçüncü bölümünde siber güvenlikte eğitimin önemi ile dünyadaki, ABD'deki ve Türkiye'deki eğitim faaliyetleri anlatılmış, dördüncü bölümünde DHO'ndaki Siber Güvenlik Yüksek Lisans Programı hakkında detaylı bilgi verilerek siber güvenliğe ilişkin farkındalığın artırılmasına yönelik faaliyetler özetlenmiş, son bölümünde sonuç ve değerlendirmeler sunulmuştur.

SİBER GÜVENLİĞE İLİŞKİN TEMEL KAVRAMLAR

Tüm dünyada olduğu gibi Türkiye'de de bilgisayar ve internet kullanımı son yıllarda önemli ölçüde yaygınlaşmaktadır. TÜİK Hane halkı Bilişim Teknolojileri Kullanım Araştırması'na göre Türkiye'de 16-74 yaş grubundaki bireylerde bilgisayar ve internet kullanım oranları, 2014 yılında sırasıyla %53,5 ve %53,8 iken bu oranlar 2015 yılı Nisan ayında sırasıyla %54,8 ve %55,9 olmuştur (TÜİK, 2015) . Bunun yanında Türkiye'de internet kullanım oranlarının 4.5G teknolojisinin yaygınlaşması ile beraber daha da artacağı değerlendirilmektedir.

İnternet kullanımının her geçen gün artmasıyla birlikte bu ortamda her türlü bilgi paylaşılır olmuştur. Bilgi çağının en önemli gücünün bilginin kendisi olduğu göz önünde bulundurulursa bilgi casusluğu, siber korsanlık vb. yasadışı eylemlerde ve siber uzaydaki tehditlerde her geçen gün artış gözlemlenmektedir. Son dönemlerde ise siber savaşlar gündemden düşmemektedir. Çıkabilecek bir üçüncü dünya savaşının siber uzayda yaşanması ihtimali uluslararası politikayı da şekillendirmektedir (Bıçakçı, 2014: 103). Bu sebeple siber güvenlik konusunda gereken önlemleri almak ve olası zararlara karşı hazırlıklı olmak gerekmektedir.

Siber Uzay

Siber uzay, tüm dünyaya ve uzaya yayılmış durumda bulunan bilişim sistemlerinden ve bunları birbirine bağlayan ağlardan oluşan veya bağımsız bilgi sistemlerinden oluşan sayısal ortamı (UDHB, 2016: 7) ifade etmektedir. En genel anlamda, insanların birbirine bağlı bilişim sistemleriyle etkileştiği ve birbirine bağlı bilişim sistemlerinin birbirleri arasında ya da insanlarla iletişim içinde olduğu fiziksel olmayan alan siber uzay olarak tanımlanmaktadır. Araştırmacılardan birçoğu sadece internet ortamına bu ismin verilmesinin uygun olduğunu düşünmektedir. Oysaki siber uzay bütün bilişim sistemlerini ve kullanıcıları içine alan bir evrendir (Bıçakçı, 2014: 106).

Günümüzde neredeyse tüm haberleşme, bilgisayarlar üzerinden siber uzayda gerçekleşmektedir. E-devlet uygulamalarında, enerji altyapılarında, ticari alanlarda, savunma sanayinde, finans sektöründe ve bunun gibi akla gelebilecek her türlü alanda bilgisayarlara, bilgisayar ağlarına ve uygulamalarına duyulan ihtiyaç günden güne artmakta ve bununla doğru orantılı olarak da siber uzay büyümekte ve paralelinde ise siber güvenliğin önemi gitgide artmaktadır. Kişi başı kullanılan internet cihazı sayısının eskiye nazaran bir hayli artması ve nesnelerin interneti (internet of things- IoT) kavramının da literatüre girmesiyle beraber önümüzdeki yıllarda internet kullanımının bir hayli artacağı tahmin edilmektedir. İnternet ağına yönelik ürünler geliştiren Cisco'nun tahminlerine göre hali hazırda kullanılmakta olan internete bağlı cihazlar ve önümüzdeki yıllarda bağlanacak olan cihazların toplamının 2020'li yıllarda 40 milyarı bulması beklenmektedir (Akın, 2015). Bunun sonucu olarak da insan sayısının yaklaşık yedi milyar olduğu dünyamızda kişi başına düşen internete bağlı cihaz sayısının ortalama altı olacağı değerlendirilmektedir. İnternete olan bağımlılığın bu denli hızla arttığı düşünüldüğünde yakın gelecekte kişisel mahremiyetin ve siber güvenliğin öneminin de hızlı bir şekilde artış göstereceği öngörülmektedir.

Siber Tehdit

Dünyanın en hızlı büyüyen ve en büyük siber güvenlik şirketlerinden biri olan Kaspersky Lab tarafından yapılan "2013 Finansal Siber Tehditler" çalışmasına göre siber suçluların, kişisel çevrimiçi hesaplara erişimi giderek artmaktadır. 2013 yılında, kötü amaçlı finansal yazılımların kullanıldığı siber saldırıların sayısı bir önceki yıla göre %27,6 artışla 28,4 milyona yükselmiştir. Türkiye, Afganistan, Bolivya, Peru, Kamerun, Moğolistan, Myanmar, ve Etiyopya'da yaşanan finansal siber suç vakaları toplam rakamın %12'sinden fazlasını oluşturmaktadır (Kaspersky Lab, 2014).

Siber uzayda yer alan her türlü bilgi, yazılımsal ve donanımsal kaynaklar gibi her türlü hizmet aracı bu ortamdaki varlıkları ifade etmektedir. Örneğin bir kurumdaki her personelin e-posta kullanıcı adı ve şifresi, o personele ait varlıkları ifade etmektedir. Siber uzayda yer alan her türlü insani ve yazılımsal açıklıklar vasıtasıyla varlıklara erişim, varlıkların niteliğinin değiştirilmesi, varlıklara zarar verilmesi vb. sağlayan etkenler ise "siber tehdit" olarak ifade edilmektedir. Sıklıkla karşılaşılan siber tehditlere örnek olarak servis dışı bırakma saldırıları (denial of service- DOS), virüs, solucan vb. zararlı yazılımlar, zararlı e-postalar ve yetkisiz erişim saldırıları verilmektedir (Bıçakçı, 2015; Güngör, 2015).

Söz konusu siber tehditlerin yıkıcı etkilerine karşı bireyler, kurumlar ve devletler tarafından alınabilecek bir takım önlemler bulunmaktadır (Öğün ve Kaya, 2013; Yılız, 2014; Bayoğlu, 2016). Bu önlemler kısaca aşağıdaki şekilde sıralanabilmektedir:

- Ulusal politika ve stratejiler geliştirilmeli ve gerekli yasal ortam oluşturulmalıdır (Yılmaz ve Sağıroğlu, 2013: 158).

- Kişisel mahremiyetin sağlanması maksadıyla kişilerde bilgi güvenliği farkındalığının arttırılması sağlanmalıdır (Yılmaz ve Sağıroğlu, 2013: 159). Bu amaçla özellikle ilköğretimde, internet ile çok hızlı bir şekilde tanışan çocuklara bilgi güvenliği farkındalığı kazandıracak dersler verilmelidir. Nitekim bilgisayarlar ve internet hayatın ayrılmaz bir parçası olmuş durumdadır ve "Z Nesli" olarak adlandırılan kuşak gelişen teknolojinin tesirinde büyümektedir.

- Ülkelerin siber savunmasını gerçekleştirebilmek amacıyla Siber Savunma Birimleri kurulmalı ve çalışma alanları belirlenmelidir.

- Her türlü yabancı yazılıma (buna işletim sistemleri de dahil) önyargı ile bakılmalı ve yerli yazılımların geliştirilmesi için gereken teknolojik hamleler gerçekleştirilmelidir (Türkay, 20 Nisan 2016).

- Siber Güvenlik için milli çözümler üretilmeli, eğitim ve koruma hizmeti verilmelidir (Türkay, 20 Nisan 2016). Kurumların network, sistem ve güvenlik altyapısında kullanılan güvenlik duvarları, saldırı tespit sistemleri, network cihazları vb. cihazların yazılım ve donanımları yerli imkanlarla geliştirilmelidir.

- Ülke çapında siber güvenlik tatbikatları yapılmalıdır (UDHB, 2013)

- Kişisel bilgisayarlarda yazılım güncellemelerinin yüklenmesi, anti-virüs uygulamalarının çalıştırılması vb. önlemler alınmalıdır (Bayoğlu, 2016).

- Ülkelerin siber güvenliğini sağlayabilecek nitelikli personel yetiştirilmesi amacıyla üniversitelerde siber güvenlik eğitimleri yaygınlaştırılmalı, siber güvenlik konusunda akademisyenler yetiştirilmelidir (UDHB, 2013).

Bu kapsamda Türkiye'de bu güne kadar gerçekleştirilen ve gerçekleştirilmeye devam edilen önemli faaliyetler şu şekilde sıralanabilir:

- TSK Siber Savunma Merkezi Başkanlığı kurulmuştur (2012) (Oğuz vd., 2015: 1-5).

- TUBİTAK Siber Güvenlik Enstitüsü kurulmuştur (2012) (Oğuz vd., 2015: 9).

- Ulaştırma, Denizcilik ve Haberleşme Bakanlığı bünyesinde Siber Güvenlik Kurulu oluşturulmuştur (2012) (BTK, 2013: 6).

- Ulusal Siber Olaylara Müdahale Merkezi kurulmuştur (2013) (Bıçakçı vd., 2015: 14).

- Çeşitli kamu, özel ve sivil toplum kuruluşlarının ortaklaşa katkısıyla Siber Güvenlik tatbikatları düzenlenmiştir (2014) (Bıçakçı, 2014: 126).

- Ulusal Siber Güvenlik Stratejisi ve 2016-2019 Eylem Planı oluşturulmuştur (2016) (UDHB, 2016: 6).

- Çeşitli devlet ve özel üniversitelerde siber güvenlik bölümleri açılmıştır.

Siber Savaş

Siber savaş, bir devletin, başka bir devletin bilgisayar sistemlerine veya ağlarına hasar vermek ya da kesinti yaratmak üzere gerçekleştirdiği sızma faaliyetleridir (Mil, 2015: 400). Bir başka ifade ile siber savaş, bilgisayar ve iletişim teknolojisinin saldırı ve savunma amaçlı olarak kullanılmasıdır (Yayla, 2014: 182). Günümüzde savaşların sadece harp meydanlarında değil siber uzayda da gerçekleşiyor olması, olası 3. Dünya Savaşı'nın en önemli cephelerinden birinin siber cephe olacağı ihtimalini de güçlendirmektedir. Siber uzayda dünya çapında şu ana kadar gerçekleşen siber savaşlara; 2007 yılında Rusya-Estonya Siber Savaşı, 2008 yılında Rusya-Gürcistan Siber Savaşı, 2010 yılında Wikileaks belgelerinin internete sızdırılması, yine 2010 yılında İran nükleer çalışmalarını engellemeye yönelik üretilen Stuxnet Solucanı ve özellikle Google'a karşı düzenlenen Aurora saldırıları, 2012 yılında Türk Hava Yolları (THY)'na yönelik saldırılar, 2015 yılında Türkiye'nin Rusya'nın uçağını düşürmesi sonucu Türkiye-Rusya arasında gerçekleşen siber saldırılar örnek olarak gösterilebilir (Emre, 2012). Birçok ülke günümüzde yaşanan ve gelecekte de artacak olan siber tehditlere karşı kendisini müdafaa etmek amacıyla gerek istihbarat teşkilatları gerekse özerk kurum bünyelerinde siber güvenlik birimleri kurmakta ve bu alanda faaliyetlerini artırmaktadırlar.

Siber tehlikeler, siber saldırı ve siber savaşlarla sınırlı değildir. İşin mahremiyet ve hukuki boyutlarını da unutmamak gerekmektedir. İnsanların sanal ortamda rahat hareket edebilmesi, her türlü hakaret ve yorum yazabilmesi sonucunu doğurmuştur. Bunun ise çeşitli hukuki yaptırımları mevcuttur. Bunun yanında sosyal platformlarda herkese açık paylaşılan verilerin artması insanların mahrem bilgilerinin farkında olmadan saldırganların eline geçmesine sebep olabilmektedir. Bilgileri ele geçiren saldırganlar bu bilgilerle kişilere sosyal mühendislik saldırılarında bulunabilmektedirler. Bütün bunlara ek olarak özgür bir ortam sunduğu ve çok daha büyük bir kitleye ulaşabildiği gibi gerekçelerle internetin çeşitli platformlarında suç içerikli eylemler gerçekleştirilmektedir. Bu türden faaliyetler ise özellikle sansürsüz ve özgür internet sağladığı düşünülen Dark-Net (Tor-Network) bünyesinde gerçekleştirilmektedir. Dark-Net'in insanlara her türlü suçun rahatça işlenebileceği bir ortam sunduğu düşünülmektedir. Dark-Net bünyesinde; Firefox, Chrome, İnternet Explorer vb. tarayıcılarla erişilemeyen ve sadece Tor Tarayıcı ile erişim sağlanan, internetin gizli bir katmanı olarak düşünülebilir. Bünyesinde uyuşturucu ticareti, kor-

san yayıncılık, çocuk pornografisi, kiralık katil siteleri vb. aklınıza gelebilecek her türlü illegal içeriği barındırmakta ve bu türden illegal işlerin izlenemeden yapılabildiği bir ortam olduğu düşünülmektedir. Fakat The Dark Net kitabının yazarı Jamie Bartlett Eylül 2015 TEDTalks konferansında Dark-Net'in Amerikan Deniz Kuvvetleri'nin istihbarat projesi olarak geliştirildiğini ve sonradan yaygınlaştırıldığını söylemesi üzerine, Dark-Net üzerinden yapılan illegal işlerin izlenemediği düşüncesinin de yanlış olduğu kanaati ortaya çıkmıştır (Bartlett, 2015). Ayrıca bu iddia ABD'nin istihbarat çalışmaları kapsamında siber uzaya verdiği önemi de göstermektedir.

Diğer taraftan yeni geliştirilen teknolojinin ilk kullanıldığı alanlardan biri olan, bilginin ve hızlı karar almanın önem taşıdığı savaş ortamında bilgisayar ve iletişim teknolojileri yoğun olarak kullanılmaktadır. Günümüz savaş sahasında siber ortamın güvenliğini sağlamak, aynı zamanda bu alanı kullanarak düşmanın silah sistemlerini etkisiz hale getirmek için devletler önemli çalışmalar yürütmektedirler (Yayla, 2014: 182). Savaş harekat ortamında kullanılan savaş yönetim sistemleri ve sensör sistemleri çoğunlukla ileri teknoloji ürünü elektronik sistemlerdir. Siber saldırılara açık olan söz konusu sistemlerin siber saldırıya maruz kalma olasılığı yüksektir. Bu sebeple anılan sistemlerin kullanıcısı ve yöneticisi olan Silahlı Kuvvetler personelinin siber güvenliğe ilişkin bilgi ve bilinç seviyesinin yüksek olması gerekmektedir.

Görülüyor ki internetin bu denli yaygınlaşması her türlü, söz ve fiilin siber uzayda rahatça gerçekleştirilmesine, mahremiyet içeren bilgilerin elden ele dolaşmasına, suç içerikli eylemlerin daha rahat gerçekleştirilmesine sebep olmaktadır. Bütün bunlar ise siber güvenlik, siber hukuk, bilgi güvenliği farkındalığı ve siber uzayda mahremiyet gibi konuların gitgide önem kazanmasına vesile olmaktadır. Bu konularda gerekli önlemlerin alınması ve yatırımların yapılması gerek kişilerin ve kurumların, gerekse devletlerin geleceği açısından önemlidir.

Siber Güvenlik

Siber Uzay'ın her geçen gün büyümesi ve her türlü siber tehdide açık olması siber ortamda güvenliğin önemini arttırmaktadır. Siber güvenlik, siber ortamı oluşturan bilişim sistemlerinin saldırılardan korunmasını, bu ortamda işlenen bilginin gizlilik, bütünlük ve erişilebilirliğinin güvence altına alınmasını, saldırıların ve siber güvenlik olaylarının tespit edilmesini, bu tespitlere karşı tepki mekanizmalarının devreye alınmasını ve sonrasında ise sistemlerin yaşanan siber güvenlik olayı öncesi durumlarına geri döndürülmesini ifade etmektedir (UDHB, 2016). Siber güvenlik ifadesi ilk olarak 1990'lı yıllarda bilgisayar mühendisleri tarafından, ağa bağlı bilgisayarlarla ilgili güvenlik sorunlarını ifade etmek için kullanılmıştır (Öğün ve Kaya, 2013: 163).

Siber güvenlik kavramı açıklanırken, sıklıkla birlikte bahsedildiği ve zaman zaman da karıştırıldığı bilgi güvencesi (information assurance), bilgisayar güvenliği (computer security) ve bilgi güvenliği (information security) kavramlarına burada değinmenin faydalı olacağı değerlendirilmektedir. Bilgi güvencesi, siber güvenliği; siber güvenlik de bilgisayar güvenliğini kapsayan kavramlardır. Bilgi güvencesi; bilginin ve bilgi sistemlerinin gizliliğini, kontrolünü, bütünlüğünü, doğruluğunu, hazır bulunurluğunu ve işe yararlılığını sağlayacak şekilde tasarlanan teknik ve yönetimsel kontroller kümesidir. Bilgisayar güvenliği ise bilgisayarın üzerindeki bilgi sistem varlıklarının ve bilginin gizliliğini, bütünlüğünü ve kullanılabilirliğini sağlayan önlemler ve kontrollerdir (McGettrick, 2013: 11-14). Bilgi güvenliği, bilgilerin izinsiz kullanımından, izinsiz ifşa edilmesinden, izinsiz yok edilmesinden, izinsiz değiştirilmesinden, bilgilere hasar verilmesinden korunma veya bilgilere yapılacak olan izinsiz erişimleri engelleme işlemidir ("Bilgi Güvenliği", 2016). Bilgi güvencesinde, bilgi sistemindeki bilgi güvenliğini sağlamak için gerekli olan teknik ve süreçsel gereksinimler daha stratejik düzeyde ele alınırken bilgi güvenliği kavramı ise daha taktik düzeyde bir anlam içermektedir (Güngör, 2015: 10).

Ülkeler arasındaki siber savaşlar, kişisel mahremiyeti alt üst eden casus yazılım ve sosyal platformlar, ticaret hacminin önemli bir oranının internet üzerinden dönmesi, hastane/eczane vb. her türlü tıbbi ortamın verilerinin internette yer alması, endüstriyel alanda birçok hizmetin internet üzerinden dönmesi, enerji altyapılarında bilgisayar ve SCADA sistemlerine olan bağımlılık, kısacası hayatımızın her safhasında bilgisayarların ve bilgisayar altyapılarının yer alması bizi yaşadığımız yüzyılda en büyük ekonomik ve güvenlik tehditlerinin siber uzayda gerçekleşeceği sonucuna ulaştırmaktadır. Siber uzayda yaşanacak bu nevi tehditler siber güvenliğin ve siber güvenlik eğitiminin önemini her geçen gün artıracaktır.

SİBER GÜVENLİK EĞİTİMİ

Teknoloji çağında bilgisayarlar, akıllı telefon ve uygulamaları, sosyal medya gibi hayatı kolaylaştıran her türlü gelişme beraberinde güvenlik ve mahremiyet problemlerini de getirmiştir. Bu problemler sadece bireyleri değil, yeri geldiği zaman tüm toplumu ve ulusal güvenliği tehdit eder boyutlara kadar ulaşabilmekte, bireylere, topluma ve devlete maddi ve manevi zararlar verebilmektedir. Bilgi toplumunun yaşadığı bu problemleri minimize etmek amacı ile her bireyin ve kurumun bilgi güvenliği farkındalığının artırılması gerekmektedir. Söz konusu farkındalığı sağlayabilmenin, siber tehditler ve bu tehditler neticesinde oluşan problemleri önlemenin veya en azından etkisini azaltmanın en etkin yollarından biri de eğitimdir. Gerek bireysel olarak bireyin kendisini

gerekse kurumsal olarak kurum personelini siber güvenlik konusunda eğitmek ve güncel bilgilerle donatmak artık kaçınılmaz hale gelmiştir (Öğün ve Kaya, 2013:173).

Diğer taraftan hem siber güvenlik eğitimlerini verebilecek hem de siber tehlikelerle mücadele edebilecek ve siber savaşlarda etkin rol alabilecek nitelikli personel ihtiyacı ortaya çıkmıştır. Bu bağlamda çeşitli özel eğitim kurumlarında ve üniversitelerde bu konu teknik ve sosyal boyutları ile birlikte işlenmeye, tartışılmaya ve araştırılmaya başlamıştır. Ülkemizde bu konuda kişisel ve kurumsal eğitim veren özel kurumlar bulunmakla beraber son yıllarda ihtiyaç duyulan nitelikli eleman sayısını arttırmak ve siber dünyada doğabilecek tehditlere çözümler sunabilmek amacıyla çeşitli özel ve devlet üniversitelerinde de Siber Güvenlik üzerine çalışmalar yoğunlaşmıştır.

Bilgisayar eğitimcileri, bilgisayar araştırmacıları ve profesyonellerinin alandaki zorluklar, yenilikler ve eğitim müfredatlarına ilişkin düşüncelerini paylaştıkları, bilgisayar bilimleri alanındaki en eski ve en geniş mesleki kuruluş olan (ACM Digital Library, 2016) Hesaplama Makineleri Derneği (Association for Computing Machinery), kısaca ACM'nin 2013 yılında hazırlamış olduğu "Siber Güvenlik Eğitim ve Öğretimi için Müfredat Kılavuzu"nda siber güvenlik dersine ilişkin müfredatın ana konuları/bilgi alanları;

- Adli bilişim (digital forensics)
- Penetrasyon testleri (penetration testing)
- e-Kanıt (e-evidence)
- Hudut savunma (perimeter defense)
- Güvenli yazılım geliştirme ve yazılım güvenliği (secure coding and software security)
- Güvenlik yönetimi (management of security)

olarak belirlenmiştir (McGettrick, 2013: 14). Bilgi güvenliği alanına odaklanmış bir araştırma firması olan Securosis ise "bilgi güvenliği"ni;

- Ağ güvenliği (network security)
- Uç/son nokta/kullanıcı güvenliği (endpoint security)
- Veri güvenliği (data security)
- Uygulama güvenliği (application security)
- Kimlik ve erişim yönetimi (identity and access management)
- Güvenlik yönetimi (security management)
- Sanallaştırma ve bulut (virtualization and cloud)

olarak yedi alt kategoriye ayırmış ve ardından bu kategorileri 32 alt başlığa bölmüştür (Securosis.com, 2016).

Kessler ve Ramsay (2014), Milli Güvenlik programı için yapmış oldukları siber güvenlik eğitimi müfredat önerisinde; "Bilgi Güvenliğinin Temelleri", "Bilgisayar ve Ağ Teknolojileri", "Bilgi Güvenliği Araçları ve Teknikleri", "Adli Bilişime Giriş", "Siber Suç ve Siber Hukuk" ve "Siber Uzayda Savaş, Terörizm ve Diplomasi" olmak üzere altı temel ders belirlemişlerdir.

Dünyadaki ve ABD'deki Siber Güvenlik Eğitim Faaliyetleri

Siber uzayda yaşanan vakaların ve siber tehditlerin her geçen gün artması tüm dünya ülkelerini olumsuz etkilemektedir. Yaşanan olumsuzlukları asgariye indirgeyebilmek için ise nitelikli personel ihtiyacının karşılanması gerekmektedir. Bu amaçla dünyanın çeşitli bölgelerinde birçok ülke üniversiteler bünyesinde siber güvenlik eğitimi vermektedirler. Bu ülkeler ve üniversitelere Estonya'da Tallinn University of Technology, Avustralya'da Edith Cowan University, İskoçya'da Edinburgh Napier University, Hollanda'da 3TU (Dutch Technical Universities – TU Delft, TU Eindhoven, University of Twente), Hindistan'da Amrita Vishwa Vidyapeetham, İngiltere'de City University of Londan, De Montfort University, University of York örnek olarak sıralanabilir. Dünyada siber güvenlik alanında yüksek lisans düzeyinde eğitim veren bu üniversitelerin geniş bir listesine Wikipedia Master of Science in Cyber Security (https://en.wikipedia.org/wiki/Master_of_Science_in_Cyber_Security) başlığı altında erişilebilmektedir.

Bunların dışında ABD'de de çok sayıda kamu ve özel üniversitelerde siber güvenlik alanında eğitimler verilmektedir. 2014 yılında HP Enterprise Security sponsorluğunda Ponemon Institute tarafından yapılan "Siber Güvenlik için En İyi Okullar- Best Schools for Cybersecurity" araştırmasına göre ABD'de siber güvenlik alanında eğitim veren en iyi üniversiteler;

- University of Texas, San Antonio,
- Norwich University,
- Missisipi State University,
- Syracuse University,
- Carnegie Mellon University,
- Purdue University,
- University of Southern California,
- University of Pittsburgh,
- George Mason University,
- West Chester University of Pennsylvania,

- U.S. Military Academy, West Point,
- University of Washington

olarak gösterilmektedir. Araştırma yapılırken dikkate alınan kriterler ise akademik mükemmellik, uygulama imkanları, fakültenin tecrübe ve uzmanlığı, öğrenci ve mezunların altyapı ve tecrübesi, üniversite siber güvenlik komitesinin alandaki itibarı olarak sıralanabilir (Ponemon Institute, 2014).

Bunların dışında açık kaynaklardan yapılan araştırmalar sonucu özellikle ABD Harp Okulları incelendiğinde, ABD Deniz Harp Okulu'nda Siber Harekat (Cyber Operations) Ana Bilim Dalı'nın kurulduğu, diğer Harp Okullarında siber güvenlik kapsamında bölüm bulunmadığı görülmektedir. ABD'deki tüm Harp Okullarında öğrencilerin oluşturduğu çalışma gruplarının mevcut araştırma merkezlerinden yararlanarak Siber Harekat kapsamında araştırma ve proje çalışmaları yapmaları teşvik edilmektedir. Ayrıca ABD Deniz Harp Okulu'nda birinci sınıfta tüm öğrencilere siber güvenlik dersi verilmekte olduğu, her yarıyıl konferanslar yapıldığı ve sınavlara iştirak edildiği bilinmektedir.

ABD'deki tüm üniversiteler siber güvenlik alanında artan personel ihtiyacını karşılamak maksadıyla genel olarak lisansüstü ve sertifikasyon programları ile iyi eğitimli mezunlar yetiştirmeyi amaçlamaktadır. Sertifika ve lisansüstü programların yanında Maryland Üniversitesi gibi bazı üniversitelerin siber güvenlik lisans programı da bulunmaktadır ("Cybersecurity Education at UMD", 2016).

Türkiye'de Siber Güvenlik Eğitim Faaliyetleri

Siber tehditlerin günden güne artması siber güvenlik uzmanlarına duyulan ihtiyacı da günden güne artırmaktadır. Bu konuda ihtiyaç duyulan nitelikli personelin yetiştirilmesi maksadıyla ülkemizde çeşitli üniversiteler siber güvenlik alanında eğitim vermeye başlamışlardır. Henüz lisans düzeyinde ülkemizde bu eğitim verilmese de doktora ve yüksek lisans düzeyinde eğitimler verilmektedir. Araştırmacılar tarafından;

- Doktora derecelerinin, gelecek nesil siber güvenlik eğitimi ve akademik araştırmalarını desteklemekle birlikte endüstri ve devlet kurumları için ihtiyaç duyulan ileri derecede uzmanlığı ve liderliği sağlayacağı;
- Yüksek lisans derecelerinin ise, gelişmiş yeteneklere sahip siber güvenlik işgücü sağlamak için esas teşkil ettiği, bilgisayar biliminde veya ilişkili bir alanda yapılan sağlam bir lisans derecesi üzerine inşa edilen, iki yıllık ek eğitimin, siber güvenliğe ilişkin ileri konularda özel bilgi, beceri ve yetenek sağlayacağı ifade edilerek üniversitelerin bilgisayar profesyonelleri için, hukuk, işletme, ekonomi vb. toplumsal konular için ve siber güvenlik operasyonları için yüksek lisans programları açması gerektiğine vurgu yapılmaktadır (McGettrick, 2013: 2-3).

Bu kapsamda Siber Güvenlik alanında ülkemizde eğitim veren üniversiteler ve ilgili programlardan bazıları şu şekilde listelenebilir:

- DHO Deniz Bilimleri ve Mühendisliği Enstitüsü (DEBİM)'nde Siber Güvenlik Yüksek Lisans Programı
- Hava Harp Okulu Havacılık ve Uzay Teknolojileri Enstitüsü (HUTEN)'nde Siber Güvenlik Yüksek Lisans programı
- TÜBİTAK'ın üniversiteler ile siber güvenlik konusunda eğitim programları yürüttüğü; BİLGEM ve Şehir Üniversitesi ortaklığı çerçevesinde, Şehir Üniversitesi Fen Bilimleri Enstitüsünde Bilgi Güvenliği Mühendisliği yüksek lisans (tezli ve tezsiz) programı,
- MEDİPOL Üniversitesinde Elektrik, Elektronik ve Siber Sistemler Doktora programı,
- Yaşar Üniversitesi Fen Bilimleri Enstitüsünde Bilgisayar Mühendisliği Ana Bilim Dalı altında Siber Güvenlik Yüksek Lisans programı
- Gazi Üniversitesi Fen Bilimleri Enstitüsünde Bilgi Güvenliği Mühendisliği Yüksek Lisans ve Doktora Programları
- İstanbul Teknik Üniversitesinde Bilgi Güvenliği Mühendisliği ve Kriptoloji Yüksek Lisans ve Doktora programları,
- Bahçeşehir Üniversitesi Fen Bilimleri Enstitüsünde Siber Güvenlik Yüksek Lisans programı
- Gebze Teknik Üniversitesi Mühendislik Fakültesi Bilgisayar Mühendisliği Siber Güvenlik Yüksek Lisans programı

Bunun yanında internetin yaygınlaşması ile beraber bilişim suçlarında (TBMM BİAK, 2013) ve dolayısıyla adli bilişim vakalarında artış gözlemlenmektedir. Adli Bilişim denildiğinde, internet ortamında daha genel bir ifade ile siber uzayda işlenebilen suçlarla mücadele ve bilgi güvenliği üzerine çalışmaların yapıldığı durumlar kastedilmektedir (Varol vd., 2013). Bu türden vakalar ile mücadele için gerekli uzmanların yetişmesi amacıyla ülkemizde çeşitli eğitim kurumları Adli Bilişim eğitimi vermektedir. Varol'un (2013) çalışmasında Adli Bilişim alanında ülkemizde eğitim veren kurumlar aşağıdaki şekilde listelenmiştir:

- Polis Akademisi Güvenlik Bilimleri Fakültesi/Enstitüsü
- Gazi Üniversitesi Bilişim Enstitüsü Adli Bilişim Anabilim Dalı
- Mustafa Kemal Üniversitesi Bilişim Teknolojisi Yüksekokulu
- Hacettepe Üniversitesi Adli Bilişim Araştırma ve Uygulama Merkezi

- Fırat Üniversitesi Adli Bilişim Mühendisliği Bölümü

Yakın gelecekte daha yoğun olarak karşılaşılması muhtemel siber savaşlar göz önünde bulundurulduğunda Türk Silahlı Kuvvetleri (TSK) personelinin Siber Güvenlik alanındaki yetişmiş insan gücü ihtiyacının karşılanması gerekmektedir. Bu kapsamdaSiber Güvenlik uzmanlarının yetiştirilmesi maksadıyla, detayları sonraki bölümde açıklanmış olan, DHO'nda açılan Siber Güvenlik Yüksek Lisans Programı, 2015-2016 Eğitim ve Öğretim yılında eğitime başlamıştır.

DHO SİBER GÜVENLİK YÜKSEK LİSANS PROGRAMI

DHO Bilgisayar Mühendisliği Bölüm Başkanlığı altında açılan ve 2015-2016 Eğitim ve Öğretim yılında eğitime başlayan Siber Güvenlik Yüksek Lisans Programının (tezli), öncelikle deniz harekat ortamında siber saldırıya açık olan savaş yönetim sistemleri ve sensör sistemlerinin kullanıcısı ve yöneticisi olan Deniz Kuvvetleri Komutanlığı (Dz.K.K.lığı) personelinin siber güvenlik konusunda bilgilenmesi, bilinçlenmesi ve uzmanlaşmasını sağlamak olmak üzere Türkiye'de Siber Güvenlik alanında nitelikli personel yetiştirilmesi sürecine katkı sağlamayı amaçlamaktadır. DHO Siber Güvenlik Yüksek Lisans programında bu amacı gerçekleştirmek maksadıyla;

- ACM'nin belirlemiş olduğu siber güvenlik dersi müfredatı ana konuları,
- A.B.D. Deniz Kuvvetleri Lisansüstü Okulu (Naval Post Graduate School)'nda verilen yüksek lisans ve sertifika programları,
- TÜBİTAK ile siber güvenlik eğitimi kapsamında işbirliği yapan üniversitelerin programları,
- TSK'daki konu ile ilgili otoritelerin öngörüleri,
- Halihazırda DHO'nda görevli öğretim üyelerinin uzmanlık alanları göz önünde bulundurularak güncel yaklaşımlara uygun bir müfredat oluşturulmuştur. Bu kapsamda verilmekte olan dersler Tablo 1'de sunulmuştur.

Programa Öğrenci Kabulü

Programa 2015-2016 Eğitim ve Öğretim yılında bir asker öğrenci kabul edilmiştir. 2016-2017 Eğitim ve Öğretim yılından itibaren programa, Harp Okulları ve Üniversitelerin Bilgisayar Mühendisliği lisans programlarından mezun olmuş hem asker hem de sivil öğrenciler kabul edilecektir. Başvuru koşulları ve tarihi ile kontenjanlar DHO resmi örün (web) sayfasından duyurul(acak/makta)dır.

Tablo 1. DHO DEBİM Siber Güvenlik Yüksek Lisans Ders Programı

DERS İSİMLERİ	DERS SAATİ (Ders + Laboratuvar)	DERS DÖNEMİ
Bilgi Sistemleri Güvenliği	2+2	1
Bilgisayar Ağları ve Haberleşme Güvenliği	2+2	1
Bilgi Yönetimi ve Güvenlik Politikaları	2+2	1
Güvenli Yazılım Geliştirme	2+2	1
Seminer	3+0	1
Zararlı Yazılımlar	2+2	2
Kablosuz Ağ Güvenliği	2+2	2
Adli Bilişim	2+2	2
Siber Güvenlik için Veri Madenciliği Uygulamaları	2+2	2
Yüksek Lisans Tezi	1+0	3 ve 4

Derslerin Yürütülmesi

Dersler, DEBİM dershanelerinde ve DHO bünyesinde kurulmuş olan Siber Güvenlik Laboratuvarında işlenmektedir. Diğer taraftan Gebze Teknik Üniversitesi ile yapılan işbirliği protokolü gereği, anılan üniversitenin Bilgisayar Mühendisliği Bölüm Başkanlığı bünyesinde açılan Siber Güvenlik Programı'ndan da dersler alınabilmektedir. Görülen lüzum üzerine Türkiye'de Siber Güvenlik alanında uzmanlığı ve derinliği olan doktoralı personel ve/veya akademik personelin de Siber Güvenlik Yüksek Lisans programı kapsamında DEBİM'de ders vermesi sağlanmaktadır.

DHO'nda Siber Güvenliğe İlişkin Faaliyetler ve Hedefler

DHO'nun stratejik planında "siber güvenlik alanında Türkiye'de marka olmak" hedefi yer almaktadır. Bu kapsamda okulda; öğrenciler ve personelin siber güvenliğe ilişkin farkındalığını artırmak maksadıyla faaliyetler düzenlenmektedir. Bu faaliyetler arasında; tüm öğrencilere zorunlu siber güvenlik dersi verilmesi, siber güvenlik alanında derinleşmiş uzmanlar tarafından konferanslar sunulması, okuldaki uygun mahallere afişler asılması, uzaktan eğitim dersleri açılarak çevrimiçi sınavlar uygulanması, e-postalar ile bilgilendirmeler yapılması, öğrenci ve öğretim elemanlarının siber güvenliğe yönelik seminer/ konferans/ sempozyum/ yarışmalara katılımının teşvik edilmesi, savunma sanayi firmaları ve/veya üniversiteler ile koordineli seminer/ konferans/ sempozyum planlanması vb. sayılabilmektedir. Diğer taraftan okuldaki öğretim elemanları, konuya ilişkin

uzmanlıklarının/derinliklerinin artırılması maksadıyla, yurtiçi ve yurtdışı eğitim imkanlarından yararlandırılmaktadır. Ayrıca, Dz.K.K. lığı'nın siber güvenlik alanında yetişmiş personel ihtiyacını karşılamak maksadıyla Bilgisayar Mühendisliği Bölüm Başkanlığı altında Siber Güvenlik Ana Bilim Dalı kapsamında 2018-2019 Eğitim ve Öğretim yılından itibaren lisans seviyesinde Siber Güvenlik eğitimi verilmesi planlanmaktadır.

SONUÇ

Siber uzayın gitgide büyümesi varlıklar üzerindeki siber tehditleri, mahremiyet problemlerini ve siber hukukun önemini artırmaktadır. Her geçen gün siber uzaya yeni varlıklar eklenmekte ve bu varlıklar hayatımızın ayrılmaz bir parçası haline gelmektedir. Siber varlıkların insan hayatına getirdiği yeniliklerin bilinçsiz kullanılması ve kullanım sırasında yeterli ölçüde önlemlerin alınmaması insanın bu teknolojiden önemli oranda zarar görmesine yol açabilmektedir. İnsanların karşılaşabileceği teknolojik zararları asgariye indirgeyebilmek için ise bir takım önlemlerin alınması gerekmektedir.

Devlet bazında, kurumsal ve kişisel bazda alınabilecek önlem silsilesinin en büyük ayağını teknolojinin bilinçli kullanılması ve nitelikli personel yetiştirilmesi oluşturmaktadır. Bunları sağlamak için ise özellikle örgün eğitim kurumlarında, gelişen teknoloji ve güncel siber tehditleri de ihtiva eden bir müfredat ile eğitim faaliyetleri düzenlenmelidir. Bu tür çalışmaların gerçekleştirilmesi amacıyla dünyada ve ülkemizde son yıllarda birçok üniversitede ilgili bölümler açılmaktadır.

Bu kapsamda DHO Bilgisayar Mühendisliği bünyesinde açılan Siber Güvenlik Yüksek Lisans Programı Deniz Kuvvetlerinin ihtiyaç duyduğu nitelikli siber güvenlik personelinin yetiştirilmesi için gerekli öğretim elemanı ve altyapı ihtiyaçlarını bünyesinde barındırmaktadır. Bilgi güvenliğinin önemi nin nesnelerin interneti (Internet of Things-IoT) gibi teknolojilerin yaygınlaşmasıyla daha da artacağı göz önünde bulundurulduğunda DHO ve diğer üniversiteler bünyesinde açılan siber güvenliğe yönelik bölümlerin gelecekte de artacak olan nitelikli siber güvenlik personeli ihtiyacını karşılama noktasında önemli bir görev üstlenmekte olduğu değerlendirilmektedir.

KAYNAKLAR

1. ACM Digital Library, http://lib.baskent.edu.tr/ACM Tanıtım Dokumani.pdf, (Erişim Tarihi: 29.05.2016).
2. AKIN, A., (21 Kasım 2015), "Siber Savaş ve Siber Güvenlik Nedir?", http://www.stratejikanaliz.com/analizler/harp-ve-strateji/siber-savas-ve-siber-guvenlik-nedir/#axzz3wUUj1An8, (Erişim Tarihi: 10.05.2016).
3. BARTLETT, J., (2015), "How the mysterious dark net is going mainstream", https://www.ted.com/talks/jamie_bartlett_how_the_mysterious_dark_net_is_going_mainstream?language=en, (Erişim Tarihi: 29.04.2016).
4. BAYOĞLU, B., (2016). "Kişisel Bilgisayarlar İçin Temel Güvenlik Adımları", TÜBİTAK Ulusal Bilgi Güvenliği Kapısı, http://www.bilgiguvenligi.gov.tr/son-kullanici-kategorisi/kisisel-bilgisayarlar-icin-temel-guvenlik-adimlari.html, (Erişim Tarihi: 19.06.2016).
5. BIÇAKÇI, S., (2014), "NATO'nun Gelişen Tehdit Algısı: 21. Yüzyılda Siber Güvenlik", *Uluslararası İlişkiler*, Cilt 10, Sayı 40, ss. 101-130.
6. BIÇAKÇI, S., Ergün, D. ve Çelikpala, M., (2015), "Türkiye'de Siber Güvenlik", *EDAM Siber Politika Kağıtları Serisi 2015/1*, ss.1-35.
7. Bilgi Güvenliği, (2016), https://tr.wikipedia.org/wiki/Bilgi_güvenliği, (Erişim Tarihi: 29.05.2016).
8. Cybersecurity Education at UMD, Maryland Cybersecurity Center, http://www.cyber.umd.edu/education, (Erişim Tarihi: 02.06.2016).
9. EMRE, B., (2016), "Siber Savaşlar: 5.Boyutta Savaş", http://www.siberguvenlik.org.tr/2013/01/siber-savaslar-5-boyutta-savas.html, (Erişim Tarihi: 03.05.2016).
10. GÜNGÖR, M., (2015), Ulusal Bilgi Güvenliği: Strateji ve Kurumsal Yapılanma, T.C. Kalkınma Bakanlığı Bilgi Toplumu Dairesi Başkanlığı Uzmanlık Tezi.
11. Kaspersky Lab., (2014), "28 milyon finansal siber saldırının çoğu Türkiye'de", http://www.kaspersky.com/tr/about/news/virus/2014/28-milyon-finansal-siber-saldirinin-cogu-Turkiyede, (Erişim Tarihi: 13.05.2016).
12. KESSLER, G.C. ve RAMSAY, J.D., (2014), "A Proposed Curriculum in Cybersecurity Education Targeting Homeland Security Students", *47th Hawaii International Conference on System Science*.
13. Master of Science in Cyber Security, (2016), https://en.wikipedia.org/wiki/Master_of_Science_in_Cyber_Security, (Erişim Tarihi: 02.06.2016).
14. MCGETTRICK, A., (30 Ağustos 2013), "Toward Curricular Guidelines for Cybersecurity Education and Training: Report of a Workshop on Cybersecurity Education and Training", https://www.acm.org/education/TowardCurricularGuidelinesCybersec.pdf , (Erişim Tarihi: 29.05.2016).

15. MİL, H.İ., (2015), Sosyal Güvenlik Kurumundaki Siber Güvenlik Yönetimi Uygulamalarının İncelenmesi ve Değerlendirilmesi, *Dicle Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, Nisan 2015, Yıl: 7, Sayı: 13, ss. 398-416.

16. OĞUZ, S., CEYHAN, E.B. ve SAĞIROĞLU, Ş., (2015), "Teknolojinin Casuslukta Kullanılması ve Karşı Önlemler", http://iscturkey2016.org/wp-content/uploads/2016/03/paper.pdf, (Erişim Tarihi: 02.05.2016).

17. ÖĞÜN, M.N. ve KAYA, A., (2013), "Siber Güvenliğin Milli Güvenlik Açısından Önemi ve Alınabilecek Tedbirler", *Güvenlik Stratejileri*, Sayı 18, ss.163-173.

18. Ponemon Institute, (2014), "Best Schools for Cybersecurity Research Report" , http://www.hp.com/hpinfo/newsroom/press_kits/2014/RSAConference2014/Ponemon_2014_Best_Schools_Report.pdf, (Erişim Tarihi: 04.06.2016).

19. Scada, https://tr.wikipedia.org/wiki/ SCADA, (Erişim Tarihi: 19.06.2016).

20. Securosis.com'dan aktaran PEKEN, M.M., (2015), "Bilgi Güvenliği Nedir ve Nasıl Sınıflandırılır?", https://www.sibergah.com/genel/bilgi-guvenligi-nedir-ve-nasil-siniflandirilir, (Erişim Tarihi: 29.05.2016)

21. TBMM Bilişim ve İnternet Araştırma Komisyonu (BİAK) Raporu, (2013), http://www.biakraporu.org, (Erişim Tarihi: 06.05.2016).

22. TÜRKAY, İ., (20 Nisan 2016), "Kamu Bilişim Zirvesi 2016'nın Değerlendirilmesi", http://www.vergialgi.net/ekonomi-maliye/kamu-bilisim-zirvesi-2016-nin-degerlendirilmesi, (Erişim Tarihi: 20.04.2016).

23. Türkiye İstatistik Kurumu, (2015), "Hanehalkı Bilişim Teknolojileri Kullanım Araştırması", http://www.tuik.gov.tr/PreHaberBultenleri.do?id=18660, (Erişim Tarihi:15.05.2016).

24. UDHB, (2013), Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı, T.C. Ulaştırma, Denizcilik ve Haberleşme Bakanlığı, https://www.btk.gov.tr/File/?path=ROOT%2f1%2fDocuments%2fSayfalar%2fBTDNewFolder%2fSiber+G%C3%BCvenlik%2f2_1_Strateji+Eylem+Plan%C4%B1+2013-2014.pdf, (Erişim Tarihi: 19.06.2016).

25. UDHB, (2016), 2016-2019 Ulusal Siber Güvenlik Stratejisi, T.C. Ulaştırma, Denizcilik ve Haberleşme Bakanlığı, http://www.udhb.gov.tr/doc/ siberg/2016-2019guvenlik.pdf, (Erişim Tarihi: 04.05.2016).

26. VAROL, A., (8-10 Aralık 2015), "Türkiye'de Adli Bilişim Eğitimi ve Denetimli Serbestlik Uygulamaları", *Türkiye'de Denetimli Serbestlik 10. Yıl Sempozyumu*, ss.1-13, İstanbul.

27. VAROL, C., Cooper, P.A. ve Varol, A., (20-21 Mayıs 2013), "Türkiye'de Adli Bilişim Eğitimi", *1st International Symposium on Digital Forensics and Security (ISDFS'13)*, Elazığ.

28. YILDIZ, M., (2014), Siber Suçlar ve Kurum Güvenliği, T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı Uzmanlık Tezi, Kasım 2014, http://www.udhb.gov.tr/images/hizlierisim/efcecbe1f21e9fe.pdf, (Erişim Tarihi: 19.06.2016).

29. YILMAZ, S. ve Sağıroğlu, Ş., (2013), "Siber Güvenlik Risk Analizi, Tehdit ve Hazırlık Seviyeleri", *6. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı Bildiriler Kitabı*, ss.158-166, Ankara.