Siber Saldırı Hedefleri ve Türkiye'de Siber Güvenlik Stratejisi

Seda YILMAZ ve Şeref SAĞIROĞLU

***Özet*—Siber güvenlik, bireysel, kurumsal ve ulusal yapılar için önemli bir husustur. Siber tehditler sadece bireylerin kişisel verilerinin güvenliğini değil aynı zamanda ülkelerin bütünlüğünü de tehdit eder bir noktaya gelmiştir. Bu çalışmada tehditlerin yöneldiği popüler hedefler, dünya üzerindeki siber saldırı ve hatta savaş denemeleri ile ülkemizde siber güvenlik konusundaki yaklaşımların neler olduğu üzerinde durulmuş, diğer ülkelerin siber güvenlik faaliyetlerinden örnekler verilmiştir. Sonuç olarak ülkemizin siber güvenlik stratejisi değerlendirilmiştir.**

***Anahtar Kelimeler*— Siber güvenlik, hedef, siberstrateji, Türkiye**

***Abstract*—Cyber security, individual, corporate and national structures is an important consideration. Cyber +threats to the security of the personal data of individuals only, but also threatens the integrity of the countries has a point. In this study, directed the popular targets of threats, cyber attacks, and even warfare experiments in the world with what is happening in our country focuses on the approaches of other countries on cyber security and cyber security are examples of activities. As a result, our country's cyber security strategy were evaluated.**

***Index Terms*— Cyber security, target, cyber strategy,Turkey**

I. GİRİŞ

Siber güvenlik ITU tarafından "siber çevre, organizasyonlar ve kullanıcının varlıklarını korumak için kullanılabilir araçlar, politikalar, güvenlik konseptleri, güvenlik önlemleri, kurallar, risk yönetimi, eylemler,eğitimler,uygulamalar ile teknolojiler bütünü" olarak tanımlanmıştır [21].

Siber tehditler her gün başka bir alanda kendini göstermekte ve siber güvenlik kavramı gün geçtikçe önem kazanarak daha çok hayatımıza dahil olmaktadır. Ülkelerin bütünlüğünü ve güvenliğini bile tehdit eden bu kavram, devletlerin vatandaşlarını korumak için tedbir almalarının zorunlu hale getirmiştir. Artık siber dünya birkaç bilgisayar korsanının oyun alanından çıkıp popular hedeflerin olduğu, amaçlı, planlı, disiplinli saldırıların gerçekleştirildiği ve hatta ülkelerin birbirlerine güç gösterisinde bulunduğu bir yer haline gelmeye başlamıştır.

Son yıllarda ülkeler bu konunun önemini dikkate alarak ulusal stratejilerini geliştirmişler ve bu konuda gerek maddi olarak gerekse insan gücü, altyapı ve yeteneklerini arttırıcı tedbirler almaya başlamışlardır. Bu çalışmada ikinci bölümde siber güvenlikte popular hedefler, üçüncü bölümde siber savaş denemeleri, dördüncü bölümde Türkiye'de siber güvenlik, beşinci bölümde Türkiye'nin siber güvenlik stratejisi konuları tartışılmış ve altıncı bölümde Dünya'dan siber güvenlik faaliyeti örnekleri verilerek sonuç ve öneriler sunulmuştur.

II. SİBER GÜVENLİKTE POPÜLER HEDEFLER

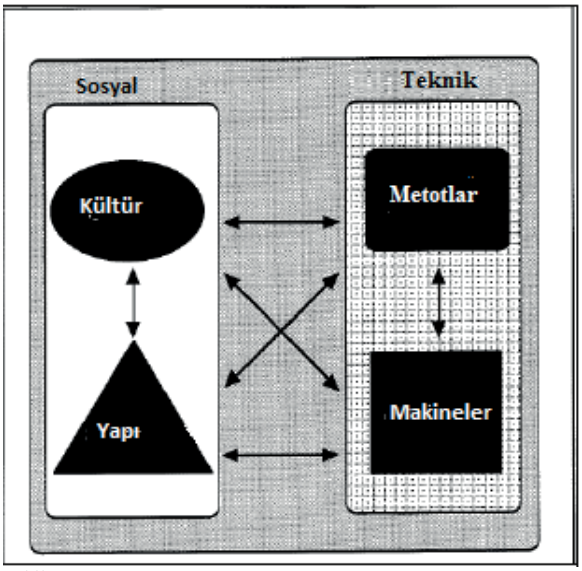
Günümüzde siber güvenlik ve savunma yaklaşımları hemen hemen her alana nüfuz etmiştir. Bu çalışmada siber güvenlik ihlallerinin en fazla olduğu ortamlar farklı başlıklar altında incelenmiştir.

A. Sosyal Ağlar

Sosyal ağlar bugün en büyük fenomendir. İnsanlar yoğun yaşam şartları içinde her yere ve her şeye yetişmek için acele edip koşuştururken en büyük insani ihtiyaç olan paylaşım ihtiyacını maalesef yeterince karşılayamamaktadır. Günlük hayatta çok şey yaşıyor, çok şey görüyor ve çok şey biriktiriyoruz. Sosyal ağlar bu konuda büyük fırsatlar sunmaktadır. Sosyal ağ uygulamaları ile paylaşımda bulunabiliyor, biriktirdiklerimizi anlatabiliyor, arkadaşlarımızla sohbet edebiliyor, fotoğraflarımızı/videolarımızı paylaşabiliyor, eski arkadaşlarımıza ulaşabiliyor, ürün tanıtımlarını yapabiliyor hatta ve hatta bir iş yeri sahibiysek işe alacağımız personel hakkında ön araştırma bile yapabiliyoruz. Çoğu zaman hayatımızı neredeyse tamamen sosyal ağ üzerinden yaşıyoruz.

Bu kadar etkin kullanılan bir sistem tabikî toplum hakkında bir takım sonuçlara ulaşılmasına da imkân sağlayacaktır. Ağa katılan farklı bireylerin üstlendikleri rolleri, davranış kalıplarını ve gizli özelliklerini ayıklamak amacıyla uygulanan analiz tekniğine Sosyal Ağ Analizi (SAA) denilmektedir. SAA iletişim, paylaşım, organizasyon, istihbarat, güvenlik gibi birçok alanda etkin olarak kullanılmakta olup bireysel analiz ve toplumsal analiz olmak üzere iki türü bulunmaktadır [2].

Kültür-Risk Teorisine göre her birey risk kavramını kendi toplumsal yapısı ve kültürünün etkisinde algılamaktadır [4]. Bireyleri, algıladıkları risklere göre analiz ederek bireysel, eşitlikçi, hiyerarşik ve kaderci olarak gruplandırmak mümkündür. Bireysel grup içine dâhil edilenler dünyayı iyimser bir yaklaşımla görmektedir. Riskin onu arayanlar için var olduğuna inanırlar. Eşitlikçi gruba dâhil olanlar çevrelerindeki olguları geçici olarak algılarlar ve risk almaktan hoşlanmazlar. Hiyerarşik olarak nitelendirilenler dünyayı hoşgörü içinde algılarlar ve belli bir limite kadar riskleri kabul ederler. Kaderci gruba dâhil olan insan profili ise olayları kaprisli bir bakış açısıyla değerlendirirler. Bu kategoriler temel alınarak ve insanların davranış özellikleri incelenerek 1990'lı yıllarda Kowalski tarafından kültür/yapı ile metot/makine incelemesinin birlikte incelendiği sosyo-teknik değerlendir-menin bilgi güvenliği için kullanılabilir bir teknik olduğu ileri sürülmüştür [4]. Sosyal ağlar üzerinden bilgi güvenliğinin sağlanmasında ve bireylerin analiz edilmesinde anlatılan teknikler temel teşkil etmektedir. Zira Amerika Ulusal Güvenlik Ajansı tarafından geliştirilen ve kabul gören 'Derin Savunma' stratejisine göre güvenliği sağlamada temel yapı taşı kullanıcıların olayları değerlendirmeleri ve davranış hareketleridir [4].



Şekil 1. Sosyo-Teknik Sistem [4].

Sosyal ağlar, kişiye ait her türlü bilginin kişinin rızası ile paylaştığı ortamlar oldukları için yemleme, önemsiz e-posta, kişinin verilerine erişim sağlamak amacıyla düzenlenen kullanıcı hesaplarının ele geçirilmesi gibi pek çok siber saldırının doğal hedefleri haline gelmişlerdir [3]. Sosyal ağlara yönelik tespit edilen ilk tehdit Şubat 2011'de kullanıcı ile sosyal ağ servis sağlayıcı arasındaki iletişimin dinlendiği PIMA saldırısı olmuştur [3].

Sosyal ağlarda kullanıcı tarafından doğrulanan bilgilerin kaydedildiği çerezlerin, korumalı olarak servis sağlayıcıya iletildiği https protokolü yerine şifresiz ve korumasız olarak iletimi gerçekleştiren http protokolünün tercih edilmesi ciddi bir tehdit oluşturmaktadır. Bu tehdit Mayıs 2011'de Windows İşletim sistemi kullanan bir makine üzerindeki IE (Internet Explorer) ile yapılan sosyal ağ servisine erişim sırasında kullanılmıştır. Bilgilerin tutulduğu çerezler, sıfır-gün açığı kullanılarak tanımlanan özel bir güvenlik bölgesine yönlendirilirken kullanıcıya da "Erişim Engellendi" mesajı döndürülmektedir. Bu şekilde istenilen bilgi elde edilmektedir. Aynı dönemde Rishi Narang'un blogunda yayınlanan bir bilgiye göre her giriş işleminden sonra bilgisayarda oluşan dosyalar ve çerezler 1 yıl kadar aktifliklerini koruyabilmekte dolayısıyla kullanıcı profillerini saklayabilmektedirler [3]. Tehlikelerin tespitinin ardından konuyla ilgili çalışmalar hızlandırılmıştır. Çalışmalar özellikle https tabanlı bağlantı protokolleri geliştirilmesi üzerinde yoğunlaşmaktadır [3].

Sosyal ağlar üzerindeki en vahim tehdit ise siber-zorbalık olarak nitelendirilen ve özellikle çocuklar ile gençleri hedef alan her türlü taciz, şiddet, sosyal manipülasyonu, dışlanma ve tehdit içerikli davranışlardır [5]. Bu davranışların tespitinde sosyo-teknik, bireysel ve toplumsal analiz yöntemleri uygulanabilir [5]. 2011'de Silva tarafından tanımlanan siber zorbalık, görsel ve metinsel iletişime dayalı sanal dışlama faaliyetleri olarak ifade edilebilir. Bu faaliyetler kimi zaman sanal şiddet boyutlarına varan sonuçlar doğurmaktadır. Bir başka çalışmaya göre de uygulanan sosyal, fiziksel, sözel ve psikolojik baskılar ile şiddet, toplumda şiddete eğilimli bir yaklaşımın yaygınlaşma tehlikesini açığa çıkarmaktadır [5].

Çocuk ve gençlerin kendilerini ispat etme,bir yere/gruba dahil olma gibi ihtiyaçları üzerinden beslenen siber-zorbalık yaklaşımında görmezden gelme, dışlama, hakaret etme, istemediği davranışlara zorlama gibi yöntemlerle bireyler üzerinde baskı oluşturulmaktadır. Bu baskı karşısında bireydeki şiddet eğilimi beslenmektedir. Ayrıca sanal dünya üzerinden kurulan yakın arkadaşlıklarla olumsuz fiziksel ve psikolojik sonuçlar doğuran tacizlerin yapılıyor olması da başka bir tehdit olarak varlığını sürdürmektedir [5].

Kişiler üzerinde maddi fiziksel ve psikolojik etkileri olan kimlik hırsızlığı sonucu karşı karşıya kalınan dolandırıcılık, kredi kartı hırsızlığı, sahte vergi işlemleri gibi uygulamalar da siber zorbalık yöntemlerine örnek gösterilebilir [5].

Sanal dünyadaki tehditlerle mücadele yöntemleri olarak; bireysel eğitime özellikle okullarda ağırlık verilmesi, teknik açıdan bireysel analiz yöntemleri geliştirilerek sosyal ağ üzerindeki davranışların takip ve analiz edilmesi, bunun yanı sıra web-metin madenciliği uygulamaları ile olası siber zorbalık içeriklerinin tespit ve takip edilmesi gibi önlemler önerilebilir [5].

B. *Akıllı Şebekeler*

Enerji, telekomünikasyon, ulaşım, kanalizasyon ve su sistemleri gibi kritik altyapı sistemleri bilgi sistem otomasyonu ile idameedilmektedir. Bu sistemlerin bir ülke için stratejik öneme sahip olduğu düşünüldüğünde doğal hedefler haline dönüşmeleri kabul edilebilir bir durumdur. Zira bir ülkeye zarar vermek, kaos yaratmak ya da ekonomisini alt üst etmek için sistemlere gerçekleştirilecek bir siber saldırı yeterli olacaktır.

En ciddi hedef, bütün sistemlerin besleyici ünitesi olan enerji sistemleridir. İşlem tabanlı bir mimarisi olan bu sistemlere saldırı düzenlemek için sadece bilgi teknolojilerine (BT) uzaktan erişim sağlamak yeterli olmayacak, sistemlerin farklı coğrafyalarda bulunması muhtemel ünitelerine erişebilmek için içerden alınacak bir desteğe de ihtiyaç duyulacaktır. Bu durum saldırıyı daha organize bir hale getirmektedir [6].

Akıllı şebekeler smart-grid adı verilen yapılar ile yönetilmektedirler. Bir akıllı şebeke tasarlanırken, iki yönlü iletişim, gelişmiş kontrol sistemleri, gelişmiş donanım bileşenleri, akıllı algılama teknolojileri ve BT uygulamaları gibi farklı teknolojilerin bir arada kullanılması verimliliği, güvenilirliği ve temiz enerji dağılımını arttırırken aynı zamanda güvenliğin sağlanması için kritik bir durum oluşturmaktadır[14].

Akıllı şebekelerin sertifika güvenlik protokolleri gerçekleştirilirken ISO / IEC 27000 serisi standartları baz alınmalıdır. Ayrıca tehdit modellemesini yapmak, saldırıları aza indirgemek için segmentasyon kullanmak, güvenlik duvarlarını aktifleştirmek, zorunlu olarak aygıt yazılımlarında imza kullanmak, hassas verileri korumak için şifreleme algoritmaları kullanmak, güvenlik açıklarını yönetmek için kontrol merkezini kullanmak, penetrasyon testlerini yapmak, güçlü kimlik doğrulama algoritmalarının kullanılmasını sağlamak ve log takiplerinin yapılmasına önem vermek güvenliğin sağlanması için alınabilecek önlemler arasındadır [14].

Şekil 2. Enerji Değer Zinciri [6].

Şekil 2'de görüldüğü gibi akıllı sistemlerle yönetilen bir altyapı olan enerjinin kullanıcılara ulaşması üretim, iletim, dağıtım ve yükleme olarak dört aşamalı bir sistemden oluşmaktadır [6]. Bu aşamalarının her birinin birbirini takip ettiği düşünüldüğünde sistemin bütününün güvenliğinin sağlanmasının her bir aşamanın bilişim sistemleri ve fiziksel erişim anlamında ayrı ayrı güvenliğinin sağlanması demek olduğu açıktır [6].

Enerji üretimi farklı coğrafi bölgelerde yapılıyor olabilir. Bu durumda bilişim sistemlerinin yanında tesislere fiziksel erişimin de kontrol altında tutulması gerekir. Üretim, iletim ve dağıtım aşamaları ağ üzerinden bilgi teknolojileri ile gerçekleştirip kontrol edildiğinden herhangi bir saldırıya maruz kalınmasının önüne geçmek adına erişim kontrollerinin yapılması, sisteme girişte kimlik bilgilerini kontrol edilmesi, donanımsal olarak zararlı içeriklerin varlığının kontrol edilmesi, yazılım güncellemelerinin yapılması, yazılımların kötü amaçlı erişimlere karşı kontrol edilmesi, güçlü bir anahtarlama ve şifreleme tekniğinin kullanılması, güvenlik protokollerinin kontrol edilmesi ve kullanıcıların güvenli şifreleme algoritmaları ile düzenlenmiş akıllı sayaçlar kullanmalarının teşvik edilmesi gereklidir. Sisteme erişimin son kullanıcılar üzerinden de gerçekleşebileceği göz önünde bulundurulmalıdır. Bu bakımdan konu değerlendirildiğinde son yıllarda popüler olan akıllı ev sistemlerinin ne kadar güvenli olduğu gelecek çalışmalar için bir inceleme konusu olarak önerilebilir [6].

C. Kapalı Devre Sistemler

Uzun yıllar kapalı devre sistemlerin internet ile bağlantısının olmaması nedeniyle daha güvenli olduğu ve virüs saldırılarına maruz kalmayacağı kanısı yaygındı. Stuxnet ile bunun aslında doğru bir kanı olmadığı gösterilmiştir. Bu sistemlerin dış ortamdaki ağ ile direk bir bağlantıları olmadığı için sistemin güvenliği erişim izni olan personel tarafından sağlanmakta ve yine güvenlik döngüsünün bu en zayıf halkası tarafından tehlikeye atılmaktadır. Bunun için "Siber Güvenlik Yönetimi Yaşam Döngüsü" modelinin kullanılması tavsiye edilmektedir [1].

Şekil 3. Siber Güvenlik Yaşam Döngüsü [1].

Şekil 3'de görüldüğü gibi siber güvenlik yaşam döngüsü birbirini takip eden aşamalardan oluşmaktadır. **Felsefe** aşamasında ilgili yapıya göre belirlenmiş bir siber güvenlik politikasının belgelendirilmesi gerçekleştirilir. **Tanımlama** aşaması bilgi varlıklarının ve potansiyel risklerinin belirlendiği aşamadır. **Rasyonelleştirme** aşamasında sistemin bütünlük içinde kullanılabilirliği için gerekli gereksinimler belirlenir. **Ayrıntılı tasarımda**, güvenlik duvarı, router, anahtarlar ve rasyonelleştirme aşamasında belirlenen gereksinimleri içeren bir mimari tasarım süreci gerçekleştirilir. **Uygulama** aşamasında aygıtlar ve bu aygıtların ayarları gerçekleştirilir. **İşlemde** ise güvenlik cihazlarının ve tüm ek fonksiyonların işlevlerini yerine getirip getirmediği kontrol edilir. **Bakım** aşamasında sistemin aksaklıkları giderilir ve idamesi sağlanır. **Değerlendirme** aşamasında sistemdeki açıklar değerlendirilir. **Değişim yönetiminde** ise siber güvenlik ayarlarının yönetimi ve ilgili değişikliklerin yapılması sağlanır [1].

Bazı kapalı devre sistemlerin ağ üzerinden dış ortamla bağlantısının olması ve/veya diğer kapalı sistemler ile iletişime geçmesi gerekebilir. Bu durumda hassasiyetle alınması gereken bazı önlemler aşağıda belirtilmiştir [1]:

- Kapalı devre sisteminin dış ağ ile bağlantısını sağlayan yapı mutlaka güvenlik duvarları, anti-virüs yazılımları ve paket filtreleme programları ile desteklemelidir.
- USB portları kapalı tutulmalıdır. Kullanılmasının zorunlu olduğu durumlarda öncelikle takılı aygıt mutlaka taramadan geçirilmelidir.
- Sistemler kabin ile korunabiliyorsa sistem odasına girilmeden gözle kontrollerin yapılabilmesi için şeffaf kapaklı modüller seçilmeli, sistemler mutlaka kilitli kapılar ardına alınmalı ve yetki kontrolü ile erişim sağlanmalıdır.
- Kapalı devre sisteminin güvenliğinin sağlanması için düzenli olarak virüs taraması yapılmalıdır.
- Tesis içi güvenlik açılarının değerlendirilebilmesi için güvenlik tarayıcı uygulamalar edinilmelidir (Örn.: Otomasyon Güvenlik 2000 (AS2000)).
- Düzenli olarak penetrasyon testileri uygulanmalıdır.

D. Acil Yardım Sistemleri

Hızla artan dünya nüfusu kaynakların yönetimini her alanda zorlaştırmaktadır. Afetler sonrası afet yönetimi, acil yardım kaynaklarının yönetimi ve hatta mevcut acil durum yardımı isteklerinin cevaplanması bile giderek zor bir hale gelmektedir. Kaynak darboğazının yaşanmaması ve en kısa sürede en iyi hizmetin ulaştırılması amacıyla acil durum (AD) yönetimine önem verilmeye başlanmıştır. Organizasyonun kolaylaştırılmasını hedefleyen acil durum yönetiminin (ADY) tasarlanmasında dikkat edilmesi gereken bazı ilkeler aşağıda özetlenmiştir [7].

- Oluşabilecek bütün acil durumlar dikkate alınarak bir planlamanın yapılması, AD (Acil Durum) görevleri ve ilgili oluşumların belirlenmesi gereklidir.
- Oluşabilecek acil ya da afet durumları için hazırlık tedbirleri belirlenmeli, müdahale edebilecek esnek gruplar tahsis edilmelidir.
- Önceliği personel ve kaynak yönetimi olan acil durum ve afet yönetim modelleri oluşturulmalıdır.
- AD gruplarınının oluşturulmasında kurum içi ve sivil vatandaşlardan oluşan karma bir topluluk seçilmelidir.

- Uygulama yapılabilecek gerçek planlar belirlenmelidir.
- Farklı gruplar arasında eşzamanlı iletişim ve hareket sağlanmalıdır.
- Planlar, değişen ve gelişen çevre koşullarına uyum sağlayabilmelidir.
- Ortak değerleri ve etik kuralları önde tutan teknolojik gelişmelere yatkın profesyonel gruplar oluşturulmasına dikkat edilmelidir.

Bilgi teknolojiler kullanılarak acil durumların planlanması, kaynakların etkin kullanımı, personel dağılımı ve koordinasyonu gibi yüksek miktardaki bilgi işlenmekte ve saklanabilmektedir. Sistemin bilgi teknolojileri ile yönetilebilir olmasının doğal sonucu olarak siber tehditler gündeme gelmiştir. Acil yardım sistemlerinin hedef alınması ile ülkeye kendi içinde ve uluslar arası platformda çok ciddi zararlar verilebilmektedir. Örneğin 2009 yılında İngiltere'nin savunma sanayisini ve acil yardım yönetimini hedef alan bir yazılım saldırısı gerçekleştirilmiş ve 2 hafta süreyle İngiliz Kraliyet Donanmasının personeli sistemler üzerine kişisel erişimlerini sağlayamamıştır. Yine aynı dönemde birçok hastanede ağ bağlantısı kesilerek hasta bilgilerine erişim engellenmiştir. Benzer bir saldırı Houston il mahkemesine yapılmış ve bu saldırı davaların sekteye uğramasına neden olmuştur [7].

E. Web Sayfaları

Yapılan çalışmalar siber saldırıların %75'inin web sayfalarını hedef alan saldırılar olduğunu göstermiştir. Bu saldırıların amaçları siteye ve servis sağlayıcıya zarar vermek, bilgilere erişmek olabileceği gibi web sayfasını bir köle sistem gibi kullanarak sayfayı ziyaret eden kullanıcıların bilgisayarlarına erişim sağlamak da olabilmektedir. Fakat bu saldırıların birçoğu maalesef çok kolay tespit edilememektedir. Saldırıların tespit edilememesinin başlıca nedenleri olarak kodlama yapılırken güvenli kodlama tekniklerinin kullanılmaması, servis sağlayıcı platformlarında bulunan güvenlik açıkları, web uygulamasının mantıksal akışındaki yanlış tasarım, sistemdeki güvenlik açıkları ya da işletme sorunları gösterilebilir. Saldırıların önlenmesi amacıyla geliştirme aşamasında kod incelenmesi, beyaz kutu testleri ile uygulamanın, sistemin ve güvenlik açıklarının taranması gibi tedbirlerin alınması gereklidir. Ayrıca güvenlik duvarlarının yerleştirilmesi ve/veya iyileştirilmesi de gerekli olan bir diğer önlemdir [8].

Web sayfalarına gerçekleştirilen saldırılar daha çok SQL enjeksiyonu, Cross-site scripting (XSS) ve Cross-Site İstek Sahteciliği (CSRF) saldırılarıdır [8].

XSS'den korunmak için veriler sayfaya yüklenme aşamasında değil veri tabanına gönderilirken ya da veri tabanından çekilirken bir filtrelemeden geçirilmelidirler. Gerekli görüldüğünde katmanlı güvenlik duvarı mimarisi de uygulanmalıdır [23,24].

Sql enjeksiyonu önlemek için girdilerin veri tabanına iletilmeden önce derlendiği parametreli "store procedure" tekniğinin kullanılması, veri tabanında salt okuma yetkisinin verilmesi, oluşan hatalarla ilgili mesajların veri tabanına dair bilgi içermeyecek şekilde düzenlemesi gibi önlemler tercih edilmelidir [9].

Saldırılardan korunmak için güncel saldırı ve güvenlik uyarıları takip edilmeli, yamaların güncellikleri kontrol edilmeli ve sunuculara mutlaka filtreleme mekanizması eklenmelidir [8].

III. SİBER SAVAŞ DENEMELERİ

Daha önceki yıllarda küçük çaplı denemeler yapılmış ise de önemli siber savaş denemeleri aşağıda kısaca açıklanmıştır.

1999:NATO'nun bilgi sistem kaynaklarına ilk saldırı gerçekleştirildi. Kosova krizi sırasında taraf olan ülkelerin NATO e-posta hesaplarına gerçekleştirilen DDOS saldırıları ile haftalarca erişim engellendi [16].

2001:ABD, Dünya Ticaret Merkezi başta olmak üzere birden çok noktaya yapılan saldırılarla binlerce insanını kaybetmiştir. Eylemin planları, koordinasyonu ve hatta eğitimleri siber dünya üzerinden yapılmış fakat ABD istihbarat örgütleri tarafından fark edilememiştir. ABD tarafından asla itiraf edilmemiş olmasına rağmen Pentagon'a kadar yaklaşan uçakların radar sistemlerinde de izlenemediği ve ABD'nin tamamen hazırlıksız yakalandığı bilinmektedir. Bu olay ABD için tam bir siber savunma zafiyeti olarak değerlendirilirken dünya üzerinde siber güvenlik ve siber savaş kavramları için dönüm noktası olmuştur [16].

2003:ABD'e karşı bilinen ilk saldırılardan biri Slammer adındaki virüs tarafından Ohio kentindeki nükleer santrale gerçekleştirilmiştir. Kapalı devre olarak çalışan sisteme kontrolsüz bir bilgisayar tarafından sızdırılan virüs yaklaşık 5 saat boyunca güvenlik izleme sistemini devre dışı bırakarak sistemi duraksatmış ve büyük bir hasara neden olmuştur. Bu saldırı işlem tabanlı sistemlerdeki güvenlik açıkları için bir erken uyarı görevini görmüştür [6].

2006: Malezya hafif raylı sistemlerini hedef alan saldırıda raylı sistem bilgi sistemi hasar görmüş ve uzun süreli servis kesintisi yaşanmıştır. Yolcuların saatlerce mahsur kaldığısaldırı sonucu yapılan açıklamada durumun teknik bir arıza olduğu ifade edilmiştir [13].

2007: Estonya ile Rusya arasında yaşanan gerginlikte Rus korsanlarının Estonya devlet kurumlarına düzenlediği DDOS saldırıları Estonya tarafından üyesi olduğu NATO'ya taşınmış ve dünya bir savaşın eşiğine getirilmiştir [15]. NATO bu olayın ardından Ocak 2008'de Siber Savunma Politikasını hazırlayarak yayınlamıştır [16].

2008:ABD'de bilgisayar korsanları tarafından elektrik nakil sistemine yapılan saldırıda birçok şehir uzun süre elektrik kesintisi yaşamıştır. Bu olay gizli tutulmuş ayrıntılara yer verilmemiştir [6].

Malezya'da borsa sistemi arızalanmış ve bütün gün işlem yapılamamıştır. Büyük maddi zarara neden olan bu durum Malezya'nın Dünya çapındaki kredibilitesini de düşürmüştür [13].

Rusya ile Gürcistan arasındaki Güney Osetya bölgesi için yaşanan savaşların bir uzantısı olarak Rus korsanlarca yapılan DDOS saldırıları sonucunda Gürcistan devlet kurumlarının bilgi varlıklarına ciddi zararlar verilmiştir [15].

2009:ABD'de Kaliforniya kentinde bir firmaya yapılan saldırıda yağ sızıntısı ihbarı verilmiş ihbar sahte olmasına rağmen müdahale sistemlerini tetiklemesi nedeniyle binlerce dolarlık hasara neden olmuştur [6].

Temmuz 2009'da Kore ana hükümet oluşumları ile sivil web sitelerini ve aynı anda ABD'de beyaz sarayın web

sayfasını hedefleyen DOS saldırıları ile büyük bir hasar verilmiş ve ülkelerin saygınlıklarının kaybına nedenolunmuştur [10].

Kasım 2009'da Çinli korsanlar tarafından sosyal mühendislik atakları, uzaktan izleme ve erişim uygulamaları ile MS Windows a ait açıklardan faydalanılarak enerji sistemlerini hedef alan bir saldırı gerçekleştirilmiştir. Bu saldırı kendini McAfee programından saklamış ve hasara neden olmuştur [6].

2010: Bilinen en büyük ve en uzun soluklu saldırı İran'ın nükleer tesislerini hedef alan Stuxnet adlı virüs saldırısıdır. Bu virüs diğerlerinden farklı olarak belirli bir endüstriyel donanım için belirli bir faaliyeti durdurmak ve üzerinde değişiklik yapmayı hedefleyerek üretilmiştir. Faaliyete geçmeden önce yaklaşık bir yıl kendini gizli tuttuğu sanılmaktadır. Virüsün ağ üzerinden kendini çoğaltığı ve birden çok bilgisayara entegre olduğu saplanmıştır. İran tarafından net bir açıklama yapılmaması nedeniyle hasarın boyutları tam olarak bilinememeklebirlikte nükleer programa büyük zarar verdiği tahmin edilmektedir. Yapısı incelendiğinde Symantec tarafından büyük bir altyapı desteği ile geliştirilmiş olması gerektiği sonucuna varılmış ve bu durum virüsün bir ülke tarafından finanse edildiği kanısının oluşmasına neden olmuştur [6].

28 Kasımda yayınladığı belgelerle dünya kamuoyunu alt üst eden Wikileaks aslında ABD'nin bir siber savaş denemesi olarak değerlendirilmektedir. ABD Dış İşleri Bakanlığı'nın gizli dosyalarına sözde yasadışı yollarla ulaşan Wikileaks elemanlarının yayınladığı belgeler dünyadaki dengeleri altüstetmiştir. Bu belgelerin tetiklediği çok sayıda isyan ile Kuzey Afrika'daki birçok ülkenin yönetimi değişmiştir. Birçok lider imaj, para ve hatta yönetimi kaybetmiştir. Hâlihazırda belgelerin etkileri devam etmekte ve dış kaynaklı silahlı bir müdahaleye gerek kalmadan dünyanın bir çok yerinde köklü rejim değişiklikleri yaşanmaktadır [13].

2011: Malezya'da hükümetin bazı web sitelerine saldırılar düzenlenmiştir. Küçük çaplı bu saldırılar sistemin açıklarının tahmin edilmesi ve gelecek saldırıların zemini olarak yorumlanmıştır [13].

IV. DÜNYA'DAN SİBER GÜVENLİK FAALİYETİ ÖRNEKLERİ

Bu başlık altında bazı ülkelerdeki siber güvenlik faaliyetleri incelenmiştir.

Amerika Birleşik Devletleri:

ABD, siber savunma konusunda en ileri bilgi ile teknoloji olanaklarına sahip olan ve bu konuda örnek alınan ülkelerin başında gelmektedir. Özellikle 2001 yılındaki olaylardan sonra siber güvenlik konusu devlet politikası olarak görülmekte, tam bir kurumsal koordinasyon ile çalışmalar yürütülmektedir [20]. Şubat 2003'de Ulusal Siber Güvenlik Politikasını yayınlayan ABD, siber güvenlik konusunda devlet, özel sektör ve vatandaşların birlikte hareket etmesinin önemini vurgulamıştır [21]. Beyaz saray bünyesinde bulunan ve ulusal siber güvenlik faaliyetlerini yürüten Siber Güvenlik Ofisi direk olarak ABD Başkanı'na bağlıdır. Bu ofis koordinasyonunda çalışan gruplardan biri olan Ulusal Siber Tepki Koordinasyon Grubu siber saldırılar karşısında federal birimler arasındaki koordinasyonu sağlamakla görevlidir. Ulusal Güvenlik ajansı ve bağlı kuruluşları izleme ve istihbarat faaliyetlerini yürütmektedir. Karşı atak ve ordu ağı savunma hizmetleri Savunma Departmanı tarafından, soruşturma süreci ise Adalet Departmanı tarafından yürütülmektedir. Bu birimlerin yanı sıra ülkenin siber güvenliğini sağlanmasında ağların trafini izlemek için kullanılan EINSTEIN programı, federal kurumların dış dünyaya açılan ağ sayısını azaltan Güvenli İnternet Bağlantıları programı ve karşı saldırı ile ilgili bilgileri içerdiği düşünülen Gizli programlardan da destek alınmaktadır [20].

Hindistan:

Siber güvenlik kavramına en çok önem veren ülkelerden birisidir. 1990'lı yıllardan beri sürdürülen çalışmalar kapsamında devlete ait alt yapıların ve kiritik sistemlerin korunmasına yönelik olarak politikalar ve kanunlar oluşturulmaktadır. Ülke genelinde Bilgi Güvenliği Farkındalığı ve Eğitimi kampanyası yürütülerek bilinç düzeyinin arttırılmasına çalışılmaktadır. Hindistan Ulusal Güvenlik Konseyi bünyesindeki oluşumlar ile 7/24 esasına dayalı olarak siber saldırı ataklarının analiz edilmesi ve erken saldırı tespitine yönelik çalışmalar yapıldığı bilinmektedir. Ülkede bilişim ve telekominikasyon alanında faaliyet gösteren ve/veya bilişim sistemlerini yoğun olarak kullanan kurum/kuruluşların ISO 27001 Bilgi Güvenliği Yönetim Sistemi Standartları Uygunluk Sertifikasına sahip olma zorunluğu bulunmakta olup halen 250 den fazla firma bu sertifikaya sahiptir. Bunların yanı sıra ülkede acil durumlara müdahale edebilecek ya da ihtiyaç halinde ulaşılabilecek kendi alanlarında uzman personelin bilgilerini tutulduğu Ulusal Veri Tabanı ve Acil Durum Müdahale Ekipleri bulunmaktadır [20].

Çin Halk Cumhuriyeti:

Çin'de siber güvenlik faaliyetleri Çin Ordusu tarafından yürütülmektedir. Bu alanda yoğun faaliyetler yürüttüğü bilinen ordunun elinde kapsamlı bir güç olduğu tahmin edilmektedir. Ayrıca ARGE faaliyetleri kapsamında süper bilgisayarların üretildiği ve bu bilgisayarlar sayesinde birçok ülkenin şifreleme yapısının çözülebildiği iddaa edilmektedir. Ordu bünyesinde siber savunma ve saldırı konularına çalışan uzmanlardan oluşan iki ayrı grup ve sadece siber güvenlik üzerine faaliyet gösteren bir ARGE yapısı bulunmaktadır. Bazı ülkeler tarafından siber suçları desteklediği düşünülse de siber suçlarla mücadele konusunda ciddi çalışmalar yürütülmektedir. Ayrıca "Altın Kalkan" adı verilen güvenlik duvarı yapısına sahip olan ülkenin siber saldırılara karşı elinin güçlü olduğu bilinmektedir [20].

Almanya:

Almanya Federal Hükümeti tarafından etkin önlemler alınmaya başlanmıştır. Çin'de olduğu gibi Almaya'da da siber savunma faaliyetleri Ulusal Siber Güvenlik Konseyinin koordinasyonunda Alman Ordusunun sorumluluğunda yürütülmektedir [20].

İsrail:

Siber tehditler konusunda İsrail en hazırlıklı ülkeler-dendir. Siber savunma ve saldırılar konusunda ciddi yatırımlar yaptığı bilinen ülkede siber güvenlik, hükümet ve vatandaşların ortak bir faaliyeti olarak kabul edilmekte ve çalışmaların büyük kısmı ordu tarafından yürütülmektedir. İsrail ordusu emekli mensupları, BT uzmanları ve emekli MOSSAD ajanlarından oluşan "Birim 8200" isimli birim ülkenin siber gücünü oluşturmaktadır. Bu birim aynı zamanda konuda uzman personelin yetiştirilmesi için akademik bir rol de üstlenmiştir. Sahip olduğu teknoloji merkezinde ileri düzey ekipmanlar ile dünya üzerinde ağ trağini izleme ve istihbarat faaliyetlerini yürütme olanağına

sahip olduğu bilinmektedir. İnter ağını büyük çoğunlukla izleme gücüne sahip olan ülke, buna rağmen kritik işlemlerin yürütüldüğü ve bilgilerin işlendiği sistemlerini internetten bağımsız olarak kendi ağı içinde devam ettirerek bilgi güvenliğini sağlamaktadır [20].

İngiltere:

İngiltere hükümeti 2010 yılında yayınladığı Siber Güvenlik Raporu ve 2011 yılında yürürlüğe koyduğu Ulusal Siber Güvenlik Stratejisi ile bu konuda önemli adımlar atmıştır. Siber tehditlerin ülkenin güvenliğini riske atan birinci öncelikli tehditler kapsamına yerleştirmiş ayrıca bütçesinin çok büyük bir kısmını da siber savunmaya ayırmıştır. Ulusal Siber Güvenlik Programı, Hükümet Kabine Ofisi bünyesinde yürütülmektedir.Savunma Bakanlığı tarafından siber savunma faaliyetleri yürütülmektedir. Bakanlık bünyesinde oluşturulan birimler arasında bu alanda operasyonel taktik ve teknik geliştirmekle sorumlu birimler de yer almaktadır. 2013 'ün başlarında kurulum çalışmaları başlayan ve yapısal oluşumu devam eden National Crime Agency isimli teşkilat ile siber suçlarla mücadelede daha etkin bir hale gelmeyi hedeflemektedir. Ayrıca eğitim giderleri ve etik bilgisayar korsanlarının yetiştirilmesi için de ciddi bir bütçe ayrılmıştır [20].

Singapur:

E-devlet projelerini büyük oranda hayata geçirmiş olan Singapur dünyanın en etkin ve gelişmiş internet ağlarından birine sahiptir. Ülkede erken uyarı sistemlerinin geliştirilmesi, ulusal düzeyde bilincin arttılması, önlemlerin alınmasının sağlanması ve kurumlar ile özel sektör arasındaki bilgi paylaşımının/koordinasyonun arttırılması çalışmaları öncelikli olarak yürütülmektedir [20].

NATO:

NATO bünyesinde üye ülkelere yönelik siber saldırılara karşı önlemler alınması ve müttefik ülkelerin birlikte hareket etmelerinini sağlamak amaçlı çalışmalar yürütmektedir. Bu kapsamda Uluslarası Siber Savunma Politikası hazırlanmıştır. Politikanın temelinde üye ülkeler arasındaki temel ve kritik iletişimin sürdürülmesinin korunması yer almaktadır. Üye ülkelerle arasında tam bir haberleşme ve koordinasyon imkanını sağlayan kendi iletişim ağı bulunmakta olup bu yapı üzerinden gerektiğinde müdahale edebilme yeteneğine sahiptir. Bunun yanı sıra erken uyarı sistemleri, bilgi paylaşımı ve farkındalık oluşturma ağları ile de üye ülkelere destek vermektedir. Bünyesinde bulunan hızlı müdahale ekipleri, talep eden ülkeye yönelik siber saldırılara yerinde müdahale edebilmektedir. NATO, siber savunma ve müdahale konusunda gelişmiş bir teknolojiye ve sağlam bir altyapıya sahiptir [20].

Avrupa Birliği:

Üye ülkelerin maruz kaldığı ve kalabileceği siber tehditler karşısında önlem almayı hedefleyen AB, 2005'de Avrupa Ağ ve Bilgi Güvenliği Ajansını (ENISA), 2007'de siber terörizmi gözlemlemek amacıyla Avrupa Polis Ofisini(Europol) oluşturmuştur. Bu birimler hem üye ülkelere siber tehditlere karşı destek vermekte hem de ülkeler arasında koordinasyonu sağlamakla ilgili çalışmalar yürütmektedirler. Özellikle siber suçlar, internet korsanlığı, siber terörizm ve çocuk pornografisi konularında yoğun çalışmalar yürütmektedirler. AB tarafından acil durum takımlarının oluşturulması ile yasal yaptırımların belirlenmesi konusunda halen çalışmalar devam etmektedir [20].

Uluslar Arası Telekomünikasyon Birliği (ITU):

İnternet üzerinden yapılan siber saldırıların giderek yaygınlaşması bu konuda ortak bir mücadele biriminin kurulmasını zorunlu hale getirmiştir. 2003-2005 yıllarında faaliyetine başlayan ITU siber tehditlerle mücadele için ortak bir plartform oluşturmayı ve standartları belirlemeyi hedeflemektedir. Özellikle gelişmekte olan ülkeleri hedef kitlesi olarak gören kuruluş Radyo-iletişim, Standartlar ve Telekonimükasyon Geliştirme sektörlerinde faaliyet göstermektedir. 2007'de yayınladığı Global Cybersecurity Agenda(GCA) ile hukuki tedbirler, teknik/prosedürel tedbirler, siber güvenlik araçları, ulusal siber güvenlik politikalarının temelleri üzerine ortak standartlar belirlemiştir. ITU halen üye ülkelere bu konularda destek olmakta ve talep gelmesi halinde siber güvenlik tedbirleri kapsamında denetlemeler yaparak sertifikasyon uygulamaları gerçekleştirmektedir [20].

V. TÜRKİYE'DE SİBER GÜVENLİK

Siber saldırılarla mücadelede en önemli unsurlardan biri stratejik hedefler olan kritik altyapıların korunmasıdır. AB konseyi tarafından kritik altyapılar *"... insanların hayati sosyal fonksiyonlarının, sağlıklarının, emniyetlerinin, güven-liklerinin, ekonomik ve toplumsal refahlarının devamı için gerekli olan ve aksama veya yok edilmesi bu fonksiyonları sürdürmede yetersiz kalma sonucunda bir üye ülkede belirgin etki gösterecek varlık, sistem veya ilgili parçaları"*şeklinde ifade edilmiş ve aşağıda belirtilen unsurlar kritik altyapı olarak nitelendirilmiştir [12].

- Enerji (örn. Elektrik, gaz, rafineriler, aktarım ve dağıtım sistemleri)
- Bilgi ve İletişim (örn. Telekomünikasyon, yayıncılık, yazılım, donanım, Internet)
- Finans (örn. Bankacılık, yatırım)
- Sağlık (örn. Hastaneler, laboratuarlar)
- Gıda (örn. Güvenlik, üretim, gıda endüstrisi)
- Su (örn. Barajlar, depolama, dağıtım)
- Ulaşım (örn. Havaalanları, demir yolları, trafik kontrol sistemleri)
- Nükleer, Biyolojik, Kimyasal ve Radyoaktif madde endüstrileri
- Uzay araştırmaları
- Kamu düzeni ve güvenliği
- Sivil yönetimler

Türkiye'de siber suçlarla mücadele 2012 yılına kadarTC.Bilim, Sanayi ve Teknoloji Bakanlığı'nın koordina-törlüğünde Bilgi Teknolojileri Kurumu (BTK) tarafından sivil toplum kuruluşları ve kurumları ile birlikte yürütülmüştür. Siber saldırıların önlenmesi ve gerekli tedbirlerin alınması için ülke unsurlarının birlikte hareket etmesinin zorunluluğu prensibine dayanılarak 2002–2010 yıllarını kapsayan süreçte kritik altyapı sistemleri ve durumlarının tespiti, kurumların farkındalığının arttırılması ve siber güvenlik için bir stratejinin oluşturulmasına yönelik çalışmalar yapılmıştır [11].

Bu kapsamda 2005-2010 yılları arasında BTK tarafından gerçekleştirilen başlıca çalışmalardan bazıları aşağıda belirtilmeye çalışılmıştır [11,21]:

- Kimlik doğrulama, inkâr edilememe, gizlilik ve bütünlük ilkelerinin kullanılmasını sağlayan e-imza uygulamasına geçilmesi ve ilgili yasal mevzuatın (TCK 5070) hayata geçirilmesi.
- Haberleşme sektöründe faaliyet gösteren firmaların

varlıklarının belirlenmesi, ilgili tehdit ve zafiyetlerin belirlenmesi, fiziksel güvenliğin unsurları, donanım-yazılım ve personel güvenliği gibi unsurlar için alınması zorunlu tedbirleri içeren Elektronik Haberleşme Güvenliği Yönetmeliğinin (TCK 5809) yayınlanması.

- İnternet üzerinden işlenen şuçlarla mücadele edilmesi amacıyla İnternet ve Yapılan Yayınlar Yoluyla İşlenen Suçlarla Mücadele Yönetmeliğinin yürürlüğe girmesi (TCK 5651)
- Kişisel veri, kişisel verinin kapsamı, gizliliğinin korunması ile ilgili usul ve şartları içeren Telekomünikasyon Sektöründe Kişisel Bilgilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmeliğin yayınlanması.
- Farkındalığın arttırılması kapsamında çeşitli raporların hazırlanması ve kamuoyu ile paylaşılması
- Siber güvenlik ve bilgi güvenliği konulu konferans ve çalıştayların gerçekleştirilmesine öncülük etmek ve katkıda bulunmak
- Yığın e-postalarının önüne geçilmesi için hazırlanan projeye koordinatörlük etmek

BTK'nun yanı sıra bilgi güvenliği konusunda etkin çalışma gösteren kurumlardan birisi de Devlet Planlama Teşkilatı(DPT)'dır. DPT, "e-Türkiye girişimi Eylem Planı 2002," ,"e-Dönüşüm Türkiye Projesi Kısa Dönem Eylem Planı (2003-200)", "e-Dönüşüm Türkiye Porjesi 2005 Eylem Planı", "Bilgi Toplumu Stretejisi (2006-2010)" ve "Bilgi Toplumu Stratejisi Eylem Planı (2006-2010)" belgeleri ile konu hakkında aktif çalışma göstermiştir. Bu belgeleri temel alan, bilgi güvenliği kapsamında önem arzeden düzenlemeleri içeren ve çalışmaların işlem makamlarını belirleyen "Bilgi Toplumu Stratejisi ve Ek'i Eylem Planı" 2006 da resmi gazeteyayınlanmıştır. Bu plandaki en önemli noktalardan biri Kişisel Verilerin Korunması Taslağınınhazırlanarak yasalaştırılmasından bahsediliyor olmasıdır [21].

Diğer kurumlarmızdan bir çoğunda siber güvenlik ve bilgi güvenliğine yönelik bilinen çalışmaların nispeten daha az olması ve yıllık strateji planlarında siber güvenliği içeren maddelerin 2010 yılından sonra yer almaya başlamış olması durumun öneminin kavranması konusunda endişe verici olsa da yapılan çalışmaların umut verici olduğunu da belirtmek gerekmektedir. Özellikle Milli Eğitim Bakanlığı tarafından öğrencilerin ve velilerin bilinçlendirilmesine yönelik uygulamalar yürütülüyor olması toplumsal bilincin arttırılması açısında önem arzetmektedir.

Siber güvenliğin ülke güvenliğinin bir unsuru olduğu gözönüne alındığında özellikle güvenlik güçlerinin de konu üzerine yapılan çalışmalarda aktif olarak yer alması önem arzetmektedir. Bir çok ülkede uzun yıllardır siber güvenlik çalışmaları orduların bünyesinde öncelikli olarak yürütülmektedir. Bu bakımdan Genel Kurmay Başkanlığı Muhabere ve Siber Savunma Komutanlığı' nın kurulmuş olması ve tatbikatlara katılması önemli bir gelişmedir. Ayrıca Emniyet Genel Müdürlüğü'nün siber suçlar konusundaki çalışmaları son yıllarda yoğunlaşmış ve başarılı sonuçlar vermektedir.

Konunun AR-GE ayağında ise etkin çalışmalar TUBİTAK başlamış ve ULAK-CSIRT adındaki oluşum ile araştırma ve eğitim çalışmalarını sürdürmektedir. Bunun yanı sıra hükümet tarafından hayata geçirilen Bilgisayar Olaylarına Acil Mudahale Ekipleri (TR-BOME) 2007 yılından beri etkin olarak NATO ile işbirliği içinde bulunmakta ve NATO tarafından yürütülen Uluslar arası Siber Savunma Çalıştaylarına aktif katılım göstermektedir. Bu kapsamda 2007'de NATO NCIRC (NATO Computer Incident Response Capability) ile TR-BOME arasında personel değişimi, tatbikatlara katılım, NCIRC gizli ağına erişim, teknik veritabanı paylaşımı ve alarm-uyarı sistemlerine erişim konularını kapsayan bir anlaşma imzalanmıştır. Bu anlaşma içeriğine uygun olarak 2008 ve 2009 yılında düzenlenen tatbikatlarda temsil ve katılım gerçekleştirilmiştir [21].

2012 yılında alınan Bakanlar Kurulu'nun 11/06/2012 tarihli ve 2012/3842 sayılı Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna ilişkin kararı ile ülkemizde siber güvenliğin sağlanması, ilgili politikaların geliştirilmesi ve ulusal siber güvenlik stratejisinin belirlenmesi görevi TC.Ulaştırma, Denizcilik ve Haberleşme Bakanlığı'na devredilmiş ve o tarihten itibaren de ilgili bakanlıkça yürütülmektedir [19].

VI. TÜRKİYE'NİN ULUSAL SİBER GÜVENLİK STRATEJİSİ

Yapılan çalışmalar sonucunda siber güvenlik konusu ciddi bir tehdit olarak algılanmaya başlanmıştır. Kimlik hırsızlığı, dolandırıcılık gibi siber suçlar yönünden mağdur olan vatandaşlarımızın ne mağduriyetleri ne de suçlulukların yakalanıp yakalanmadığı malesef konunun magazin değerinin olmaması nedeniyle medyada yeterince yer almamaktadır. Bunun yanı sıra kurumlarımız kendilerine yapılan saldırıları ve kaybettikleri verilerin miktarını gerek itibar kaybı endişesi gerekse özel nedenlerle gizlemek konusunda çok kararlıdır. Yani siber saldırılar konusunda kim ne yaşıyor maalesef tam olarak bilinememektedir [17]. Ulusal siber güvenliğin sağlanması bu belirsizliğin ortadan kaldırılması, toplumun birey ve kurum bazında bilinçlendirilmesi ile mümkün olacaktır.

TC.Ulaştırma, Denizcilik ve Haberleşme Bakanlığı'nın sorumluluğunda gerçekleştirilen çalışmalar sonucunda kurum ve kuruluşlarca sağlanan her türlü bilgi teknolojileri temelli hizmetlerinin korunması, kritik altyapıların korunması ve olası siber saldırılar sonrasında sistemlerin en kısa sürede eski performanslarına dönmeleri ile saldırıların soruşturulmasında daha etkin imkanlar sağlamak için altyapı oluşturmak amacıyla "Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı" hazırlanarak yürürlüğe girmiştir. Eylem Planında siber risklerin neler olduğu, kurumlar arası işbirliği ile öngörülen dönemde yapılması ve daha sonraki yıllarda devamının sağlanması hedeflenen adımlar belirlenmiş ve uygulamaya koyulmuştur [19].

Ulusal Siber Güvenlik Stratejisi'ne göre güvenlik anlamında orta ve uzun vadede öncelikle dikkate alınması gereken bazı konular ve atılması gereken adımlar vardır. Bu konular aşağıda genel başlıkları ile belirtilmiştir [18].

1) Uluslar Arası İşbirliği: İnternetin sayesinde dünyanın her yerinden herhangi bir kuruma ya da ülkeye kolaylıkla saldırı gerçekleştirilebiliyor olması ülkeler arasındaki işbirliğini zorunlu bir hale getirmiştir. Ülkemizin müttefik ülkelerle dil birliğini azami seviyede tutmak, BM, AB, OECD ve NATO gibi örgütler bünyesindeki çalışmalara destek vermek ve katılmak, bölgesel ve küresel anlaşmalara taraf olmak, yapılan konferans, çalıştay, seminer gibiuluslar arası aktivitelere katılmak gerekliliği önem arz

etmektedir [18].

2) Siber Güvenlik Kültürünün Oluşturulması: Özellikle kritik altyapı sistemlerinden başlayarak kamu kurum ve kuruluşlarının yönetici, personelleri ve teknik hizmet personelleri siber güvenlik, tehdit/saldırılar konusunda eğitilmeli ve bilinçlendirilmelidir [18].

3) Yasal Düzenlemeler: Uluslar arası hukuk kuralları, kamu yararı, kritik altyapı sistemlerinin korunması ve kişisel veri güvenliğinin sağlanması amacıyla siber suçlarla mücadele kapsamında caydırıcı yasal yükümlülükler getirilmeli ve uygulanmalıdır. Yasal düzenlemeler yapılırken kişisel verilerin korunması, herkesin bilgi edinme hakkının korunması, haberleşmenin gizliliği esasının korunması ve bilgi güvenliği unsurları kapsamında gerekli tedbirlerin alınmasının önemi gibi kritik konular da göz önünde bulundurulmalıdır [18].

4) Kurumsal Yapılanma: Mücadelenin ve savunmanın koordineli bir şekilde yapılması için bir takım kurumsal yapılanmaların oluşturulmasına önem verilmedir. Ulusal siber güvenlik merkezi, müdahale merkezi strateji belirleme kurumu gibi yapılar oluşturularak hükümet, devlet kurumları ve sivil oluşumlar arasında iş birliği ve koordinasyon sağlanmalıdır [18].

5) Eğitim: Siber güvenlikte en önemli ve en zayıf halka olan bireylerin siber güvenlik konusunda eğitilmesi gereklidir. Teknik personelin yetiştirilmesi için gerekli lisans ve lisansüstü eğitim programları açılmalı ve personel bu konuda teşfik edilmelidir [18].

6) Kamu, Üniversite ve Özel Sektör İşbirliği: Ar-Ge çalışmalarının yapılması, sektörler arası iş birliğinin arttırılması ve akademik programların yaygınlaştırılmasının yanı sıra kamu-özel sektör, kamu-üniversite ile üniversite-özel sektör arasındaki iş birliğinin teşvik edilmesi ve çalışma ortamlarının sağlanması gereklidir [18].

7) Milli Teknoloji Geliştirme: Bilgi teknolojilerinde özellikle siber güvenlik alanında kullanılacak yazılım ve donanımların uluslar arası standartlara uygun olarak milli sermaye ve iş gücüyle üretilmesini teşvik etmek ve milli ürünlerin kullanımı tercih etmek önem arz etmektedir [18].

8) Belgelendirme: Bilgi teknolojileri üreten/kullanan kurum ve kuruluşların uluslar arası güvenlik sertifikaları ile belgelendirilmiş olmasına özen gösterilmelidir. Kamu kurumlarının belgelendirme konusundaki eksiklikleri giderilmelidir [18].

Ülkemizin ilk resmi siber güvenlik eylem planında gerçekleştirilmesi hedeflenen adımlar aşağıda özetlenmiştir [19]:

- Kurum ve kuruluşların yetki ve sorumluluklarının belirlenmesi ile hukuki anlamdaki düzenlemelerin yapılması
- Ulusal ve uluslar arası mevcut mevzuatın incelenmesi ve gerekli iyileştirmelerin yapılması
- Ortak terminoloji oluşturulma çalışmalarının yapılması
- Saldırıların tespiti ve gerekli delillerin temini için sistemin desteklenmesi
- Delillendirmede görevli kurum/kuruluşların en son teknoloji ürünlerinin temini ve devamlılığının sağlanması konusunda desteklenmesi
- Ulusal Siber Olaylarla Mücadele Merkezi'nin (USOM) ve Siber Olaylara Müdahale Ekipleri'nin (SOME) kurulması
- USOM ile koordineli çalışacak olan kurum SOME'lerinin kurulması
- Öncelikle kritik kurum/kuruluşlar olmak üzere bütün organların risk analizlerinin yapılması
- Acil eylem planlarının sektörel olarak oluşturulması ve hayata geçirilmesinin sağlanması
- Bilişim sistemlerinin, özellikle kritik altyapı sistemlerinin güçlendirilmesine öncelik verilmesi
- Kamu kurum/kuruluşlarına yönelik zorunlu denetim uygulamalarının geliştirilmesi
- Yetkili ve etkin teknik personel yetiştirilmesi için gerekli düzenlemelerin yapılması
- Teknik personele yönelik sertifikasyon ve akademik eğitim çalışmalarının uygulanması
- Yerli teknolojilerin geliştirilmesinin desteklenmesi
- Siber güvenlik tatbikat ve çalıştaylarına önem verilmesi
- Siber güvenlik tatbikatlarına ulusal ve uluslar arası düzeyde yüksek oranda katılımın sağlanması
- Tehditlerin belirlenmesine yönelik tehdit analiz ve trafik izleme başta olmak gerekli tespit mekanizmalarının kurulması
- Bilgi sistem hizmet sağlayıcılarının belgelendirilmesi
- İnternet sitesi servis sağlayıcıları ile veri kaynağı saklayıcılarında yerli sermayenin desteklenmesi ve kamu kurumlarının bu servislerden faydalanmasının sağlanması
- Açık kaynak kodlu ürünlerin kullanımının teşvik edilmesi
- Ar-Ge çalışmalarının desteklenmesi
- Siber güvenlikten sorumlu kurumların etki alanının ulusal ve uluslar arası platformda genişletilmesi

Eylem planında kurumların sorumluluklarının belirtilmesi önemli olmakla beraber kurumlar arasında tam bir işbirliğinin temel alınıyor olması planın gerçekleştirilebilirliğini arttırmaktadır. Sistemin tam güvenliğinin sağlanması sistem içindeki mekanizmaların ve alt sistemlerin her birinin güvenliğinin sağlanmasına bağlıdır. Bunun yanı sıra işbirliği, genel bilgi birikiminin ve kalitenin de artmasını sağlayacaktır.

VII. SONUÇ VE ÖNERİLER

Siber dünyanın etkinliğinin artması ve bilgiye erişimin birden çok yolla gerçekleşebiliyor olması aslında karşılaşılması muhtemel senaryoların hiç de uzakta olmadığının bir göstergesidir. Bireylerin bilgileri yasadışı yollarla ele geçirilebilir, bu bilgilerle dolandırıcılık, sahtecilik gibi bireylere zarar verecek işlemler yapılabilir, kurumların bilgi varlıklarına, kritik altyapıları etkileyecek saldırılarla ülkenin enerji kaynaklarına, hatta ve hatta ülkenin güvenlik unsurlarına zarar verilebilir. Anlaşılacağı üzere siber güvenlik kavramı bireyler, kurumlar ve ülkeler için dikkate alınması gereken bir kavramdır. Toplumun bütün grupları arasında koordinasyon ile tam iş birliğinin yapılması zorunludur.

Yapılan incelemede görülmüştür ki ülkemizde yapılan çalışmalarla var olan tehlikenin farkında olunduğu fakat alınabilecek önlemler konusunda daha çok çaba sarfedilmesinin ve özellikle kurumların bilinç düzeyinin arttırılmasının gerekliliği ön plana çıkmıştır. Bu bağlamda Ulusal Siber .Güvenlik Stratejisinin yayınlaması ve 2013-2014 Eylem Planın uygulama koyulması önemli ve umut vadeden bir adımdır. Stratejinin etkinliğini arttırmak için okullardan başlamak üzere medyanında desteğini alarak bütün toplumu hedef alan bir bilinçlendirme programının başlatılması, siber güvenlik tatbikatlarına ağırlık verilerek özellikle kritik altyapı sistemlerinin ve ulusal güvenlik unsurlarının zaafiyetlerinin belirlenmesine ve giderilmesine öncelik verilmesi, kamu kurum ve kuruluşlarında farkındalığı arttırmak ve tehlikeye dikkat çekmek için habersiz saldırılarla sistemlerin kontrol edilmesi gibi uygulamalar önerilebilir. Kritik öneme haiz olan verilerin bulunduğu ve işlemlerin yapıldığı sistemlerin internet ortamından bağımsız olarak oluşturulacak yerel bir ağ ile yürütülmesi de önerilebilecek başka bir yöntemdir. Bunların yanı sıra oluşturulacak siber güvenlik merkezlerinin kamu kurum ve kuruluşlarındaki teknik personel, özel sektör, üniversite ve sivil toplum kuruluşları temsilcileri ile güvenlik güçleri ve beyaz şapkalı bilgisayar korsanlarının da aralarında bulunduğu geniş bir kitle ile teşkil edilmesinin siber güvenlik kavramına daha geniş bir pencereden bakılmasına olanak sağlayacağı, oluşturulacak siber güvenlik merkezlerinin yanı sıra siber saldırılar karşısında acil müdahale ekiplerinin bulundurulmasının güvenlik konusundaki etkinliği artıracağı değerlendirilmektedir.

KAYNAKLAR

[1] KITAI T. TAKAI T. ,UCHIDA H. "Multiple and Independent Protection Layer Concept for Plant Cyber Security", SICE Annual Conference (SICE), 2012 Proceedings of, Agustos 2012, (963 – 966)EMRE Bâkır, "Siber Savaşlar – Başlangıç", http://www.siberguvenlik.org.tr/ makaleler/siber-savaslar-i/, Aralık 2012

[2] HEWETT Rattikorn," Toward Identification of Key Breakers in Social Cyber-Physical Networks", Systems, Man, and Cybernetics (SMC), Ocak 2011,(2731 - 2736)

[3] CASHİON Jeffrey, BASSİOUNİ Mostafa,"Protocol for Mitigating the Risk of Hijacking Social Networking Sites", Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom), Ocak 2011, (324 – 331)

[4] SABBAGH Bilal Al, KOWALSKİ Stewart," ST(CS)2 - Featuring socio-technical cyber security warning systems ", Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), 2012 International Conference on, Haziran 2012,(312 – 316)

[5] OCHOA A. ,PONCE J. ,JARAMILLO R. ,ORNELAS F. ,HERNANDEZ A. ,AZPEITIA D. ,ELIAS A. , HERNANDEZ A.,"Analysis of Cyber-Bullying in a Virtual Social Networking", Hybrid Intelligent Systems (HIS), 2011 11th International Conference on, Aralık 2011, (229 – 234)

[6] LİNE Maria B., TØNDEL Inger Anne, JAATUN Martin G., "Cyber Security Challenges in Smart Grids", Innovative Smart Grid Technologies (ISGT Europe),Aralık 2011,(1 – 8)

[7] WALKER Jessie, WİLLİAMS Byron J., SKELTON Gordon W., "Cyber Security for Emergency Management", Technologies for Homeland Security (HST), 2010 IEEE International Conference on, 2010 ,(476 - 480)

[8] DWEN-REN Tsai; CHANG A.Y., PEİCHİ Liu, HSUAN-CHANG Chen, "Optimum Tuning of Defense Settings for Common Attacks on the Web Applications", Security Technology, 2009. 43rd Annual 2009 International Carnahan Conference on ,Ocak 2009, (89 – 94)

[9] OWASP "Reviewing Code for SQL Injection", https://www.owasp.org/index.php/Reviewing_Code_for_SQL_Injection, 2010

[10] PARK Won Hyung," A Study on Risk Analysis and Assessment of Damages to Cyber Attack", Information Science and Applications (ICISA), 2010 International Conference on, Nisan 2010(1 - 6)

[11] ÜNVER Mustafa, CANBAY Cafer , "Ulusal ve Uluslar Arası Boyutlarıyla Siber Güvenlik",EMO- elektrik mühendisliği, Mart 2010, (94-103)

[12] ÜNVER Mustafa, CANBAY Cafer , ÖZKAN Hüseyin Burhan," Kritik Altyapıların Korunması", Bilgi Teknolojileri ve Koordinasyon Dairesi Başkanlığı, Mayıs 2010

[13] Azmi, I.M.A.G., Zulhuda, S. ,Jarot, S.P.W. "Data Breach on the Critical Information Infrastructures: Lessons from the Wikileaks", Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), 2012 International Conference on,Haziran 2012 (306 – 311)

[14] PALLOTTI E., MANGIATORDI F, " Smart Grid Cyber Security Requirements", Environment and Electrical Engineering (EEEIC), 2011 10th International Conference on,Mayıs 2011, (1 – 4)

[15] ALTUNDAL Ömer Faruk, "DDoS nedir, ne değildir?", http://www.siberguvenlik.org.tr/makaleler/ddos-nedir-ne-degildir/, Ağustos 2012

[16] Dr.THEİLER Olaf, " New threats: the cyber dimension", http://www.nato.int/docu/ review/2011/11-september/Cyber-Threads, Eylül 2011

[17] "Türkiye'nin Ulusal Siber Güvenlik Politikası Siber Savaş İçin Hazır mı?", http://www.siberguvenlik.org.tr/genel/turkiyenin-ulusal-siber-guvenlik-politikasi-siber-savas-icin-hazir-mi/ ,Nisan 2012

[18] ALKAN Mustafa, SAĞIROĞLU Şeref, TÜREKÇİ Tolga, ATALAY Ahmet Hamdi, BİLİRGEN Cabir, CANBEK Gürol, İNCEEFE Mehmet Ali, ÖZBİLEN Alper, ÜNVER Mustafa, YAZICI Ali, "Ulusal Bilgi Güvenliği Stratejisi", http://www.bilgiguvenligi.org.tr/index_files/pdf/Ulusal_Siber_Guvenlik_Stratejisi.pdf, Ekim 2012

[19] "Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı", www.resmigazete.gov.tr, Haziran 2013

[20] DURNA İlke Deniz, ÇALIŞKAN Emin, GÜL Ahmed Furkan, ONAY Oktay, GÖZÜKÜÇÜK Merve, TAŞÇI Burak, DÖVER Zeynep Sena, ÇELİK Burak, KINIKOĞLU Batu Yakup, ,ÜNAL Ahmet, Mehmet Bedii KAYA, "Siber Güvenlik Raporu", İstanbul Bilgi Üniversitesi Bilişim ve Teknoloji Enstitüsü,http://www.dktr-legal.com/upload/makaleler/Ulusal-Siber-Guvenlik-Raporu-Siber-Guvenlik-Calisma-Grubu-4.pdf, Mayıs 2012

[21] ŞENTÜRK Hakan, ÇİL C.Zaim, SAĞIROĞLU Şeref, " Cyber Security Analysis of Turkey", International Journal of Information Security Science, Vol 1, Mayıs 2012, (112-125)

Seda YILMAZ Gazi Üniversitesi Bilişim Enstitüsü Bilgisayar Bilimleri Bölümünde yüksek lisans eğitimine devam etmektedir. Araştırma konuları arasında kablosuz sensor ağlarda güvenlik, web yazılım güvenliği, siber güvenlik, bilgi ve bilgisayar güvenliği yer almaktadır.

Şeref SAĞIROĞLU Gazi Üniversitesi Mühendislik Fakültesi Bilgisayar Mühendisliği Bölümü öğretim üyesidir. Zeki sistem kimliklendirme, tanıma ve modelleme, ve kontrol; yapay sinir ağları ve yapay zeka uygulamaları; sezgisel algoritmalar; endüstriyel robotlar; zeki anten analizi ve tasarımı; internet, web ve bilişim sistemleri ve uygulamaları; yazılım mühendisliği; bilgi ve bilgisayar güvenliği; biometri, elektronik ve mobil elektronik imza ve açık anahtar altyapısı; kötücül ve casus yazılımlar gibi konularda çalışmaktadır. 50'nin üzerinde SCI tarafından taranan uluslar arası dergilerde yayınlanmış makalesi, 50'nin üzerinde ulusal dergilerde yayınlanmış makalesi, 100'ün üzerinde uluslar arası konferans ve sempozyum bildirisi ile ulusal sempozyum, konferans ve çalıştaylarda sunulmuş100'e yakın bildirisi bulunmaktadır. 3 adet alınmış patenti vardır. 5 adet yayınlanmış kitabı, 2 adet kitapta bölüm yazarlığı bulunmaktadır. 4 kitabın da editörlüğünü yapmıştır.

Ulusal ve uluslar arası pek çok proje yürütmüş ve konferanslar düzenlemiş olup akademik çalışmalarına devam etmektedir.